Data Processing Agreement

Effective October 8, 2026

This Data Processing Agreement is part of the Terms of Service between 24 DEALS FINDER LLC, doing business as WeeklyCert, a company organized in the State of Wyoming, United States ("Provider"), and the Customer that uses WeeklyCert. It is made of this Cover Page and the Common Paper Data Processing Agreement Standard Terms Version 1.1 printed below it, with the two changes listed at the end. It applies as soon as Customer accepts the Terms of Service; nothing more needs to be signed. A copy signed by both parties is available on request.

Cover Page

Key terms

Agreement. The Terms of Service at weeklycert.com/legal/terms.

Provider Security Contact. support@weeklycert.com, and in writing at 5830 E 2nd St, Ste 7000 #21954, Casper, WY 82609, USA.

Security Policy. Provider's written information security program, kept under New York General Business Law §899-bb and summarized in Annex II.

Governing Member State. Ireland, only where Section 3.2 applies. Customer Personal Data is about workers in the United States, so Sections 3.2 to 3.4 are not expected to apply.

Incident notice. Under Section 4.1, Provider notifies Customer without undue delay and no later than 72 hours after becoming aware of a Security Incident. Provider does not notify workers or authorities on Customer's behalf; Customer, as the owner of the data, decides on and gives those notices, and Provider helps with the facts.

Audits. Customer may send one written security questionnaire every 12 months to the Provider Security Contact, under Section 5.3. There are no on-site audits.

Annex I. Parties and processing details

A. Parties. Customer is the controller of Customer Personal Data (or the processor, where it acts for another company). Provider is the processor (or subprocessor), 24 DEALS FINDER LLC, 5830 E 2nd St, Ste 7000 #21954, Casper, WY 82609, USA, reached at support@weeklycert.com.

B. Categories of Data Subjects. Workers whose hours and pay Customer reports, and Customer's Users.

Categories of Personal Data. For workers: name, home address, the last four digits of the Social Security number or the date of birth, classification, apprentice registration, hours, rates, pay, fringe benefits and deductions. For Users: name, email address, role, sign-in records and the electronic signature on a certification. No full Social Security numbers and no bank or card account numbers.

Special Category Data. None. A health plan appears only as an amount per hour.

Nature and Purpose of Processing. Storing hours and pay data, calculating and checking certified payroll, producing the NYSDOL XML file and the WH-347, keeping the records Customer exports, sending the emails Customer's Users ask for, and support.

Frequency of Transfer. Continuous, while Customer uses the Service.

Duration of Processing. For the term of the Agreement and 30 days after it, during which Customer keeps read-only access and export; then Customer Personal Data is deleted and the key that encrypts workers' details is destroyed. Deleted data leaves backups as they expire, within 13 months.

Location. Customer Personal Data is stored in the United States. People authorized by Provider, currently one person, may access it remotely from outside the United States to support Customer and run the Service, under confidentiality obligations and the access controls in Annex II. Customer Personal Data is not exported to or stored outside the United States, except what Customer itself sends to support (Annex III, Zoho).

Annex II. Technical and organizational security measures

In transit. HTTPS only, TLS 1.2 or higher, with HSTS, end to end to the application server. The connection from the application to the database is encrypted.

At rest. The database and file storage are encrypted at rest by the hosting providers. In addition, workers' home addresses and dates of birth are encrypted in the database with a key that belongs to one Customer alone, itself encrypted with a master key kept outside the database.

Minimization. There is no field for a full Social Security number. When an imported file holds one, the Service keeps only its last four digits and does not store the file. A date of birth is kept only for a worker without the last four digits of a Social Security number. Worker home addresses are never printed on the WH-347.

Separation between customers. Every table that holds Customer data is restricted to one Customer in the database itself (row-level security), and tests check that one Customer can never read another's data.

Access control. Six roles with fixed permissions, set by the account owner. Two-factor authentication is required for the owner, administrators, signers and bookkeepers. Signing a certification asks for the password again.

Logging. Every change to business data and every security event is written to an audit log the account owner can read. Every read of a worker's home address or date of birth is logged, and the owner can see who read it and when. Application logs and error reports have personal data removed.

Backups and recovery. The database is backed up by the hosting provider and, separately, dumped daily to encrypted storage; a restore into an empty database is tested every week.

People. Access to production systems is limited to people authorized by Provider, currently one, who use two-factor authentication on every provider account. Access is reviewed every quarter.

Incidents. A written incident plan: contain, assess, notify Customer within 72 hours, fix and record.

Annex III. Approved Subprocessors

DigitalOcean, LLC. United States (New York). Hosts the application and its database; all Customer Personal Data.

Backblaze, Inc.. United States. Stores generated files, imports and encrypted database backups; all Customer Personal Data.

Cloudflare, Inc.. United States, with a global network. DNS, TLS and the network in front of the application; Customer Personal Data passes through it in transit and is not stored.

Stripe, Inc.. United States (for a seller in the EU: Ireland). Subscription billing. Receives the account owner's billing details, never worker data.

Resend (Plus Five Five, Inc.). United States. Delivers the emails the application sends to Users: names of Users, and names of projects and workers where a reminder needs them.

Functional Software, Inc. (Sentry). United States. Error reports from the application, with personal data removed before they are sent.

Zoho Corporation B.V.. European Union. The mailbox behind support@weeklycert.com: whatever Customer writes to support, including any Customer Personal Data Customer chooses to send.

Common Paper Data Processing Agreement Standard Terms Version 1.1

1. Processor and Subprocessor Relationships

1.1 Provider as Processor. In situations where Customer is a Controller of the Customer Personal Data, Provider will be deemed a Processor that is Processing Personal Data on behalf of Customer.

1.2 Provider as Subprocessor. In situations where Customer is a Processor of the Customer Personal Data, Provider will be deemed a Subprocessor of the Customer Personal Data.

2. Processing

2.1 Processing Details. Annex I(B) on the Cover Page describes the subject matter, nature, purpose, and duration of this Processing, as well as the Categories of Personal Data collected and Categories of Data Subjects.

2.2 Processing Instructions. Customer instructs Provider to Process Customer Personal Data: (a) to provide and maintain the Service; (b) as may be further specified through Customer's use of the Service; (c) as documented in the Agreement; and (d) as documented in any other written instructions given by Customer and acknowledged by Provider about Processing Customer Personal Data under this DPA. Provider will abide by these instructions unless prohibited from doing so by Applicable Laws. Provider will immediately inform Customer if it is unable to follow the Processing instructions. Customer has given and will only give instructions that comply with Applicable Laws.

2.3 Processing by Provider. Provider will only Process Customer Personal Data in accordance with this DPA, including the details in the Cover Page. If Provider updates the Service to update existing or include new products, features, or functionality, Provider may change the Categories of Data Subjects, Categories of Personal Data, Special Category Data, Special Category Data Restrictions or Safeguards, Frequency of Transfer, Nature and Purpose of Processing, and Duration of Processing as needed to reflect the updates by notifying Customer of the updates and changes.

2.4 Customer Processing. Where Customer is a Processor and Provider is a Subprocessor, Customer will comply with all Applicable Laws that apply to Customer's Processing of Customer Personal Data. Customer's agreement with its Controller will similarly require Customer to comply with all Applicable Laws that apply to Customer as a Processor. In addition, Customer will comply with the Subprocessor requirements in Customer's agreement with its Controller.

2.5 Consent to Processing. Customer has complied with and will continue to comply with all Applicable Data Protection Laws concerning its provision of Customer Personal Data to Provider and/or the Service, including making all disclosures, obtaining all consents, providing adequate choice, and implementing relevant safeguards required under Applicable Data Protection Laws.

2.6 Subprocessors.

a. Provider will not provide, transfer, or hand over any Customer Personal Data to a Subprocessor

unless Customer has approved the Subprocessor. The current list of Approved Subprocessors includes the identities of the Subprocessors, their country of location, and their anticipated Processing tasks. Provider will inform Customer at least 10 business days in advance and in writing of any intended changes to the Approved Subprocessors whether by addition or replacement of a Subprocessor, which allows Customer to have enough time to object to the changes before the Provider begins using the new Subprocessor(s). Provider will give Customer the information necessary to allow Customer to exercise its right to object to the change to Approved Subprocessors. Customer has 30 days after notice of a change to the Approved Subprocessors to object, otherwise Customer will be deemed to accept the changes. If Customer objects to the change within 30 days of notice, Customer and Provider will cooperate in good faith to resolve Customer's objection or concern.

b. When engaging a Subprocessor, Provider will have a written agreement with the Subprocessor that ensures the Subprocessor only accesses and uses Customer Personal Data (i) to the extent required to perform the obligations subcontracted to it, and (ii) consistent with the terms of Agreement.

c. If the GDPR applies to the Processing of Customer Personal Data, (i) the data protection obligations described in this DPA (as referred to in Article 28(3) of the GDPR, if applicable) are also imposed on the Subprocessor, and (ii) Provider's agreement with the Subprocessor will incorporate these obligations, including details about how Provider and its Subprocessor will coordinate to respond to inquiries or requests about the Processing of Customer Personal Data. In addition, Provider will share, at Customer's request, a copy of its agreements (including any amendments) with its Subprocessors. To the extent necessary to protect business secrets or other confidential information, including personal data, Provider may redact the text of its agreement with its Subprocessor prior to sharing a copy.

d. Provider remains fully liable for all obligations subcontracted to its Subprocessors, including the acts and omissions of its Subprocessors in Processing Customer Personal Data. Provider will notify Customer of any failure by its Subprocessors to fulfill a material obligation about Customer Personal Data under the agreement between Provider and the Subprocessor.

3. Restricted Transfers

3.1 Authorization. Customer agrees that Provider may transfer Customer Personal Data outside the EEA, the United Kingdom, or other relevant geographic territory as necessary to provide the Service. If Provider transfers Customer Personal Data to a territory for which the European Commission or other relevant supervisory authority has not issued an adequacy decision, Provider will implement appropriate safeguards for the transfer of Customer Personal Data to that territory consistent with Applicable Data Protection Laws.

3.2 Ex-EEA Transfers. Customer and Provider agree that if the GDPR protects the transfer of Customer Personal Data, the transfer is from Customer from within the EEA to Provider outside of the EEA, and the transfer is not governed by an adequacy decision made by the European Commission, then by entering into this DPA, Customer and Provider are deemed to have signed the EEA SCCs and their Annexes, which are incorporated by reference. Any such transfer is made pursuant to the EEA SCCs, which are completed as follows:

a. Module Two (Controller to Processor) of the EEA SCCs apply when Customer is a Controller and Provider is Processing Customer Personal Data for Customer as a Processor.

b. Module Three (Processor to Sub-Processor) of the EEA SCCs apply when Customer is a Processor and Provider is Processing Customer Personal Data on behalf of Customer as a

Subprocessor.

c. For each module, the following applies (when applicable):

i. The optional docking clause in Clause 7 does not apply;

ii. In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of Subprocessor changes is 10 business days;

iii. In Clause 11, the optional language does not apply;

iv. All square brackets in Clause 13 are removed;

v. In Clause 17 (Option 1), the EEA SCCs will be governed by the laws of Governing Member State;

vi. In Clause 18(b), disputes will be resolved in the courts of the Governing Member State; and

vii. The Cover Page to this DPA contains the information required in Annex I, Annex II, and Annex III of the EEA SCCs.

3.3 Ex-UK Transfers. Customer and Provider agree that if the UK GDPR protects the transfer of Customer Personal Data, the transfer is from Customer from within the United Kingdom to Provider outside of the United Kingdom, and the transfer is not governed by an adequacy decision made by the United Kingdom Secretary of State, then by entering into this DPA, Customer and Provider are deemed to have signed the UK Addendum and their Annexes, which are incorporated by reference. Any such transfer is made pursuant to the UK Addendum, which is completed as follows:

a. Section 3.2 of this DPA contains the information required in Table 2 of the UK Addendum.

b. Table 4 of the UK Addendum is modified as follows: Neither party may end the UK Addendum as set out in Section 19 of the UK Addendum; to the extent ICO issues a revised Approved Addendum under Section 18 of the UK Addendum, the parties will work in good faith to revise this DPA accordingly.

c. The Cover Page contains the information required by Annex 1A, Annex 1B, Annex II, and Annex III of the UK Addendum.

3.4 Other International Transfers. For Personal Data transfers where Swiss law (and not the law in any EEA member state or the United Kingdom) applies to the international nature of the transfer, references to the GDPR in Clause 4 of the EEA SCCs are, to the extent legally required, amended to refer to the Swiss Federal Data Protection Act or its successor instead, and the concept of supervisory authority will include the Swiss Federal Data Protection and Information Commissioner.

4. Security Incident Response

4.1 Upon becoming aware of any Security Incident, Provider will: (a) notify Customer without undue delay when feasible, but no later than 72 hours after becoming aware of the Security Incident; (b) provide timely information about the Security Incident as it becomes known or as is reasonably requested by Customer; and (c) promptly take reasonable steps to contain and investigate the Security Incident. Provider's notification of or response to a Security Incident as required by this DPA will not be construed as an acknowledgment by Provider of any fault or liability for the Security Incident.

5. Audit & Reports

5.1 Audit Rights. Provider will give Customer all information reasonably necessary to demonstrate its compliance with this DPA and Provider will allow for and contribute to audits, including inspections by

Customer, to assess Provider's compliance with this DPA. However, Provider may restrict access to data or information if Customer's access to the information would negatively impact Provider's intellectual property rights, confidentiality obligations, or other obligations under Applicable Laws. Customer acknowledges and agrees that it will only exercise its audit rights under this DPA and any audit rights granted by Applicable Data Protection Laws by instructing Provider to comply with the reporting and due diligence requirements below. Provider will maintain records of its compliance with this DPA for 3 years after the DPA ends.

5.2 Security Reports. Provider does not currently hold an audit report by an independent third-party auditor, and there is no Report. Upon written request, Provider will give Customer, on a confidential basis, a summary of its then-current written information security program so that Customer can review Provider's compliance with the Security Policy.

5.3 Security Due Diligence. In addition to the Report, Provider will respond to reasonable requests for information made by Customer to confirm Provider's compliance with this DPA, including responses to information security, due diligence, and audit questionnaires, or by giving additional information about its information security program. All such requests must be in writing and made to the Provider Security Contact and may only be made once a year.

6. Coordination & Cooperation

6.1 Response to Inquiries. If Provider receives any inquiry or request from anyone else about the Processing of Customer Personal Data, Provider will notify Customer about the request and Provider will not respond to the request without Customer's prior consent. Examples of these kinds of inquiries and requests include a judicial or administrative or regulatory agency order about Customer Personal Data where notifying Customer is not prohibited by Applicable Law, or a request from a data subject. If allowed by Applicable Law, Provider will follow Customer's reasonable instructions about these requests, including providing status updates and other information reasonably requested by Customer. If a data subject makes a valid request under Applicable Data Protection Laws to delete or opt out of Customer's giving of Customer Personal Data to Provider, Provider will assist Customer in fulfilling the request according to the Applicable Data Protection Law. Provider will cooperate with and provide reasonable assistance to Customer, at Customer's expense, in any legal response or other procedural action taken by Customer in response to a third-party request about Provider's Processing of Customer Personal Data under this DPA.

6.2 DPIAs and DTIAs. If required by Applicable Data Protection Laws, Provider will reasonably assist Customer in conducting any mandated data protection impact assessments or data transfer impact assessments and consultations with relevant data protection authorities, taking into consideration the nature of the Processing and Customer Personal Data.

7. Deletion of Customer Personal Data

7.1 Deletion by Customer. Provider will enable Customer to delete Customer Personal Data in a manner consistent with the functionality of the Services. Provider will comply with this instruction as soon as reasonably practicable except where further storage of Customer Personal Data is required by Applicable Law.

7.2 Deletion at DPA Expiration.

a. After the DPA expires, Provider will return or delete Customer Personal Data at Customer's instruction unless further storage of Customer Personal Data is required or authorized by Applicable Law. If return or destruction is impracticable or prohibited by Applicable Laws, Provider will make reasonable efforts to prevent additional Processing of Customer Personal Data and will continue to protect the Customer Personal Data remaining in its possession, custody, or control. For example,

Applicable Laws may require Provider to continue hosting or Processing Customer Personal Data.

b. If Customer and Provider have entered the EEA SCCs or the UK Addendum as part of this DPA, Provider will only give Customer the certification of deletion of Personal Data described in Clause 8.1(d) and Clause 8.5 of the EEA SCCs if Customer asks for one.

8. Limitation of Liability

8.1 Liability Caps and Damages Waiver. **To the maximum extent permitted under Applicable Data Protection Laws, each party's total cumulative liability to the other party arising out of or related to this DPA will be subject to the waivers, exclusions, and limitations of liability stated in the Agreement.**

8.2 Related-Party Claims. **Any claims made against Provider or its Affiliates arising out of or related to this DPA may only be brought by the Customer entity that is a party to the Agreement.**

8.3 Exceptions. This DPA does not limit any liability to an individual about the individual's data protection rights under Applicable Data Protection Laws. In addition, this DPA does not limit any liability between the parties for violations of the EEA SCCs or UK Addendum.

9. Conflicts Between Documents

9.1 This DPA forms part of and supplements the Agreement. If there is any inconsistency between this DPA, the Agreement, or any of their parts, the part listed earlier will control over the part listed later for that inconsistency: (1) the EEA SCCs or the UK Addendum, (2) this DPA, and then (3) the Agreement.

10. Term of Agreement

10.1 This DPA will start when Provider and Customer agree to a Cover Page for the DPA and sign or electronically accept the Agreement and will continue until the Agreement expires or is terminated. However, Provider and Customer will each remain subject to the obligations in this DPA and Applicable Data Protection Laws until Customer stops transferring Customer Personal Data to Provider and Provider stops Processing Customer Personal Data.

11. Definitions

11.1 **"Applicable Laws"** means the laws, rules, regulations, court orders, and other binding requirements of a relevant government authority that apply to or govern a party.

11.2 **"Applicable Data Protection Laws"** means the Applicable Laws that govern how the Service may process or use an individual's personal information, personal data, personally identifiable information, or other similar term.

11.3 **"Controller"** will have the meaning(s) given in the Applicable Data Protection Laws for the company that determines the purpose and extent of Processing Personal Data.

11.4 **"Cover Page"** means a document that is signed or electronically accepted by the parties that incorporates these DPA Standard Terms and identifies Provider, Customer, and the subject matter and details of the data processing.

11.5 **"Customer Personal Data"** means Personal Data that Customer uploads or provides to Provider as part of the Service and that is governed by this DPA.

11.6 **"DPA"** means these DPA Standard Terms, the Cover Page between Provider and Customer, and the policies and documents referenced in or attached to the Cover Page.

11.7 **"EEA SCCs"** means the standard contractual clauses annexed to the European Commission's

Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the European Council.

11.8 **"European Economic Area"** or **"EEA"** means the member states of the European Union, Norway, Iceland, and Liechtenstein.

11.9 **"GDPR"** means European Union Regulation 2016/679 as implemented by local law in the relevant EEA member nation.

11.10 **"Personal Data"** will have the meaning(s) given in the Applicable Data Protection Laws for personal information, personal data, or other similar term.

11.11 **"Processing"** or **"Process"** will have the meaning(s) given in the Applicable Data Protection Laws for any use of, or performance of a computer operation on, Personal Data, including by automatic methods.

11.12 **"Processor"** will have the meaning(s) given in the Applicable Data Protection Laws for the company that Processes Personal Data on behalf of the Controller.

11.13 **"Report"** means audit reports prepared by another company according to the standards defined in the Security Policy on behalf of Provider.

11.14 **"Restricted Transfer"** means (a) where the GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; and (b) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not subject to adequacy regulations adopted pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

11.15 **"Security Incident"** means a Personal Data Breach as defined in Article 4 of the GDPR, or a breach of the security of the system as defined in New York General Business Law §899-aa, affecting Customer Personal Data.

11.16 **"Service"** means the product and/or services described in the Agreement.

11.17 **"Special Category Data"** will have the meaning given in Article 9 of the GDPR.

11.18 **"Subprocessor"** will have the meaning(s) given in the Applicable Data Protection Laws for a company that, with the approval and acceptance of Controller, assists the Processor in Processing Personal Data on behalf of the Controller.

11.19 **"UK GDPR"** means European Union Regulation 2016/679 as implemented by section 3 of the United Kingdom's European Union (Withdrawal) Act of 2018 in the United Kingdom.

11.20 **"UK Addendum"** means the international data transfer addendum to the EEA SCCs issued by the Information Commissioner for Parties making Restricted Transfers under S119A(1) Data Protection Act 2018.

The Standard Terms above are the Common Paper Data Processing Agreement Standard Terms Version 1.1 (https://commonpaper.com/standards/data-processing-agreement/1.1), by Common Paper, Inc., licensed under CC BY 4.0 (https://creativecommons.org/licenses/by/4.0/). The Cover Page is ours.

Changes to the Standard Terms: Section 5.2 (Security Reports) is replaced, because Provider is not audited by an independent third party and has no audit report; Section 11.15 ("Security Incident") also covers a breach of the security of the system under New York General Business Law §899-aa. Everything else is printed without change.