This Data Processing Addendum ("**Addendum**") may be referenced and incorporated by reference into an Enterprise Services Agreement (the "**Agreement"**) between Ironclad, Inc. ("**Ironclad**") and a customer ("**Customer**" (collectively the "**Parties**")).

1. **Subject Matter and Duration.**

    a. **Subject Matter.** This Addendum reflects the Parties' commitment to abide by Applicable Data Protection Laws concerning the Processing of Customer Personal Data in connection with Ironclad's execution of the Agreement. All capitalized terms that are not expressly defined in this Data Processing Addendum will have the meanings given to them in the Agreement. If and to the extent language in this Addendum or any of its Exhibits conflicts with the Agreement, this Addendum shall control.

    b. **Duration and Survival.** This Addendum will become legally binding upon the Effective Date of the Agreement or upon the date upon which both Parties have signed this Addendum, if it is completed after the Effective Date of the Agreement. Ironclad will Process Customer Personal Data until the relationship terminates as specified in the Agreement. Ironclad's obligations and Customer's rights under this Addendum will continue in effect so long as Ironclad Processes Customer Personal Data.

2. **Definitions.** For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

    a. **"Applicable Data Protection Law(s)"** means the relevant data protection and data privacy laws, rules and regulations to which the Customer Personal Data are subject. "Applicable Data Protection Law(s)" shall include, but not be limited to, EU General Data Protection Regulation 2016/679 ("GDPR") principles and requirements, the United Kingdom Data Protection Act 2018, and the California Consumer Privacy Act of 2018 ("CCPA"), and its implementing regulations. For the avoidance of doubt, if Ironclad's processing activities involving Customer Personal Data are not within the scope of an Applicable Data Protection Law, such law is not applicable for purposes of this Addendum.

    b. **"Customer Personal Data"** means Personal Data pertaining to Customer's users or employees Processed by Ironclad to provide the Services. The Customer Personal Data and the specific uses of the Customer Personal Data are detailed in **Exhibit 1** attached hereto, as required by the GDPR.

    c. **"Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

    d. **"Personal Data"** shall have the meaning assigned to the terms "personal data" or "personal information" under Applicable Data Protection Law(s).

    e. **"Process," "Processes," "Processing," "Processed"** means any operation or set of operations which is performed on data or sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

    f. **"Processor"** means a natural or legal person, public authority, agency or other body which Processes Customer Personal Data on behalf of Customer subject to this Addendum.

    g. **"Security Incident(s)"** means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data Processed by Ironclad.

    h. **"Services"** means any and all services that Ironclad performs under the Agreement.

    i. **"Standard Contractual Clauses"** means the UK Standard Contractual Clauses, and/or the 2021 Standard

Contractual Clauses.

j. **"Third Party(ies)"** means Ironclad's authorized contractors, agents, vendors and third party service providers that Process Customer Personal Data.

k. **"UK Standard Contractual Clauses"** means the Standard Contractual Clauses for data controller to data processor transfers approved by the European Commission in decision 2010/87/EU.

l. **"2021 Standard Contractual Clauses"** means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.

3. **Data Use and Processing.**

a. Compliance with Laws. Customer Personal Data shall be Processed in compliance with the terms of this Addendum and all Applicable Data Protection Law(s).

b. Purpose Limitation. Ironclad will not Process Customer Personal Data for any purpose other than for the specific purposes set forth in the Agreement, unless obligated to do otherwise by applicable law. In such case, Ironclad will inform Customer of that legal requirement before the Processing unless legally prohibited from doing so.

c. Documented Instructions. Ironclad and its Third Parties shall Process Customer Personal Data only in accordance with the documented instructions of Customer. The Agreement, including this Addendum, along with any applicable statement of work, constitute Customer's complete and final instructions to Ironclad regarding the Processing of Customer Personal Data, including for purposes of the Standard Contractual Clauses. Ironclad will, unless legally prohibited from doing so, inform Customer in writing if it reasonably believes that there is a conflict between Customer's instructions and applicable law or otherwise seeks to Process Customer Personal Data in a manner that is inconsistent with Customer's instructions.

d. Authorization to Use Third Parties. To the extent necessary to fulfill Ironclad's contractual obligations under the Agreement or any statement of work, Customer hereby authorizes (i) Ironclad to engage Third Parties and (ii) Third Parties to engage subprocessors.

e. Ironclad and Third Party Compliance. Ironclad agrees to (i) enter into a written agreement with Third Parties regarding such Third Parties' Processing of Customer Personal Data that imposes on such Third Parties (and their subprocessors) data protection and security requirements for Customer Personal Data that are at least as restrictive as the obligations in this Addendum; and (ii) remain responsible to Customer for Ironclad's Third Parties' (and their subprocessors if applicable) failure to perform their obligations with respect to the Processing of Customer Personal Data.

f. Right to Object to Third Parties. Ironclad's list of Third Parties that Process Customer Personal Data is available at https://ironcladapp.com/subprocessors/. Solely for Acceptance Services, Ironclad will also use the following additional Third Parties that Process Customer Personal Data.

Third Party	**Processing Activity**
Amazon Web Services	Cloud service provider for hosting
MongoDB Atlas	Cloud service provider for database hosting and management

Twilio	Inbound/outbound SMS and mobile messaging provider
Twilio SendGrid	Outbound email service provider
MailChimp	Outbound email service provider
FullStory	Cloud-based customer experience and insight service provider
Intercom	Cloud-based customer support and live chat service provider
Planhat	Cloud-based customer success service provider
Zapier	Cloud-based workflow automation service provider

Prior to engaging any new Third Parties that Process Customer Personal Data, Ironclad will notify Customer via email and allow Customer thirty (30) days to object. If Customer has legitimate objections to the appointment of any new Third Party, the parties will work together in good faith to resolve the grounds for the objection for no less than thirty (30) days, and failing any such resolution, Customer may terminate the part of the service performed under the Agreement that cannot be performed by Ironclad without use of the objectionable Third Party.

g. Confidentiality. Any person or Third Party authorized to Process Customer Personal Data must agree to maintain the confidentiality of such information or be under an appropriate statutory or contractual obligation of confidentiality.

h. Personal Data Inquiries and Requests. Upon written request from Customer, Ironclad agrees to provide reasonable assistance and comply with all reasonable instructions from Customer related to any requests from individuals exercising their rights in Customer Personal Data granted to them under Applicable Data Protection Laws (e.g., access, rectification, erasure, data portability, etc.). If a request is sent directly to Ironclad, Ironclad shall promptly notify Customer and shall not respond to the request unless Customer has authorized Ironclad to do so.

i. Data Protection Impact Assessment and Prior Consultation. Upon written request from Customer, Ironclad agrees to provide reasonable assistance at Customer's expense to Customer where, in Customer's judgment, the type of Processing performed by Ironclad is likely to result in a high risk to the rights and freedoms of natural persons (e.g., systematic and extensive profiling, Processing sensitive Personal Data on a large scale and systematic monitoring on a large scale, or where the Processing uses new technologies) and thus requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

j. Sale of Customer Personal Data Prohibited. Ironclad shall not sell Customer Personal Data as the term "sell" is defined by the CCPA.

k. CCPA Certification. Ironclad hereby certifies that it understands its restrictions and obligations set forth in this Addendum and will comply with them.

4. **Cross-Border Transfers of Personal Data.**

    a. Cross-Border Transfers of Personal Data. Customer authorizes Ironclad and its Third Parties to transfer

Customer Personal Data across international borders, including from the European Economic Area (the "**EEA**"), the United Kingdom, and Switzerland to the United States, and if Customer's Order Form includes Acceptance Services, from the United States to Japan. Ironclad and Customer agree to use the Standard Contractual Clauses as the adequacy mechanism supporting the transfer and Processing of Customer Personal Data, as further detailed below.

b. UK Standard Contractual Clauses. For transfers of Customer Personal Data out of the United Kingdom that are subject to Section 4(a) of this Addendum, the UK Standard Contractual Clauses will apply and are incorporated into this Addendum by reference, provided that the illustrative indemnification clause within Appendix 2 of the UK Standard Contractual Clauses will not apply. **Exhibit 1** of this Addendum will serve as Appendix 1 of the UK Standard Contractual Clauses.

c. 2021 Standard Contractual Clauses. For transfers of Customer Personal Data out of the EEA or Switzerland that are subject to Section 4(a) of this DPA, the 2021 Standard Contractual Clauses will apply and are incorporated into this Addendum. For purposes of this Addendum, the 2021 Standard Contractual Clauses will apply as set forth in this Section 4(c). "Module Two: Transfer controller to processor" will apply and all other module options will not apply. Under Annex 1 of the 2021 Standard Contractual Clauses, the "data exporter" is Customer and the "data importer" is Ironclad and the information required by Annex 1 can be found in **Exhibit 1**. For the purposes of Annex 2 of the Standard Contractual Clauses, the technical and organizational measures implemented by the data importer are those listed in Section 5 of this Addendum. Clause 7 will not apply. For clause 9, the Parties choose Option 2 and the Parties agree that the time period for prior notice of Third Party changes will be as set forth in 3(f) of this Addendum. For clause 11, the optional language will not apply. For clause 17, the Parties choose Option 1 and the Parties agree that the governing law will be the Republic of Ireland. For clause 18, the Parties agree that the courts of the Republic of Ireland will apply for subsection (b).

d. Each party's signature to this Addendum shall be considered a signature to the Standard Contractual Clauses. If required by the laws or regulatory procedures of any jurisdiction, the Parties shall execute or re-execute the Standard Contractual Clauses as separate documents. In case of conflict between the Standard Contractual Clauses and this Addendum, the Standard Contractual Clauses will prevail.

5. **Information Security Program.**

a. Ironclad agrees to implement appropriate technical and organizational measures designed to protect Customer Personal Data as required by Applicable Data Protection Law(s) (the "I**nformation Security Program**"). Such measures shall be designed to include:

i. Pseudonymisation of Customer Personal Data where appropriate, and encryption of Customer Personal Data in transit and at rest;

ii. The ability to ensure the ongoing confidentiality, integrity, availability of Ironclad's Processing and Customer Personal Data;

iii. The ability to restore the availability and access to Customer Personal Data in the event of a physical or technical incident;

iv. A process for regularly testing, assessing and evaluating the effectiveness of Ironclad's Information Security Program to ensure the security of Customer Personal Data from reasonably suspected or actual accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.

6. **Security Incidents.**

a. Security Incident Procedure. Ironclad will deploy and follow policies and procedures to detect, respond to, and otherwise address Security Incidents including procedures to (i) identify and respond to reasonably

suspected or known Security Incidents, mitigate harmful effects of Security Incidents, document Security Incidents and their outcomes, and (ii) restore the availability or access to Customer Personal Data in a timely manner.

b. Notice. Ironclad agrees to provide prompt written notice without undue delay and within the time frame required under Applicable Data Protection Law(s) (but in no event longer than forty-eight (48) hours) to Customer's Designated POC upon becoming aware that a Security Incident has taken place. Such notice will include all available details required under Applicable Data Protection Law(s) for Customer to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident.

7. **Audits.**

a. Right to Audit; Permitted Audits. Ironclad shall make available to Customer and its regulators all information necessary to demonstrate compliance with Applicable Data Protection Laws and this Addendum. Customer and its regulators shall have the right to inspect Ironclad's architecture, systems, and documentation which are relevant to the security and integrity of Customer Personal Data, or as otherwise required by a governmental regulator:

   i. Following any notice from Ironclad to Customer of an actual or reasonably suspected Security Incident involving Customer Personal Data;

   ii. Upon Customer's reasonable belief that Ironclad is not in compliance with Applicable Data Protection Laws, this Addendum or its security policies and procedures under the Agreement;

   iii. As required by governmental regulators;

   iv. For any reason, or no reason at all, once annually.

b. Audit Terms. Any audits described in this Section shall be:

   i. Conducted by Customer or its regulator, or through a third party independent contractor selected by one of these parties, and to whom Ironclad does not reasonably object.

   ii. Conducted during reasonable times.

   iii. Conducted upon reasonable advance notice to Ironclad.

   iv. Of reasonable duration and scope and shall not unreasonably interfere with Ironclad's day-to-day operations.

   v. Conducted in such a manner that does not violate any agreement between Ironclad and its service providers, including cloud providers, or violate or cause Ironclad to violate its reasonable policies related to security and confidentiality.

c. Third Parties. In the event that Customer conducts an audit through a third party independent auditor or a third party accompanies Customer or participates in such audit, such third party shall be required to enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect Ironclad's and Ironclad's customers' confidential and proprietary information. For the avoidance of doubt, regulators shall not be required to enter into a non-disclosure agreement.

d. Audit Results. Upon Ironclad's request, after conducting an audit, Customer shall notify Ironclad of the manner in which Ironclad does not comply with any of the applicable security, confidentiality or privacy obligations or Applicable Data Protection Laws herein. Upon such notice, Ironclad shall make any necessary changes to ensure compliance with such obligations at its own expense and without unreasonable delay and shall notify Customer when such changes are complete. Notwithstanding anything to the contrary in the Agreement, Customer may conduct a follow-up audit within six (6) months of Ironclad's notice of completion of any necessary changes. To the extent that a Customer audit identifies any material security vulnerabilities,

Ironclad shall promptly remediate those vulnerabilities.

8. **Data Storage and Deletion.**

    a. Data Storage. Ironclad will not store or retain any Customer Personal Data except as necessary to perform the Services under the Agreement.

    b. Data Deletion. Ironclad will abide by the following with respect to deletion of Customer Personal Data:

        i. Within ninety (90) calendar days of the Agreement's expiration or termination, Ironclad will securely destroy (per subsection (iii) below) all copies of Customer Personal Data (including automatically created archival copies).

        ii. Upon Customer's request, Ironclad will promptly return to Customer a copy of all Customer Personal Data within thirty (30) calendar days and, if Customer also requests deletion of the Customer Personal Data, will carry that out as set forth above.

        iii. All deletion of Customer Personal Data will be conducted in accordance with standard industry practices for deletion of sensitive data.

        iv. Tapes, printed output, optical disks, and other physical media will be physically destroyed by a secure method, such as shredding performed by a bonded provider.

        v. Upon Customer's request, Ironclad will provide evidence that Ironclad has deleted all Customer Personal Data. Ironclad will provide the "Certificate of Deletion" within thirty (30) calendar days of Customer's request.

9. **Contact Information.**

    a. Ironclad and the Customer agree to designate a point of contact for urgent privacy and security issues (a "**Designated POC**"). The Designated POC for both parties are:

        - Ironclad Designated POC: John Fiedler, support@ironcladhq.com
        - Customer Designated POC: The individual and email specified in Section 2.5 of the Agreement. If no individual and email is specified in Section 2.5 of the Agreement, then the Customer notice email specified in the Notices section of the Agreement.

Exhibit 1

1.1 Subject Matter of Processing	The subject matter of Processing is the Services pursuant to the Agreement.
1.2 Duration of Processing	The Processing will continue until the expiration or termination of the Agreement.
1.3 Categories of Data Subjects	Includes the following: ● Prospects, customers, business partners and vendors of Customer (who are natural persons) ● Employees or contact persons of Customer's prospects, customers, business partners and vendors ● Employees, agents, advisors, freelancers of Customer (who are natural persons)

1.4 Nature and Purpose of Processing	Includes the following: Nature: Processing of the data uploaded by Customer to Ironclad's contract management SaaS application. The purpose of Processing of Customer Personal Data by Ironclad is the performance of the Services pursuant to the Agreement.
1.5 Types of Personal Information	Includes the following: ● First and last name ● Title ● Position ● Employer ● Contact information (company, email, phone, physical business address) ● Identification Data (notably email addresses and phone numbers) ● Electronic identification data (notably IP addresses and mobile device IDs)