

# DATA PROCESSING AGREEMENT

*Pazar platform | Controller to Processor | Version 1.5 | 11 October 2026*

This Data Processing Agreement (“DPA”) forms part of, and is incorporated into, the agreement for the provision of the Pazar platform and related services (the “Principal Agreement”) between Pazar IP, Inc., a Delaware corporation with offices at 2554 Lincoln Blvd, Number 2006, Venice, CA 90291, United States (“Pazar” or “Processor”), and the customer identified in the Principal Agreement (“Customer” or “Controller”). Each is a “Party” and together the “Parties.”

This DPA reflects the Parties’ agreement on the Processing of Personal Data in connection with the Services. Where Customer acts on behalf of its own affiliates or clients, references to Controller include those parties as applicable.

## 1. Definitions

- 1.1 Capitalized terms used but not defined in this DPA have the meaning given in the Principal Agreement.
- 1.2 “Data Protection Laws” means all laws and regulations applicable to the Processing of Personal Data under the Principal Agreement, including, as applicable: (a) the EU General Data Protection Regulation (Regulation (EU) 2016/679) (“EU GDPR”); (b) the EU GDPR as it forms part of the law of the United Kingdom (the “UK GDPR”) and the Data Protection Act 2018; (c) the Swiss Federal Act on Data Protection (the “FADP”); and (d) US State Privacy Laws.
- 1.3 “US State Privacy Laws” means the California Consumer Privacy Act, as amended by the California Privacy Rights Act (the “CCPA”), and other comprehensive US state privacy statutes applicable to the Processing, including those of Virginia, Colorado, Connecticut, and similar states.
- 1.4 “Controller,” “Processor,” “Data Subject,” “Personal Data,” “Personal Data Breach,” “Processing,” and “Special Categories of Personal Data” have the meanings given in the EU GDPR. Equivalent terms in other Data Protection Laws (including “Business,” “Service Provider,” “Sale,” and “Share” under the CCPA) carry their corresponding meanings.
- 1.5 “Standard Contractual Clauses” or “EU SCCs” means the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission in Implementing Decision (EU) 2021/914.
- 1.6 “Sub-processor” means any third party engaged by Pazar to Process Personal Data in connection with the Services.

## 2. Roles and Scope

- 2.1 For Personal Data Processed under the Principal Agreement, Customer is the Controller and Pazar is the Processor. Where Customer is itself a processor acting on behalf of a third-party controller, Pazar acts as sub-processor and the obligations in this DPA apply to Pazar accordingly.
- 2.2 This DPA applies to the Processing of Personal Data by Pazar on behalf of Customer in the course of providing the Services, as described in Annex 1.

2.3 Each Party shall comply with its respective obligations under Data Protection Laws.

### **3. Processing of Personal Data**

3.1 Pazar shall Process Personal Data only on documented instructions from Customer, including with regard to international transfers, unless required to do otherwise by applicable law. In that case, Pazar shall inform Customer of the legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

3.2 The Principal Agreement, this DPA, and Customer's configuration and use of the Services constitute Customer's complete documented instructions. Any additional instruction outside the scope of the Services requires prior written agreement of the Parties.

3.3 Pazar shall inform Customer without undue delay if, in its opinion, an instruction infringes Data Protection Laws and may suspend the execution of the relevant instruction until Customer confirms or modifies it.

3.4 The subject matter, duration, nature and purpose of the Processing, the types of Personal Data, and the categories of Data Subjects are set out in Annex 1.

3.5 Customer shall not submit Special Categories of Personal Data to the Services.

### **4. Confidentiality**

4.1 Pazar shall ensure that persons authorized to Process the Personal Data are bound by an appropriate duty of confidentiality and have received appropriate guidance on their responsibilities.

4.2 Pazar shall limit access to Personal Data to personnel who require access to perform the Principal Agreement, on a need-to-know basis.

### **5. Security**

5.1 Taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of Processing, and the risk to Data Subjects, Pazar shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as described in Annex 3.

5.2 Pazar may update its security measures from time to time, provided that such updates do not materially reduce the overall level of protection of the Personal Data.

### **6. Sub-processing**

6.1 Customer provides general written authorization for Pazar to engage Sub-processors to Process Personal Data, subject to this Section 6. The Sub-processors engaged as of the effective date are listed in Annex 2.

6.2 Pazar shall impose on each Sub-processor, by written contract, data protection obligations no less protective than those set out in this DPA, and shall remain liable to Customer for the performance of each Sub-processor's obligations.

6.3 Pazar shall notify Customer of any intended addition or replacement of a Sub-processor at least thirty (30) days in advance, by email or through the Services, giving Customer the opportunity to object on reasonable data protection grounds. If Customer objects, the

Parties shall work together in good faith to resolve the concern. If no resolution is reached, Customer may, as its sole remedy, terminate the affected Services.

## **7. Data Subject Rights**

- 7.1 Taking into account the nature of the Processing, Pazar shall assist Customer by appropriate technical and organizational measures, insofar as reasonably possible, in fulfilling Customer's obligation to respond to requests by Data Subjects exercising their rights under Data Protection Laws.
- 7.2 If Pazar receives a request from a Data Subject relating to Personal Data Processed on behalf of Customer, Pazar shall, unless legally prohibited, promptly forward the request to Customer and shall not respond directly except on Customer's documented instructions.

## **8. Personal Data Breach**

- 8.1 Pazar shall notify Customer without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach affecting Customer's Personal Data.
- 8.2 The notification shall, to the extent available, describe the nature of the breach, its likely consequences, and the measures taken or proposed to address it. Pazar shall provide further information in phases as it becomes available.
- 8.3 Pazar shall take reasonable steps to mitigate and, where possible, remediate the Personal Data Breach.

## **9. Data Protection Impact Assessments**

- 9.1 Pazar shall provide reasonable assistance to Customer with data protection impact assessments and prior consultations with supervisory authorities that Customer is required to carry out under Data Protection Laws, taking into account the nature of the Processing and the information available to Pazar.
- 9.2 Taking into account the nature of the Processing and the information available to Pazar, Pazar shall provide reasonable assistance to Customer in ensuring compliance with Customer's obligations under Articles 32 to 36 of the EU GDPR, including obligations relating to the security of Processing, the notification and communication of Personal Data Breaches, data protection impact assessments and prior consultation with supervisory authorities.

## **10. Deletion or Return of Personal Data**

- 10.1 Upon termination or expiry of the Principal Agreement, Pazar shall, at Customer's choice, delete or return all Personal Data Processed on behalf of Customer and delete existing copies, within ninety (90) days, unless applicable law requires continued storage. Backup copies are erased or overwritten within a further thirty (30) days. The deletion obligations in this Section 10 do not extend to (a) signature completion and audit-trail evidence that the e-signature Sub-processor retains for at least seven (7) years to support the legal validity of signed documents, and (b) copies in that Sub-processor's backup systems, which are deleted under its standard backup cycle, in each case as disclosed in Annex 2.

10.2 Customer may export the activity history of each deal in the Services at any time and may request a full export or the deletion of its Personal Data by contacting Pazar; Pazar shall comply within thirty (30) days.

## **11. Audits**

11.1 Pazar shall make available to Customer the information reasonably necessary to demonstrate compliance with this DPA, including, where available, third-party audit reports or certifications (such as SOC 2 or ISO 27001).

11.2 Where such documentation is insufficient, Customer, or an independent auditor mandated by Customer and reasonably acceptable to Pazar and bound by confidentiality, may conduct an audit no more than once in any twelve (12) month period, on at least thirty (30) days' prior written notice, during business hours, and in a manner that does not unreasonably disrupt Pazar's operations. Each Party shall bear its own costs. More frequent audits may be carried out where required by a supervisory authority or following a Personal Data Breach.

## **12. International Transfers**

12.1 Customer authorizes Pazar to transfer Personal Data outside the European Economic Area, the United Kingdom, and Switzerland to the extent necessary to provide the Services, subject to appropriate safeguards under this Section 12 and Annex 4.

12.2 Where Pazar Processes Personal Data subject to the EU GDPR in a country that has not received an adequacy decision, the EU SCCs are incorporated into this DPA by reference and completed as set out in Annex 4: Module Two (Controller to Processor) where Customer acts as controller, and Module Three (Processor to Processor) where Customer acts as processor on behalf of a third-party controller.

12.3 For Personal Data subject to the UK GDPR, the EU SCCs as supplemented by the UK International Data Transfer Addendum (the "UK Addendum") apply, completed as set out in Annex 4.

12.4 For Personal Data subject to the FADP, the EU SCCs apply with the Swiss amendments set out in Annex 4.

12.5 To the extent Pazar or a Sub-processor self-certifies under the EU-US Data Privacy Framework (and its UK Extension or the Swiss-US Data Privacy Framework, as applicable), that framework may serve as an alternative basis for the relevant transfers. The Parties acknowledge that the EU SCCs serve as the primary transfer mechanism under this DPA.

## **13. US State Privacy Laws**

13.1 To the extent Pazar Processes Personal Data subject to US State Privacy Laws as a Service Provider or Processor on behalf of Customer (acting as Business or Controller), the terms of Annex 5 apply.

## **14. General**

14.1 Pazar's and Customer's liability under this DPA is subject to the limitations and exclusions of liability set out in the Principal Agreement.

14.2 In the event of a conflict between this DPA and the Principal Agreement, this DPA prevails with respect to its subject matter. In the event of a conflict between this DPA and the EU SCCs, the EU SCCs prevail.

14.3 This DPA is governed by the law specified in the Principal Agreement, except where Data Protection Laws or the EU SCCs require otherwise.

14.4 This DPA takes effect on the effective date of the Principal Agreement and remains in force for as long as Pazar Processes Personal Data on behalf of Customer.

**Agreed by the Parties:**

**PROCESSOR**

Pazar IP, Inc.

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

**CONTROLLER**

[CUSTOMER LEGAL NAME]

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

## Annex 1 – Details of the Processing

### A. List of Parties

Data Exporter / Controller: Customer, as identified in the Principal Agreement. Role: Controller (or processor where acting for a third-party controller). Activities: use of the Pazar platform to negotiate, execute, manage and administer licensing agreements.

Data Importer / Processor: Pazar IP, Inc., 2554 Lincoln Blvd, Number 2006, Venice, CA 90291, United States. Role: Processor. Activities: provision and operation of the Pazar platform and related services.

### B. Description of the Processing

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Subject matter</b>              | Provision of the Pazar licensing platform and related services to Customer.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Nature and purpose</b>          | Hosting, storage, transmission and processing of deal-room, contract and licensing data so that Customer can negotiate, execute, manage and administer licensing agreements, including AI-assisted document processing (analysis, extraction and summarization), AI-assisted rights analysis and royalty assessment, and AI-assisted discovery between licensors and potential partners operating on obfuscated data.                                                                                                                                                                                                                                                                                                                                 |
| <b>Categories of Data Subjects</b> | Customer's authorized users, to the extent their Personal Data is contained in Customer Content (including messages, approvals, electronic signatures and audit history); Customer's counterparties to licensing agreements and their representatives, including contact persons, employees, agents and authorized signatories, including Personal Data contained in correspondence with such counterparties and Personal Data included in, or associated with, the relevant agreements, including signature and signature audit information. Account and authentication data of authorized users that Pazar Processes for its own account administration is Processed under Pazar's own responsibility as controller and is not subject to this DPA. |
| <b>Categories of Personal Data</b> | Identification and contact data (names, email addresses, postal addresses, telephone numbers); business and professional data (company, role, title); agreement and transaction data (signatory details, deal terms, royalty data); electronic signature data; communications and audit history.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Special Categories</b>          | None                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Frequency</b>                   | Continuous, for the duration of the Services.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Duration</b>                    | For the term of the Principal Agreement plus the retention period in Section 10.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

### C. Competent Supervisory Authority

Where the data exporter is established in the EU, the competent supervisory authority shall be the supervisory authority of the Member State in which the data exporter is established. Where the data exporter is not established in the EU, the competent supervisory authority shall be determined in accordance with Clause 13(a) of the EU SCCs.

## Annex 2 – Sub-processors

Customer authorizes the engagement of the following Sub-processors as of the effective date. This list may be updated in accordance with Section 6.

| Sub-processor                                               | Purpose                                                                            | Location                                 | Transfer basis                                                              |
|-------------------------------------------------------------|------------------------------------------------------------------------------------|------------------------------------------|-----------------------------------------------------------------------------|
| Amazon Web Services, Inc. and Amazon Web Services EMEA SARL | Cloud hosting, database and file storage                                           | European Union (Frankfurt, eu-central-1) | AWS Data Processing Addendum; SCCs / DPF for any access from outside the EU |
| Amazon Web Services (Amazon Bedrock)                        | AI-assisted document processing, rights analysis, royalty assessment and discovery | European Union (Frankfurt, eu-central-1) | AWS Data Processing Addendum; no model training on inputs or outputs        |
| Cloudflare, Inc.                                            | DNS, edge network and application protection                                       | United States (global edge network)      | SCCs / DPF                                                                  |
| Resend (Plus Five Five, Inc.)                               | Transactional email (invitations, notifications)                                   | United States                            | SCCs / DPF                                                                  |
| Clerk, Inc.                                                 | Authentication and user identity management                                        | United States                            | SCCs / DPF                                                                  |
| Stripe, Inc.                                                | Subscription billing and tax; optional payment link for royalty invoices           | United States                            | SCCs / DPF                                                                  |
| Verdocs, Inc.                                               | Electronic signature and signature audit log                                       | United States (AWS, Virginia)            | Art. 28 GDPR terms; EU SCCs on request (see note)                           |

*Verdocs: Art. 28 GDPR terms in the order form (Schedule 3) and the data protection rider of 23 July 2026; EU SCCs are executed on request under those terms. Verdocs retains signature completion and audit-trail evidence for at least seven (7) years after signing to support the legal validity of signed documents; copies in its backup systems are deleted under its standard backup cycle (Section 10.1).*

*The current list of Sub-processors is published at [pazar-ip.com/legal/subprocessors](https://pazar-ip.com/legal/subprocessors). Pazar will update this Annex when Sub-processors change, in accordance with Section 6.*

## Annex 3 – Technical and Organizational Measures

Pazar implements and maintains the following technical and organizational measures, appropriate to the risk of the Processing:

| Measure                          | Description                                                                                                                                                                          |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Encryption                       | Personal Data is encrypted in transit using TLS, and at rest using industry-standard encryption provided by the underlying cloud infrastructure.                                     |
| Access control                   | Role-based access control and least-privilege principles; individual user authentication; access to production systems and Personal Data restricted to authorized personnel.         |
| Authentication                   | User authentication and session management provided through a dedicated identity provider, with support for strong credentials and multi-factor authentication.                      |
| Network and application security | Segregation of environments, secure software development practices, and protection of the application and its interfaces against unauthorized access.                                |
| Logging and monitoring           | Logging of relevant system and access events and monitoring to detect and respond to anomalies.                                                                                      |
| Resilience and backup            | Regular encrypted backups retained for a limited period, and resilient cloud infrastructure located in the European Union, to support availability and restoration of Personal Data. |
| Personnel                        | Confidentiality obligations for personnel and guidance on data protection responsibilities.                                                                                          |
| Sub-processor management         | Selection and contractual flow-down of data protection obligations to Sub-processors, as set out in Section 6.                                                                       |
| Incident response                | Procedures to detect, report and respond to Personal Data Breaches, as set out in Section 8.                                                                                         |
| Physical security                | Physical and environmental security of the infrastructure is delegated to the cloud provider (AWS data centers, ISO 27001 and SOC 2 certified).                                      |

## Annex 4 – Transfer Mechanisms

### 1. EU Standard Contractual Clauses (Modules Two and Three)

The EU SCCs are incorporated by reference and completed as follows:

- (a) Module Two (Controller to Processor) applies where Customer acts as controller; Module Three (Processor to Processor) applies where Customer acts as processor for a third-party controller. In each case Customer is the data exporter and Pazar is the data importer.
- (b) Clause 7 (Docking clause): applies.
- (c) Clause 9 (Use of sub-processors): Option 2 (general written authorization) applies, with a minimum prior notice period of thirty (30) days as set out in Section 6.
- (d) Clause 11 (Redress): the optional independent dispute resolution body does not apply.
- (e) Clause 17 (Governing law): the EU SCCs are governed by the law of Ireland, or, where that law does not allow for third-party beneficiary rights, the law of the EU member state in which the data exporter is established.
- (f) Clause 18 (Choice of forum): disputes shall be resolved before the courts of Ireland or of the data exporter's member state, as applicable under Clause 17.
- (g) Annex I.A (Parties): as set out in Annex 1.A. Annex I.B (Description): as set out in Annex 1.B. Annex I.C (Competent supervisory authority): as set out in Annex 1.C.
- (h) Annex II (Technical and organizational measures): as set out in Annex 3. Annex III (Sub-processors): as set out in Annex 2.

### 2. UK International Data Transfer Addendum

For transfers subject to the UK GDPR, the UK Addendum issued by the Information Commissioner's Office applies to the EU SCCs above. Table 1 (Parties) and Table 2 (Selected SCCs) are completed by reference to this DPA and its Annexes. Table 3 (Appendix Information) is completed by Annexes 1, 2 and 3. For Table 4, neither Party may end the Addendum as set out in Section 19 of the Addendum, except that the data importer may do so where required.

### 3. Swiss Amendments

For transfers subject to the FADP, the EU SCCs apply with the following amendments: (a) references to the EU GDPR are to be understood as references to the FADP insofar as the transfer is governed by the FADP; (b) the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner (the "FDPIC"); (c) the term "member state" must not be interpreted to exclude Data Subjects in Switzerland from suing for their rights in their place of habitual residence; and (d) until the entry into force of the revised FADP, the clauses also protect the data of legal entities.

## **Annex 5 – US State Privacy Laws Addendum**

This Annex applies where Pazar Processes Personal Data subject to US State Privacy Laws on behalf of Customer. Pazar acts as a Service Provider or Processor, and Customer acts as a Business or Controller.

1. Pazar shall Process Personal Data only to provide the Services (the business purpose) and in accordance with Customer's documented instructions, as set out in this DPA.
2. Pazar shall not: (a) sell or share Personal Data; (b) retain, use or disclose Personal Data for any purpose other than providing the Services, or outside the direct business relationship with Customer, except as permitted by US State Privacy Laws; or (c) combine Personal Data with personal information obtained from other sources, except as permitted by US State Privacy Laws.
3. Pazar certifies that it understands the restrictions in this Annex and will comply with them.
4. Pazar shall assist Customer in responding to verifiable consumer requests and shall notify Customer without undue delay if it determines that it can no longer meet its obligations under US State Privacy Laws.
5. Customer may take reasonable and appropriate steps to confirm that Pazar's use of Personal Data is consistent with Customer's obligations under US State Privacy Laws.

*End of Data Processing Agreement*