# DATA PROCESSING AGREEMENT

***Last updates***: December 9, 2025

At Humanly, Inc. ("Company", "we", "us", "our"), we are committed to respecting and protecting you ("you" "your" "Customer") and your Personal Information in accordance with this Data Processing Agreement ("DPA"). This DPA is subject to the Humanly Terms of Service ("Terms of Service") and Privacy Policy under which the Company provides certain services ("Services") to Customer. Any capitalized terms used but not defined in this DPA will have the meanings ascribed to them in the Terms of Service and Privacy Policy.

1. Definitions and Interpretation.

1.1 The following definitions and rules of interpretation apply in this DPA.

"Business Purpose" means the provision of Services to Customer pursuant to the Terms of Service, including any processing necessary to provide, maintain, secure, and improve the Services, or for any other purpose set forth in the Privacy Policy or otherwise agreed to by the parties in writing.

"Data Subject" means an individual who is the subject of the Personal Information and to whom or about whom the Personal Information relates or identifies, directly or indirectly.

"Personal Information" means any information the Company processes solely on behalf of Customer and solely as submitted to the Services by Customer or its authorized users, or generated by the Services in the course of providing functionality to Customer that (a) identifies or relates to an individual who can be identified directly or indirectly from that data alone or in combination with other information in the Company's possession or control, including, where applicable, "personal data" as defined under European Data Protection Law, or (b) the relevant Privacy and Data Protection Requirements otherwise define as protected personal information.

"Processing, processes, or process" means any activity that involves the use of Personal Information or that the relevant Privacy and Data Protection Requirements may otherwise include in the definition of processing, processes, or process. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including, but not limited to, organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Personal Information to third parties.

"European Data Protection Law" means (i) the EU GDPR; (ii) the UK Data Protection Laws; and (iii) the Swiss DPA.

"Privacy and Data Protection Requirements" means all applicable federal state, and foreign laws and regulations relating to the processing, protection, or privacy of the Personal Information, including where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction. This includes, but is not limited to: (i) the General Data Protection Regulation (EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC) ("EU GDPR"); (ii) in respect of the United Kingdom, the Data Protection Act 2018 and the General Data Protection Regulation as retained in UK law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR") (collectively, the "UK Data Protection Laws"); (iii) the Swiss Federal Data Protection Act of 25 September 2020, as amended ("Swiss DPA"); and (iv) the California Consumer Privacy Act of 2018 ("CCPA"), as amended by the California Privacy Rights Act of 2020 ("CPRA"), and any other applicable U.S. statutes governing the Processing of Personal Information, all as amended, replaced, or superseded.

"Security Breach" means any act or omission that compromises the security, confidentiality, or integrity of Personal Information or the physical, technical, administrative, or organizational safeguards put in place to protect it. The loss of or unauthorized access, disclosure, or acquisition of Personal Information is a Security Breach whether or not the incident rises to the level of a security breach under the Privacy and Data Protection Requirements.

"Standard Contractual Clauses, or SCC" means the European Commission's standard contractual clauses for the transfer of personal data from the European Union to third countries (Module Two), as set out in the Annex to Commission Decision (EU) 2021/914.

1.2 This DPA is subject to the terms of the Terms of Service and is incorporated into the Terms of Service. Interpretations and defined terms set forth in the Terms of Service apply to the interpretation of this DPA.

1.3 The Appendices form part of this DPA and will have effect as if set out in full in the body of this DPA. Any reference to this DPA includes the Appendices.

1.4 A reference to writing or written includes faxes and email.

1.5 In the case of conflict or ambiguity between: (a) any provision contained in the body of this DPA and any provision contained in the Appendices, the provision in the body of this DPA will prevail; (b) the terms of any accompanying invoice or other documents annexed to this DPA and any provision contained in the Appendices, the provision contained in the Appendices will prevail; (c) any of the provisions of this DPA and the provisions of the Terms of Service, the provisions of this DPA will prevail; and (d) any of the provisions of this DPA and if applicable, the Standard Contractual Clauses, the provisions of the Standard Contractual Clauses will prevail to the extent applicable.

1.6 Notwithstanding anything to the contrary in this DPA, this DPA is subject to any limitations of liability and disclaimers of damages set forth in the Terms of Service.

2. Personal Information and Processing Purposes.

2.1 **Roles of the Parties.** For the purposes of European Data Protection Law, the Customer is the "Controller" and the Company is the "Processor." For the purposes of the CCPA, the Customer is the "Business" and the Company is the "Service Provider."

2.2 **Processing on Behalf of Customer.** Company will process Personal Information only on documented instructions from Customer, including as provided through Customer's use of the Services and as described in this DPA. Company will not process Personal Information for its own independent purposes.

2.3 **Scope of Processing.** The relationship between the parties is limited to the provision of Services to Customer under the Terms of Service. This includes any processing necessary to provide, operate, maintain, secure, support, and improve the Services, or any other processing purpose set forth in the Privacy Policy or agreed to by the parties in writing. Any processing for service improvement uses only deidentified or aggregated information that does not identify Customer or any Data Subject.

2.4 **Customer Responsibilities.** The Customer retains control of the Personal Information and remains responsible for its compliance obligations under applicable Privacy and Data Protection Requirements, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to the Company.

2.5 **Ownership of Personal Information.** Customer retains all rights, title, and interest in and to Customer Personal Information. Company does not obtain any rights in the Personal Information except for the limited rights necessary to perform the Services.

2.6 **Appendix A** describes the general Personal Information categories and related types of Data Subjects the Company may process to fulfill the Business Purposes. The Customer discloses Personal Information to the Company only for the limited and specified Business Purposes.

3. Company's Obligations.

3.1 The Company will only process, retain, use, or disclose the Personal Information to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's instructions. The Company will not process, retain, use, or disclose the Personal Information for any other purpose, outside of the parties' business relationship, or in a way that does not comply with this DPA or Privacy and Data Protection Requirements. The Company will promptly notify the Customer if, in its opinion, the Customer's instruction would not comply with the Privacy and Data Protection Requirements.

3.2 The Company will promptly comply with any reasonable Customer request or instruction requiring the Company to amend, transfer, or delete the Personal Information, or to stop, mitigate, or remedy any unauthorized processing.

3.3 Company will maintain the confidentiality of all Personal Information and will not sell it to anyone, share it for cross-context behavioral advertising (targeted advertising) with anyone, or disclose it to third parties without specific authorization from the Customer or this DPA, unless required by law. If a law requires the Company to process or disclose Personal Information, the Company will inform the Customer of the legal requirement and give the Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.

3.4 The Company will reasonably assist the Customer with meeting the Customer's compliance obligations under Privacy and Data Protection Requirements, taking into account the nature of the Company's processing and the information available to the Company. To the extent required by European Data Protection Law, this assistance shall include help with data protection impact assessments and prior consultations with supervisory authorities. Customer will be responsible for any reasonable costs and fees incurred by the Company for providing such assistance.

3.5 The Company shall notify the Customer if it can no longer meet its obligations under this DPA due to a change in applicable law.

3.6 The Customer acknowledges that the Company is under no duty to investigate the completeness, accuracy, or sufficiency of any specific Customer instructions or the Personal Information other than as required under the Privacy and Data Protection Requirements.

4. Company's Employees.

4.1 The Company will limit Personal Information access to: (a) those employees who have a reasonable need to access such Personal Information to meet the Company's obligations under this DPA and the Terms of Service; and (b) the part or parts of the Personal Information that those employees strictly require for the performance of their duties.

4.2 The Company will ensure that all employees: (a) are informed of the Personal Information's confidential nature and use restrictions and are obliged to keep the Personal Information confidential; (b) have undertaken training on the Privacy and Data Protection Requirements relating to handling Personal Information and how it applies to their particular duties; and (c) are aware both of the Company's duties and their personal duties and obligations under the Privacy and Data Protection Requirements and this DPA.

5. Security

5.1 The Company must at all times implement appropriate technical and organizational measures designed to safeguard Personal Information against unauthorized or unlawful processing, access, copying, modification, storage, reproduction, display, or distribution, and against accidental loss, destruction, unavailability, or damage. These technical measures may include, but are not limited to items listed in our Appendix (Technical and Organizational Measures).

5.2 The Company must take reasonable precautions to preserve the integrity of any Personal Information it processes and to prevent any corruption or loss of the Personal Information, including but not limited to establishing effective back-up and data restoration procedures.

6. Security Breaches; Audits.

6.1 The Company will without undue delay, and in each case in accordance with any notice timeframe applicable under Privacy and Data Protection Requirements, notify the Customer if it becomes aware of any Security Breach involving Customer's Personal Information.

6.2 Immediately following any Security Breach, the parties will co-ordinate with each other to investigate the matter. The Company will reasonably co-operate with the Customer in the Customer's handling of the matter, including assisting with any investigation and making relevant records, logs, files, data reporting, and other materials required to comply with all Privacy and Data Protection Requirements.

6.3 The Company will not inform any third party of a Security Breach without first obtaining the Customer's prior written consent, except when law or regulation requires it.

6.4 Company will cover reasonable expenses associated with the performance of the obligations under Section 6.1 and Section 6.2, unless the matter arose from the Customer's specific instructions, negligence, willful default, or breach of this DPA, in which case the Customer will cover all expenses.

6.5 The Company shall make available to the Customer information necessary to demonstrate compliance with this DPA and applicable Privacy and Data Protection Requirements. Upon the Customer's written request, and subject to appropriate confidentiality obligations, the Company will provide a copy of its then-most recent third-party audits or certifications, such as SOC 2 Type 2 reports or ISO 27001 certifications. To the extent that such information is not sufficient to demonstrate compliance and an audit is required under applicable Privacy and Data Protection Requirements (including, where applicable, the GDPR), the Company shall permit an audit to be conducted by the Customer. The Company and Customer will discuss and agree in advance on the reasonable start date, scope, duration of, and security and confidentiality controls applicable to any such audit. The Company reserves the right to charge a fee (based on the Company's reasonable costs) for any such audit.

7. Cross-Border Transfers of Personal Information.

7.1 **Appendix A** lists all of the countries where the Company may receive, access, transfer, or store Personal Information. The Company must not receive, access, transfer, or store Personal Information outside the countries listed on Appendix A without the Customer's prior written consent.

7.2 The parties agree that the Standard Contractual Clauses (Module Two) are incorporated by reference into this DPA. The parties further agree that the completed Annexes attached to this DPA shall form part of the Standard Contractual Clauses.

7.3 If any Personal Information transfer between the Company and the Customer requires execution of Standard Contractual Clauses in order to comply with the Privacy and Data Protection Requirements, the parties will complete all relevant details in, and execute, the Standard Contractual Clauses, and take all other actions required to legitimize the transfer, including, implementing any needed supplementary measures or supervisory authority consultations.

7.4 The Company will not transfer any Personal Information to another country unless the transfer complies with the Privacy and Data Protection Requirements.

8. Sub-processors. Customer agrees and consents to the Company's use of sub-processors to process Personal Information. A list of the Company's current sub-processors is available as described in **Appendix A**. To the extent required by Privacy and Data Protection Requirements, the Company shall provide Customer with advance written notice of any proposed changes to the list of sub-processors. Customer may object to the appointment of a new sub-processor in writing within ten (10) business days of such notice, provided that such objection is based on reasonable grounds relating to data protection. If Customer objects, the Company will use reasonable efforts to make a commercially reasonable change in the configuration of its Services to avoid processing of Personal Information by the objected-to sub-processor. If the Company is unable to make such a change within a reasonable period, which shall not exceed thirty (30) days, Customer may, as its sole and exclusive remedy, terminate the applicable subscriptions or services for convenience. The Company will remain fully liable for the performance of its sub-processors' obligations.

9. Data Subject Requests, Complaints, and Third Party Rights.

9.1 The Company must notify the Customer promptly if it receives a request from a Data Subject to exercise any rights the individual may have regarding their Personal Information, such as access, correction, deletion, or to opt-out of or limit certain activities like sales, disclosures, or other processing actions.

9.2 The Company must notify the Customer promptly and without undue delay if it receives any other complaint, notice, or communication that directly or indirectly relates to the Personal Information processing or to either party's compliance with the Privacy and Data Protection Requirements.

9.3 The Company will reasonably cooperate in responding to any complaint, notice, communication, or Data Subject request.

9.4 The Company must not disclose the Personal Information to any Data Subject or to a third party unless the disclosure is either at the Customer's request or instruction, permitted by this DPA, or is otherwise required by law.

10. Term and Termination.

10.1 This DPA will remain in full force and effect so long as: (a) the Terms of Service remains in effect; or (b) the Company retains any Personal Information related to the Terms of Service in its possession or control (the "Term").

10.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Terms of Service in order to protect Personal Information will remain in full force and effect.

10.3 If a change in any Privacy and Data Protection Requirement prevents a party from fulfilling all or part of its Terms of Service obligations, the parties will suspend the processing of Personal Information until the party's processing complies with the requirements. If the parties are unable to bring the Personal Information processing into compliance with applicable law within 30 days, Customer may terminate the Terms of Service.

## APPENDIX A

**Personal Information Processing Details**

**A. Data Subject Types**

Company may process Personal Information relating to the following categories of Data Subjects, as submitted or instructed by Customer:

- Customer's employees and personnel
- Customer's clients, customers, and end users
- Customer's business partners, vendors, and contractors
- Any other individuals whose information Customer uploads, stores, or processes through the Services

Company does not determine which individuals are included. All Data Subjects are determined solely by Customer.

**B. Categories of Personal Information**

Company processes the following types of Personal Information **solely on behalf of Customer** as part of providing the Services:

1. **Contact Information**
   Name, email address, phone number, organizational role, or other contact identifiers submitted by Customer.
2. **Business and Operational Records**
   Data contained in Customer-managed records within the Services, including project data, workflow data, forms, tasks, files, metadata, and any related information uploaded by Customer or its users.
3. **System-Generated Metadata**
   Technical information generated by the use of the Services, including:
   - IP address
   - Device and session information
   - Log data
   - Timestamps, usage analytics, and audit trail events

     This metadata is processed for security, delivery of the Service, diagnostics, and performance improvement only and is not used for marketing or cross-context advertising.
4. **Account Administration Information**
   User account credentials, access roles, permission settings, and user activity logs as part of account management.
5. **Support and Communications Data**
   Information provided by Customer when interacting with Company support, including messages, attachments, and diagnostic information.

**Excluded:**
Personal Information collected directly by Company from Customer in its independent role (such as Company's own marketing subscribers) is not Customer Personal Information and is processed under the Privacy Policy, not this DPA.

**C. Purpose of Processing**

Company processes Customer Personal Information **solely for the following purposes**, and only according to Customer's instructions:

- To provide, operate, host, and maintain the Services
- To secure the Services, prevent fraud, and ensure system integrity
- To provide support, troubleshooting, and incident response
- To manage user authentication, access permissions, and audit logs
- To perform analytics that improve the performance and reliability of the Service, using only aggregated or deidentified data
- To comply with applicable law or lawful requests
- Any additional purposes expressly agreed to in writing by Customer

  Company does not use Customer Personal Information for advertising, marketing, profiling, or cross-context behavioral advertising.

**D. Categories of Recipients**

Customer Personal Information may be disclosed only to:

- Authorized sub-processors listed in Appendix C
- Company employees and contractors authorized under this DPA
- Third parties as required by law
- Customer-specified recipients when Customer instructs the Service to share or export data

Company does not sell or share Customer Personal Information and does not disclose it for advertising or profiling.

**E. Duration of Processing**

Company processes Customer Personal Information:

- For the term of the Customer's subscription to the Services
- Until deletion or return of Personal Information upon termination, in accordance with the DPA
- With backups retained no longer than ninety (90) days after deletion

**Sub-processors:**

Company uses the following sub-processors to support delivery of the Services. Each sub-processor processes Customer Personal Information only to the extent necessary to provide its assigned functionality and is bound by written agreements that meet the requirements of applicable Privacy and Data Protection Requirements.

| Sub-processor | Purpose of Processing | Location | Notes |
|---|---|---|---|
| Amazon Web Services (AWS) | Hosting, storage, compute, databases, backups, search infrastructure | USA | Primary infrastructure provider; SOC 2 and ISO 27001 certified |
| GoDaddy | DNS and domain services | USA | DNS resolution only; no direct access to Customer Personal Information |
| Cloudflare | Content delivery network | USA / Global | May process IP addresses and request metadata |
| SMTP2GO | Transactional email delivery | USA / Global | Processes recipient email addresses and message metadata |
| Google | User authentication (OAuth) | Global | Identity provider; processes only identifiers required for authentication |
| Microsoft | User authentication (OAuth) | Global | Identity provider; processes only identifiers required for authentication |
| Apple | User authentication (OAuth / Sign-in with Apple) | Global | Identity provider; processes only identifiers required for authentication |
| Stripe | Payment processing (billing) | USA | Processes Customer billing details; no access to Customer-submitted platform data |
| OpenAI | AI assisted template creation, automated content creation, and features requiring machine learning | USA/Global | Processes only the data submitted for AI-assisted operations; bound by OpenAI API Data Usage Policy (no training on Customer data) |

**Countries:**
where the Company may receive, access, transfer or store Personal Information: United States of America, or any other country mutually agreed to by the parties in writing.

**Technical and Organizational Measures (TOMs)**

Company implements the following minimum technical and organizational security controls:

**1. Access Control**

- Role based access with least privilege enforcement
- Multi factor authentication for administrative access
- Unique user accounts with logged activity

**2. Data Encryption**

- TLS encryption in transit
- AES 256 encryption at rest for stored data, backups, and replicas

**3. Network and Application Security**

- Firewalls and network segmentation
- Regular vulnerability scanning
- Secure SDLC practices
- Rate limiting and automated abuse detection

**4. Logging and Monitoring**

- Centralized logging of authentication events and system operations
- Retention of logs for forensic purposes

**5. Data Backup and Recovery**

- Daily encrypted backups
- Tested disaster recovery procedures
- Backup retention not exceeding ninety (90) days

**6. Physical Security**

- Data centers with access control, surveillance, and environmental safeguards

**7. Incident Response**

- Formal incident response plan

**8. Personnel Security**

- Mandatory security awareness training
- Confidentiality obligations for all employees