Standalone Version October 21, 2026

Data Processing Agreement

This Data Processing Agreement supplements the [Master Services Agreement OR Terms and Conditions OR Tonic Pilot Services Agreement] effective [effective date of the services agreement] ("Services Agreement") between "Customer" and Tonic AI, Inc. ("Tonic" or the "Processor") (together, the "Parties").

Notwithstanding anything to the contrary, this Agreement shall only apply to the extent Processor is processing Customer Personal Data as a Processor or Service Provider, as defined under the applicable Data Protection Laws. For the avoidance of doubt, this Agreement shall not apply when Processor is Processing Customer Personal Data as a "Controller" under Data Protection Laws. This Addendum incorporates by reference all relevant terms of the Services Agreement. Any term not defined in this Agreement shall have the meaning ascribed to it in the Services Agreement.

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "Agreement" means this Data Processing Agreement and all Schedules;

1.1.2 "Customer Personal Data" means any Personal Data Processed by Processor on behalf of Customer pursuant to or in connection with the Pilot Agreement;

1.1.3 "Data Protection Laws" means, to the extent applicable to the Processor's Processing of Customer Personal Data, GDPR, UK GDPR, Swiss FDPA, US Data Protection Laws, and data protection or privacy laws of any other country;

1.1.4 "EEA" means the European Economic Area;

1.1.5 "GDPR" means EU General Data Protection Regulation 2016/679;

1.1.6 "Services" means Customer's use of services Processor provides to Customer under the Pilot Agreement.

1.1.7 "Subprocessor" means any person appointed by or on behalf of Processor to process Customer Personal Data on behalf of Customer in connection with the Services, Pilot Agreement or this Agreement.

1.1.8 "Standard Contractual Clauses" means where the GDPR applies, 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 Council ("EU SCCs"); or where the UK GDPR applies, the applicable standard data protection clauses adopted pursuant to Article 46(2)(c) or (d) of the UK GDPR; or where the Swiss FDPA applies, the applicable standard data protection clauses adopted pursuant to Article 6 of the Swiss FDPA.

1.1.9 "Swiss FDPA" means the Federal Data Protection Act of 19 June 1992 (Switzerland) (with the Ordinance to the Federal Data Protection Act of 14 June 1993), or the revised Federal Data

Protection Act of 25 September 2020 (with the Ordinance to the Federal Data Protection Act of 31 August 2022).

1.1.10 “UK GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018;

1.1.11 “US Data Protection Laws” means the California Consumer Privacy Act as amended (“CCPA”), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Utah Consumer Privacy Act, and the Connecticut Data Privacy Act, and any other similar data or privacy law in effect in the United States.

1.1.12 The terms, “Commission”, “Controller”, “Data Subject”, “Member State”, “Personal Data”, “Personal Data Breach”, “Processing” and “Supervisory Authority” shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Processing of Customer Personal Data

2.1 The subject matter, nature, purpose, type of Personal Data and categories of data subjects are described in Schedule 1, attached hereto.

2.2 To the extent the CCPA applies to the Processing of Customer Personal Data, such Customer Personal Data will be disclosed by Customer to Processor to perform the Services, and Processor will act as Customer’s “Service Provider” as such terms are defined under CCPA, with respect to such data.

2.3 The Parties agree that the specific “business purpose(s)”, as “business purpose” is defined under CCPA, of Processor’s Processing of Customer Personal Data are identified in Schedule 1. Customer is providing Customer Personal Data to Processor only for the limited and specified purposes listed in Schedule 1.

2.4 Processor:

2.4.1 shall comply with all Data Protection Laws in the Processing of Customer Personal Data;

2.4.2 shall not Process Customer Personal Data other than on Customer’s documented instructions, unless otherwise required by law, including, without limitation, as necessary for Processor to provide the Services or comply with its obligations in the Pilot Agreement and as described in Schedule 1;

2.4.3 shall immediately inform Customer if, in Processor’s opinion, an instruction from Customer related to Processing Customer Personal Data infringes any Data Protection Laws; and

2.4.4 shall provide reasonable assistance to Customer as necessary for Customer to comply with its obligations under Data Protection Laws, including as may be applicable under UK GDPR and taking into account the nature of the Processing and the information available, assisting Customer to meet its obligations to keep Personal Data secure; notifying the Information Commissioner’s Office (“ICO”) of Personal Data Breaches; notifying the data subjects of Personal Data Breaches, carrying out data protection impact assessments (“DPIA”) when required; and consulting ICO where a DPIA indicates there is a high risk that cannot be mitigated.

2.5 To the extent the CCPA applies to the Processing of Customer Personal Data, Processor:

2.5.1 shall not: (a) “sell” or “share” Customer Personal Data, as “sell” and “share” are defined under CCPA; (b) retain, use, or disclose Customer Personal Data: (i) for any purpose other than those listed in Schedule 1, unless permitted by CCPA, (ii) for a commercial or any other purpose other than for the specific purpose of providing, managing, or supporting the Services, or as otherwise permitted by the CCPA, or (iii) outside of the direct business relationship between Processor and Customer, unless expressly permitted by CCPA; or (c) combine Customer Personal Data subject to the CCPA from another Processor customer, unless permitted by CCPA;

2.5.2 shall notify Customer no later than ten business days after its determination that it can no longer meet its obligations under CCPA; and

2.5.3 hereby grants Customer the right, upon notice, to take reasonable and appropriate steps to stop and remediate any of Processor’s use of Customer Personal Data.

2.6 Controller:

2.6.1 shall comply with all Data Protection Laws;

2.6.2 agrees that it has the lawful right and authority to provide Customer Personal Data to Processor in connection with the performance of the Pilot Agreement and this Agreement; and

2.6.3 shall notify Processor of any consumer requests made pursuant to CCPA that Processor must comply with and shall provide any information necessary for Processor to so comply.

3. Processor Personnel

3.1 Processor shall take reasonable steps to: (a) ensure the reliability of any of its personnel or Subprocessor who has access to Customer Personal Data; (b) ensure in each case that access is limited to those individuals who need to know and/or access the relevant Customer Personal Data; (c) require personnel or Subprocessors to comply with Data Protection Laws in the context of that individual’s duties to Processor; and (d) ensure that all such individuals are subject to confidentiality undertakings or obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Processor shall in relation to Customer Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, to the extent applicable, the measures referred to in Article 32(1) of the GDPR and Article 32 of the UK GDPR. The security measures with regard to the Processing of Customer Personal Data undertaken by Processor at minimum include the measures identified in Schedule 2.

4.2 In assessing the appropriate level of security, Processor shall take into account the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Subprocessing

5.1 The Processor may, and Customer provides its general written authorization for Processor to, engage any Subprocessor as necessary to provide the Services under the Pilot Agreement or this Agreement.

5.2 Processor engages the Subprocessors identified in Annex III. provide a mechanism to subscribe to notifications of new Subprocessors. If Customer requires notice of any additions to the Subprocessors identified in Annex III, Customer will subscribe to such notification services. At least ten (10) days before enabling any new Subprocessor to access or participate in the processing of Customer Personal Data, Processor will notify Customer via email of such proposed Subprocessor.. To the extent legally permitted by Data Protection Laws, Customer may reasonably object in writing to Processor's appointment of a new Subprocessor in accordance with this paragraph, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution. If the parties are not able to achieve resolution, Customer, as its sole and exclusive remedy, may terminate the specific services supplied pursuant to the Pilot Agreement that rely upon and cannot be provided without the appointment of the new Subprocessor. If Customer does not object to the engagement of a third party in accordance herewith within ten (10) days of receipt of notice by Processor, that third party will be deemed an approved Subprocessor for the purposes of this Agreement.

5.3 To the extent Processor engages a Subprocessor for carrying out specific processing activities on behalf of Customer, the same obligations in this Agreement shall be imposed on Subprocessor. Where that Subprocessor fails to fulfill its data protection obligations, Processor shall remain fully liable to Customer for the performance of the Subprocessor's obligations.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, Processor shall implement appropriate technical and organizational measures, insofar as this is possible to assist Customer with its obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify Customer if it receives a request from a Data Subject or consumer under any Data Protection Law related to Customer Personal Data; and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Customer or as required by applicable laws to which the Processor is subject, in which case Processor shall to the extent permitted by applicable laws inform Customer of that legal requirement before the Subprocessor responds to the request.

7. Personal Data Breach

7.1 Processor shall notify Customer without undue delay upon Processor becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information to allow Customer to meet any obligations to report or inform Data Subjects or Supervisory Authorities of the Personal Data Breach under the Data Protection Laws.

7.2 Processor shall cooperate with Customer and take reasonable commercial steps as reasonably requested by Customer to assist in the investigation, mitigation, and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation.

8.1 Processor shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities required by Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, the Processor.

9. Deletion or return of Customer Personal Data

9.1 Upon the termination of the Services provided pursuant to the Pilot Agreement, at Customer's choice, Processor shall either delete or return to Customer all Customer Personal Data that Processor has Processed, to the extent possible, and shall delete any existing copies of Customer Personal Data unless storage of the same is required by any applicable law. Notwithstanding the foregoing digital backups made by Processor in the ordinary course of business will be securely maintained and destroyed by Processor in accordance with its standard operating procedures. All such retained Customer Personal Data shall remain subject to this Agreement during the retention period.

10. Audit rights

10.1 Processor shall make available to Customer on reasonable request information necessary to demonstrate compliance with Article 28 of GDPR, Article 28 of UK GDPR, Article 9 of Swiss FDPA and any applicable US Data Protection Law. To the extent legally required and taking into account the nature of the Processing and the information available to Processor, Processor shall allow for and contribute to audits, including inspections, by Supervising Authorities in relation to the Processing of Customer Personal Data at Customer's expense. Customer shall provide Processor with advanced notice of such audits.

11. Data Transfer

11.1 Customer authorizes Processor to transfer and process any Customer Personal Data subject to GDPR, Swiss FDPA, or UK GDPR outside of the EEA, Switzerland and the United Kingdom order to provide the Services pursuant to the Pilot Agreement, and for Processor's other legitimate interests, provided that Processor has taken appropriate measures designed to ensure the transfer and resulting processing is in compliance with Data Protection Laws.

11.2 If, in the performance of the Pilot Agreement, Customer Personal Data subject to the GDPR, Swiss FDPA, or UK GDPR is transferred to any third party located in a country outside the EEA, Switzerland and/or the UK that the applicable authorities have not recognized as providing an adequate level of protection for Customer Personal Data, then the Standard Contractual Clauses shall apply, unless an alternative transfer mechanism (e.g., Binding Corporate Rules) permitted by Data Protection Laws exists, in which case, the alternative transfer mechanism shall be documented in writing. To the extent (and where required) pursuant to the Data Protection Laws, Customer is considered a data exporter and Processor is considered a data importer.

11.3 In relation to transfers of Customer Personal Data protected by GDPR, the EU SCCs shall apply, completed as follows:

11.3.1 Module Two will apply;

11.3.2 In Clause 7, the optional docking clause will apply;

11.3.3 In Clause 9, Option 2 will apply, and the time period for prior notice of Subprocessor changes shall be set out in Section 5.2 of this Agreement;

11.3.4 In Clause 11, the optional language will not apply;

11.3.5 In Clause 17, Option 2 will apply, and the EU SCCs will be governed by Irish law;

11.3.6 In Clause 18(b), disputes shall be resolved before the courts of the Republic of Ireland;

11.3.7 Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1 to this Agreement, as applicable; and

11.3.8 Subject to Section 4 of this Agreement, Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 2 of this Agreement.

11.3.9 Annex III of the EU SCCs shall be deemed completed with the information set out in Schedule 3 of this Agreement.

11.4 In relation to transfers of Customer Personal Data protected by the UK GDPR, the EU SCCs shall apply along with the International Data Transfer Addendum ("IDTA"), completed as follows:

11.4.1 In Table 1 of the IDTA, the parties' details and key contact information are located in Annex 1(A) of Schedule 1 of this Agreement;

11.4.2 In Table 2 of the IDTA, information about the version of the Approved EU SCCs, modules and selected clauses which this UK International Data Transfer Agreement is appended to is located in Section 11.3 of this Agreement; and

11.4.3 In Table 3 of the IDTA: The list of Parties is located in Annex I(A) of Schedule 1. The description of the transfer is set forth in Annex 1(B) (Nature and Purpose of the Processing) of Schedule 1 (Description of the Processing/Transfer). Annex II is located in Schedule 2. The list of sub-processors is located in Schedule 3.

11.5 In relation to transfers of Customer Personal Data protected by the Swiss FDPA, the EU SCCs shall apply, and for the purposes of localizing the EU SCCs to Swiss law, the parties agree to the following:

11.5.1 The parties agree that the references to provisions of the GDPR in the SCCs are to be understood as references to the corresponding provisions of the Swiss Federal Data Protection Act in the version applicable at the moment of initiation of any dispute.

11.5.2 Clause 13 and Annex I(C): The competent authorities under Clause 13, and in Annex I(C), shall include the Federal Data Protection and Information Commissioner.

11.5.3 Clause 17 shall include Swiss law as the governing law in case the data transfer is exclusively subject to the Swiss FDPA.

11.5.4 The term "member state" in Clause 18 shall be extended to include Switzerland for the purpose of allowing Swiss data subjects to pursue their rights in their place of habitual residence.

SCHEDULE 1 – DESCRIPTION OF THE PROCESSING/TRANSFER

ANNEX 1(A): LIST OF PARTIES

Data exporter: Customer

Contact person's name, position and contact details:
Activities relevant to the data transferred under these Clauses: Receipt of services provided by the data importer in accordance with the Agreement.

Role (controller/processor): Controller

Data importer:

Name: Tonic AI, Inc.
Address:
548 Market St., #49486
San Francisco, CA, 94104
Contact person's name, position and contact details:
Karl Hanson, Chief Operating Officer
privacy@tonic.ai

Activities relevant to the data transferred under these Clauses: The data importer provides the Services to the data exporter in accordance with the Agreement.

Role (controller/processor): Processor

ANNEX 1(B): DESCRIPTION OF PROCESSING/TRANSFER

Categories of data subjects whose personal data is transferred

Employees, contractors, interns, staff or other individual end-users assigned permission to access the Tonic application

Categories of personal data transferred

All customers

- Directory information (given and surname, employee id/reference, job title, location, timezone, photograph)
- Grouping or categories of employees as defined and sent to the application. These categories typically are department, functional unit, or team.
- Communication/Contact Details (email address, telephone number)
- Online identifiers (advertising id – mobile only, IP Address, cookie)
- Usage data (jobs initiated, workspace settings, application usage)

Tonic Cloud (Hosted) customers

- Any data sent by the Customer to be processed by the purchased Tonic application (Tonic Structural, Tonic Textual, Tonic Fabricate, or any other product offering by Tonic AI, Inc)

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

None

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

- If enabled, continuous during use of the application.

Nature of the processing

Provisioning, maintenance, support, training and monitoring of service being provided by Tonic AI, Inc.

Purpose(s) of the data transfer and further processing

The performance of the services by Tonic AI, Inc. as set forth in the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The personal data will be retained for as long as necessary for the purpose of the processing and taking into account applicable laws.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

See Schedule 3.

ANNEX 1(C): COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

SCHEDULE 2 – TECHNICAL AND ORGANIZATIONAL MEASURES

Measures of pseudonymisation and encryption of personal data

Tonic maintains an "Encryption Policy" that defines acceptable cryptographic controls, key management, certificate management, and acceptable algorithms and key sizes. This policy is updated annually based on current industry guidance. This policy is approved by Tonic's Board of Directors and must be accepted annually by staff.

All sensitive data transferred to destinations outside of Tonic's environments must be encrypted with at least 256-bit keys.

Access to Tonic infrastructure requires use of VPN with access occurring over AES-256 encrypted tunnel. Authentication is performed at connection using Tonic's centralized identity provider.

Wi-Fi Protected Access (i.e. WPA2/WPA3) encryption is mandatory for all Tonic business wireless networks.

All corporate endpoint devices/laptops are encrypted using NIST standard encryption algorithms at the disk or volume level leveraging technologies incorporated in the operating system.

Application credentials and service accounts are encrypted and stored in centrally managed solutions.

Amazon RDS Databases are encrypted at the database level using NIST AES standard of 128-bit encryption or higher.

The Tonic application uses industry-standard hashing algorithms for all end-user passwords and only ever stores the hashed output of that computation.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Tonic possesses an SOC 2 Type II audit report, which is renewed annually by an AICPA accredited third party. This audit ensures that Tonic's internal controls align with the AICPA Trust Service Criteria and have processes in place designed to ensure confidentiality, integrity and availability of its systems for the benefit of customers.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Tonic maintains a "Disaster Recovery Plans" and a "Business Continuity Plan" that define procedures for the continued operation of vital systems and the business as a whole if there are unexpected operational or technical incidents. These plans are updated annually based on current risks and industry guidance. These plans are tested at minimum once annually.

Tonic uses Infrastructure as Code (IaC) codebooks for the construction of its networks to ensure they can be rebuilt quickly and uniformly in the event of a catastrophic incident resulting in the loss of a network.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Tonic possesses an SOC 2 Type II audit report, which is renewed annually by an AICPA accredited third party. This audit ensures that Tonic's internal controls align with the AICPA Trust Service Criteria and have processes in place designed to ensure confidentiality, integrity and availability of its systems for the benefit of customers.

Tonic performs annual external penetration tests on its application using a reputable third-party testing agency.

Tonic performs internal control and risk assessments using industry standard assessments.

Measures for user identification and authorisation

Tonic maintains a "Password Policy" and "System Access Control Policy" that define authentication and authorisation requirements for system access. These policies are updated annually based on current risks and industry guidance. These policies are approved by Tonic's Board of Directors and must be accepted annually by staff.

Centralized Identity Provider (Okta) auto provisions access for the team member with appropriate access for their role.

Tonic staff manually audit access to systems no less than annually or when there are staffing changes.

Measures for the protection of data during transmission
Tonic maintains an "Encryption Policy" that defines acceptable cryptographic controls, key management, certificate management, and acceptable algorithms and key sizes. This policy is updated annually based on current industry guidance. This policy is approved by Tonic's Board of Directors and must be accepted annually by staff.
All sensitive data transferred to destinations outside of Tonic's environments must be encrypted with at least 256-bit keys.
Access to Tonic infrastructure requires use of VPN with access occurring over AES-256 encrypted tunnel. Authentication is performed at connection using Tonic's centralized identity provider.
Wi-Fi Protected Access (i.e. WPA2/WPA3) encryption is mandatory for all Tonic business wireless networks.
Ingress traffic to Tonic networks terminates using either TLS 1.2 or SSH. For TLS, Tonic uses ciphers and algorithms defined by AWS as ELBSecurityPolicy-TLS-1-2-2017-01.

Measures for the protection of data during storage
Tonic maintains an "Encryption Policy" that defines acceptable cryptographic controls, key management, certificate management, and acceptable algorithms and key sizes. This policy is updated annually based on current industry guidance. This policy is approved by Tonic's Board of Directors and must be accepted annually by staff.
All devices and services used to support Tonic networks (instances, databases, S3, etc) are configured with industry-standard AES-256 data encryption.

Measures for ensuring physical security of locations at which personal data are processed
Customer data is housed in AWS where their physical security controls are leveraged (www.aws.amazon.com/security & www.aws.amazon.com/compliance)

Measures for ensuring events logging
All critical devices, systems, datastores, and applications have event logging enabled. Logging events must contain what occurred, who or what caused the event, when the event occurred (i.e. timestamp), and the associated system applications or data affected by the events.
Where possible, the following system, datastore, and application types of events should be logged:

- All authentication events (success and fail)
- Account or role creation, modification, or deletion
- Changes to system or application configuration
- All alerts raised by the access control system
- Administrator or operator activities

Centrally collected event logs from systems, datastores, and applications. Access to centrally collected event logs is controlled by these teams and limited to "need to know" scenarios. Centrally collected event logs are retained for a period of no less than 12 months. Tonic uses AWS Control Tower to manage its AWS accounts and aggregate logs into audit and security environments to prevent tampering.

Measures for ensuring system configuration, including default configuration
Tonic uses Infrastructure as Code (IaC) codebooks for the construction of its networks to ensure they can be rebuilt quickly and uniformly in the event of a catastrophic incident resulting in the loss of a network.
Tonic has developed system baselines and standards for production and development workloads. These baselines and standards are updated on a regular basis based on industry guidance.
Tonic uses AWS and other commercial monitoring tools, and preventive and detective controls to ensure deployed devices align with Tonic's configuration standards.

Measures for internal IT and IT security governance and management
Personal data is protected with least privilege access and handled with appropriate operational procedures. Access shall be limited to the minimum necessary to perform the assigned duties (principle of least privilege).
Tonic has developed system baselines and standards for workstations and mobile devices. These baselines and standards are updated on a regular basis based on industry guidance. These standards include (but are not limited to):

Centralized management of devices (lock, erase, push policy, push configuration)
Full disk encryption
Access to device must be authenticated
Anti-malware system is installed and operational
Password meets password policy
Secure defaults are configured
Auto-lock after timeout
Operating system is automatically updated with security patches

Tonic enforces its workstation and mobile device standards on its fleet of devices using Mobile Device Management tools (Kandji for macOS and iOS devices, Intune for Windows and Linux devices).
Wi-Fi Protected Access (i.e. WPA2/WPA3) encryption is mandatory for all Tonic business wireless networks.

Measures for certification/assurance of processes and products

Tonic possesses an SOC 2 Type II audit report, which is renewed annually by an AICPA accredited third party. This audit ensures that Tonic's internal controls align with the AICPA Trust Service Criteria and have processes in place designed to ensure confidentiality, integrity and availability of its systems for the benefit of customers.

Measures for ensuring data minimisation

Tonic possesses an SOC 2 Type II audit report, which is renewed annually by an AICPA accredited third party. This audit ensures that Tonic's internal controls align with the AICPA Trust Service Criteria and have processes in place designed to ensure confidentiality, integrity and availability of its systems for the benefit of customers.
Personal data is protected with least privilege access and handled with appropriate operational procedures.
Access shall be limited to the minimum necessary to perform the assigned duties (principle of least privilege).
The Tonic application only processes data under the direct control of the Customer. Tonic staff do not have visibility into what the application processes.

Measures for ensuring data quality

Disaster Recovery Testing is conducted annually.
Tonic's SDLC includes multiple phases of testing. This testing includes (but is not limited to):

Peer review of code changes by at least one other team member
Automated unit testing
Manual feature testing
Static code analysis and vulnerability scanning
Automated integration and end-to-end testing
Container vulnerability scanning

Tonic possesses an SOC 2 Type II audit report, which is renewed annually by an AICPA accredited third party. This audit ensures that Tonic's internal controls align with the AICPA Trust Service Criteria and have processes in place designed to ensure confidentiality, integrity and availability of its systems for the benefit of customers.

Measures for ensuring limited data retention

Tonic maintains an "Data Retention Policy" that defines the length of time data in production systems may be processed and stored. This policy is updated annually based on current industry guidance. This policy is approved by Tonic's Board of Directors and must be accepted annually by staff.
Where possible, Tonic has implemented automated mechanisms on its production systems to automatically delete data when it reaches the end of its retention period.

Measures for ensuring accountability

All critical devices, systems, datastores, and applications have event logging enabled. Logging events must contain what occurred, who or what caused the event, when the event occurred (i.e. timestamp), and the associated system applications or data affected by the events.
Where possible, the following system, datastore, and application types of events should be logged:

All authentication events (success and fail)
Account or role creation, modification, or deletion

Changes to system or application configuration
All alerts raised by the access control system
Administrator or operator activities

Centrally collected event logs from systems, datastores, and applications. Access to centrally collected event logs is controlled by these teams and limited to "need to know" scenarios. Centrally collected event logs are retained for a period of no less than 12 months. Tonic uses AWS Control Tower to manage its AWS accounts and aggregate logs into audit and security environments to prevent tampering.
Tonic has alarms on logging systems that ensure unexpected behavior is brought to the attention of staff.

Measures for allowing data portability and ensuring erasure
Erasure Requests: Tonic has implemented procedures for account deletion requests. End-users wishing to have their Personal Information should contact privacy@tonic.ai

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter
Tonic performs initial and annual due diligence activities on its sub-processors to ensure they provide an equivalent or greater level of security and data protection assurance than its own systems.

SCHEDULE 3 – LIST OF SUB-PROCESSORS

All Customers

Organization	Address	Purpose	Data Processed
Salesforce	Salesforce Tower 415 Mission St., 3rd Floor San Francisco, CA 94105 800-NO-SOFTWARE	Account management	Name, email, job title, picture of staff who interact with Tonic to manage purchase, renewal, billing and cancellation of licenses
Google	1600 Amphitheatre Parkway Mountain View, CA 94043 650-253-0000	Customer support (if used)	Name, email, job title, picture (when interacting with Tonic staff)
Zapier, Inc	548 Market St., #62411 San Francisco, CA 94104	Ephemeral data coordination	Name, email, job title
Hubspot, Inc.	25 First Street, 2nd Floor Cambridge, MA 02141	Product announcements	Name, email

Application Delivery

Organization	Address	Purpose	Data Processed
Atlassian (Jira Software, Halp, and JSM products)	350 Bush Street 13th Floor San Francisco, CA 94104 (415) 701-1110	Development	For this purpose, Atlassian does not collect any Personal Information.

AWS	410 Terry Avenue North Seattle, WA 98109	Development	For this purpose, AWS does not collect any Personal Information.
GitHub	88 Colin P Kelly Jr St. San Francisco, CA 94107 (877) 448-4820	Application development, testing and deployment	For this purpose, GitHub does not collect or process any Personal Information.
Quay.io (Red Hat, Inc.)	100 E. Davie Street Raleigh, NC 27601 (888) 733-4281	Container repository	IP addresses and technical identifiers of devices that retrieve application images

Tonic Cloud (Hosted) Customers

Tonic offers both hosted and on-prem deployments of its software. On-prem customers can deploy their software in an environment using technical and organisational measures of their choosing and optionally choose to share data with Tonic for the purposes of providing support.

Organization	Address	Purpose	Data Processed
AWS	410 Terry Avenue North Seattle, WA 98109	Application hosting	All data processed by the Tonic application as selected by the Customer. This will include any data that is chosen for processing. Personal Information about staff accessing this system, including email, name, access location (country and state), IP address, hashed passwords, language preference, device type
Microsoft Corporation	One Microsoft Way Redmond, Washington 98052-6399 (800) 285-7772	Application hosting	All data processed by the Tonic application as selected by the Customer. This will include any data that is chosen for processing. Personal Information about staff accessing this system, including email, name, access location (country and state), IP address, hashed passwords, language preference, device type

Google Cloud GCP	1600 Amphitheatre Parkway Mountain View California 94043 (650) 253-0000	Application hosting	All data processed by the Tonic application as selected by the Customer. This will include any data that is chosen for processing. Personal Information about staff accessing this system, including email, name, access location (country and state), IP address, hashed passwords, language preference, device type
Stripe	354 Oyster Point Blvd. South San Francisco CA	Credit card processing	Name, email, access location (country and state), IP address, language preference, device type
Anthropic, PBC	548 Market St., PMB 90375 San Francisco, CA 94104	Data Processing	Data processed by the Tonic application to facilitate user interaction with a subset of AI features. This includes the user's primary input as well as required contextual data sent to the Anthropic model to generate the requested output Tonic AI and Anthropic, PBC have executed an agreement that mandates Zero Data Retention (ZDR) for this data. All submitted data is utilized for temporary, session-based processing only and is not stored, retained, or used by Anthropic for any purpose—including model training, analysis, or service improvement—after the request is fulfilled.
OpenAI OpCo, LLC	1455 3rd Street, San Francisco, CA 94158	Data Processing	Data processed by the Tonic application to facilitate user interaction with a subset of AI features. This may include the user's primary input as well as required contextual data sent to the OpenAI model to generate the requested output.

Hosted customers do not have the ability to opt-out of optional sub-processors and all optional sub-processors in categories below are explicitly authorized.

Data De-identification Services

Tonic offers end-to-end de-identification services that use the subprocessors listed below, which are not used by Tonic's other products. These services may also use the subprocessors listed in the Tonic Cloud (Hosted) Customers section.

Organization	Address	Purpose	Data Processed
Databricks, Inc.	160 Spear Street, 15th Floor, San Francisco, CA 94105	Data Processing	Customer-supplied data, including structured and unstructured files of various types, ingested, stored, and processed by Tonic for transformation and de-identification workloads.
OpenRouter, Inc.	169 Madison Avenue, New York, NY 10016	Data Processing	Data processed by Tonic to provide AI-assisted de-identification and related features. This may include Customer-supplied data and required contextual data sent through OpenRouter to the selected model provider to generate the requested output.

Analytics, Performance Management, Issue Debugging

These sub-processors are optional for on-prem deployments. They are deemed authorized if Customer chooses to use them.

Organization	Address	Purpose	Data Processed
Amplitude	201 3rd Street Suite 200 San Francisco, CA 94103 (650) 988-5131	User experience and product research	Email, name, access location (country and state), IP address, language preference, device type
AWS	410 Terry Avenue North Seattle, WA 98109	Log aggregation	Log data that may include technical identifiers (IP addresses, machine identifiers, etc.) and basic Personal Information (name, email) of the user who initiated a job.
Dynatrace	1601 Trapelo Road Suite 116 Waltham, MA 02451	Application performance management, debugging	Ephemeral data related to the performance of the Tonic application. This data may include incidental Personal Data included in stack traces.

Snowflake Inc.	106 East Babcock Street Suite 3A Bozeman, Montana 59715	Analytics	Log data that may include technical identifiers (IP addresses, machine identifiers, etc). and basic Personal Information (name, email, title)
Sigma Computing, Inc.	116 New Montgomery St. #700 San Francisco, CA 94105	Analytics	Log data that may include technical identifiers (IP addresses, machine identifiers, etc). and basic Personal Information (name, email, title)

Customer Support and Account Management

These sub-processors are optional for on-prem deployments. They are deemed authorized if Customer chooses to use them.

Organization	Address	Purpose	Data Processed
Atlassian (Jira Software, Halp, and JSM products)	350 Bush Street Floor 13 San Francisco, CA 94104 (415) 701-1110	Customer support management, software project management	Name, email, job title, picture
GitHub	88 Colin P Kelly Jr St. San Francisco, CA 94107 (877) 448-4820	Application development, testing and deployment	May process incidental Personally Identifying pieces of Personal Information related to bugs reported and supporting documentation.
Google (when using email as a customer support option)	1600 Amphitheatre Parkway Mountain View CA 94043 (650) 253-0000	Customer support (if used)	Name, email, job title, picture
Intercom, Inc.	55 2nd Street, 4th Floor San Francisco, CA 94105 415-673-3820	Customer support chat-in app	Name, email, job title, picture
Microsoft (when using Microsoft Teams for chat support and/or video trainings)	One Microsoft Way Redmond, WA 98052-6399	Customer support (if used)	Name, email, job title, picture
Salesforce	Salesforce Tower 415 Mission St., 3rd Floor San Francisco, CA 94105 800-NO-SOFTWARE	Account management	Name, email, phone number, job title of staff who interact with Tonic to manage purchase, renewal, billing and cancellation of licenses.
Slack (when using Slack Connect for chat support)	500 Howard Street San Francisco, CA 415-579-9122	Customer support (if used)	Name, email, job title, picture (when using Slack as a customer support option)
Zoom, Inc. (when using Zoom for customer support or training)	55 Almaden Blvd. San Jose CA 95113	Customer support (if used)	Name, email, job title, picture, voice

Tonic will provide a mechanism for Customer to subscribe to notifications of new subcontractors. If Customer subscribes to such notification services, Tonic shall notify Customer if it adds any new subcontractor at least ten (10) days' prior to allowing such subcontractor to gain access to or to process any Personal Data of Customer. To the extent legally permitted by Data Protection Laws, Customer may reasonably object in writing (which may be via email) to Tonic's appointment of a new subcontractor in accordance with this paragraph, provided that such objection is based on reasonable grounds relating to data protection. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution. If the parties are not able to achieve resolution, Customer, as its sole and exclusive remedy, may terminate the specific services supplied pursuant to this DPA that rely upon and cannot be provided without the appointment of the new subcontractor.