DATA PROCESSING AGREEMENT

Between Customer and ticura GmbH

Effective Date: Date of full signing

Version: 1.1 (March 2026)

---

1. DEFINITIONS AND SCOPE

1.1 Key Definitions

- **"Customer"** means the entity that has entered into the Master Service Agreement with ticura.
- **"Customer Data"** means any Personal Data that ticura processes on behalf of Customer.
- **"GDPR"** means Regulation (EU) 2016/679 on the protection of personal data.
- **"Personal Data"** means any information relating to an identified or identifiable natural person.
- **"Services"** means the threat intelligence platform and related services provided by ticura.
- **"Sub-processor"** means any third party appointed by ticura to process Customer Data.

1.2 Roles and Application

Customer acts as Data Controller and ticura acts as Data Processor. This DPA applies to all processing of Customer Data and forms an integral part of the Master Service Agreement. In case of conflict, this DPA prevails on data protection matters.

---

2. PROCESSING DETAILS

2.1 Nature and Purpose

ticura processes Customer Data to provide threat intelligence analysis, security event monitoring, threat detection, incident response support, and reporting through its cloud-based platform.

2.2 Categories of Data

Data Subjects: Customer's employees, contractors, authorized users, clients, security incident victims, system administrators, and identified threat actors.

Personal Data Types:

- Identity Data: names, usernames, email addresses, job titles
- Technical Data: IP addresses, system logs, network identifiers, device information
- Security Event Data: authentication logs, access records, security alerts, incident reports

- Usage Data: platform access logs, session information
- Communication Data: support tickets, incident reports, analyst comments

2.3 Duration

Processing continues for the term of the Master Service Agreement plus thirty (30) days for data return or deletion.

---

3. PROCESSOR OBLIGATIONS

3.1 Processing Instructions

ticura shall process Customer Data only on Customer's documented instructions as set forth in this DPA and the Master Service Agreement, unless required by EU or Member State law.

3.2 Confidentiality

All ticura personnel are subject to confidentiality obligations and receive appropriate data protection training. Access to Customer Data is limited to personnel who require it to perform Services.

3.3 Security Measures

ticura implements appropriate technical and organizational measures including:

- Encryption in transit (TLS 1.2+) and at rest (AES-256)
- Role-based access control and multi-factor authentication
- Firewalls
- Regular backups with disaster recovery capabilities
- Security monitoring, logging, and incident response procedures
- Annual penetration testing and vulnerability scanning
- Cloud Service Providers with appropriate Security Measures and Certifications

ticura shall provide security documentation (certifications, audit reports) upon reasonable request.

---

4. SUB-PROCESSORS

4.1 Authorization and List

Customer authorizes ticura to engage Sub-processors, dependent of used ticura features. Current Sub-processors are listed at https://app.ticura.io/privacy #subprocessors and include:

4.2 Changes and Objection Rights

ticura shall notify Customer at least thirty (30) days before adding or replacing Sub-processors. Customer may object on reasonable data protection grounds within fourteen (14) days. If unresolved, Customer may terminate affected Services without penalty.

4.3 Sub-processor Requirements

ticura imposes equivalent data protection obligations on all Sub-processors and remains fully liable for their performance.

---

5. DATA SUBJECT RIGHTS AND BREACH NOTIFICATION

5.1 Assistance with Data Subject Requests

ticura shall assist Customer in responding to Data Subject requests (access, rectification, erasure, restriction, portability, objection) using available technical measures. Self-service tools enable Customer to directly manage most requests.

If ticura receives a Data Subject request directly, it shall notify Customer within five (5) business days and not respond except on Customer's instructions.

5.2 Personal Data Breach Notification

ticura shall notify Customer within seventy-two (72) hours of becoming aware of a Personal Data Breach affecting Customer Data, including:

- Nature of the breach and data categories affected
- Contact details for further information
- Likely consequences
- Measures taken or proposed to address the breach

ticura shall investigate, mitigate effects, provide updates, and preserve evidence. Notification does not constitute acknowledgment of liability.

---

6. INTERNATIONAL DATA TRANSFERS

6.1 Transfer Mechanism

Customer Data is processed and stored primarily in the EEA (Germany, Netherlands, Sweden). Where processing occurs outside the EEA, the EU Standard Contractual Clauses (Module Two: Controller to Processor) apply as set forth in **Annex 1**.

For the Standard Contractual Clauses:

- Customer is "data exporter"; ticura is "data importer"
- Module Two applies with general Sub-processor authorization
- Governing law: Germany; Jurisdiction: Frankfurt am Main

6.2 Supplementary Measures

ticura implements end-to-end encryption, strict access controls, audit logging, and contractual prohibitions on unlawful access. ticura shall notify Customer of government access requests where legally permitted and challenge unlawful requests.

---

7. DATA RETENTION AND DELETION

7.1 Deletion Upon Termination

Upon termination, Customer may elect (within 14 days) to:

1. Receive a copy of Customer Data in machine-readable format (within 30 days), or
2. Have ticura delete all Customer Data (within 90 days)

If no election is made, ticura shall delete Customer Data within ninety (90) days. Data required by law may be retained during the legal retention period only.

7.2 Deletion Certification

Upon request, ticura shall provide written certification of deletion.

---

8. AUDIT RIGHTS

8.1 Audit Procedures

Customer may audit ticura's compliance once per twelve (12) months with thirty (30) days' notice. Audits must not unreasonably interfere with operations and are subject to confidentiality agreements.

8.2 Alternative Documentation

In lieu of on-site audit, Customer may request:

- Third-party audit reports and certifications, if applicable
- Security controls documentation
- Completed security questionnaires

8.3 Remediation

If audit reveals non-compliance, ticura shall take prompt corrective action within a reasonable timeframe.

---

9. COMPLIANCE ASSISTANCE

9.1 DPIAs and Consultation

ticura shall provide reasonable assistance with Data Protection Impact Assessments (GDPR Article 35) and prior consultation with supervisory authorities (GDPR Article 36) relating to ticura's processing activities.

9.2 Records

ticura maintains processing records as required by GDPR Article 30(2), available to supervisory authorities upon request.

---

10. LIABILITY

10.1 Limitation

Each party's liability is subject to limitations in the Master Service Agreement, except where prohibited by Data Protection Laws.

10.2 Indemnification

- **ticura:** Indemnifies Customer against claims from ticura's breach of this DPA or Data Protection Law violations, except claims arising from Customer's instructions or violations.
- **Customer:** Indemnifies ticura against claims from Customer's instructions, violations of Data Protection Laws, or misuse of Services.

---

11. DATA PROTECTION OFFICER

ticura Data Protection Officer:
Email: privacy@ticura.io
Address: ticura GmbH, Data Protection Officer, Ludwig-Erhard-Straße 4, 34131 Germany

---

12. AMENDMENTS AND GENERAL PROVISIONS

12.1 Amendments

ticura may amend this DPA to reflect legal changes, regulatory guidance, or processing updates. Material amendments require thirty (30) days' notice. Continued Service use constitutes acceptance.

12.2 Order of Precedence

In case of conflict: (1) Standard Contractual Clauses, (2) this DPA, (3) Master Service Agreement.

12.3 Governing Law

This DPA is governed by German law. Exclusive jurisdiction: courts of Frankfurt am Main, Germany.

12.4 Survival

Sections 3.2 (Confidentiality), 5.2 (Breach Notification), 7 (Data Retention), 10 (Liability), and 12 (General Provisions) survive termination.

---

13. SIGNATURES

By entering into the Master Service Agreement, clicking "I Accept," or using the Services, Customer agrees to be bound by this DPA.

For Customer:

Name: ______________________________

Title: ______________________________

Date: ______________________________

Signature: ______________________________

For ticura GmbH:

Name: ______________________________

Title: ______________________________

Date: ______________________________

Signature: ______________________________

ANNEX 1: EU STANDARD CONTRACTUAL CLAUSES

MODULE TWO: Controller to Processor

Note: The full text of the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914) is incorporated by reference and available at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

Key Parameters for Standard Contractual Clauses

Module: Module Two (Controller to Processor)

Parties:

- **Data Exporter:** Customer (Controller)
- **Data Importer:** ticura GmbH (Processor)

Clause 7 (Docking): Accepted

Clause 9 (Sub-processors): Option 2 applies (general authorization with 30-day notification and objection rights)

Clause 11 (Optional Language): Not applicable

Clause 17 (Governing Law): Germany

Clause 18 (Jurisdiction): Courts of Frankfurt am Main, Germany

---

ANNEX I TO STANDARD CONTRACTUAL CLAUSES

A. LIST OF PARTIES

Data Exporter (Customer):

- **Name:** As specified in Master Service Agreement
- **Address:** As specified in Master Service Agreement
- **Contact:** As designated by Customer
- **Activities:** Uses ticura's threat intelligence platform for cybersecurity monitoring, threat detection, and incident response
- **Role:** Controller

Data Importer (ticura GmbH):

- **Name:** ticura GmbH
- **Address:** Ludwig-Erhard-Straße 4, 34131 Germany
- **Contact:** Data Protection Officer, privacy@ticura.io
- **Activities:** Provides cloud-based threat intelligence platform that collects, analyzes, correlates, and presents cybersecurity threat data
- **Role:** Processor

B. DESCRIPTION OF TRANSFER

Data Subjects: Customer's employees, contractors, users, clients, security incident victims, system administrators, threat actors identified in logs

Personal Data Categories: Identity data, technical data (IP addresses, logs, network identifiers), security event data, usage data, communication data

Sensitive Data: Not applicable (Services not designed for GDPR Article 9/10 data)

Frequency: Continuous during service term

Nature: Hosting, storing, analyzing, correlating, presenting threat intelligence data

Purpose: Cybersecurity threat monitoring, detection, analysis, incident response, reporting

Retention Period: Service term plus 30 days (or as required by law)

Sub-processors: Cloud infrastructure, email service, security monitoring, backup service providers (list at https://ticura.io/privacy #subprocessor)

C. COMPETENT SUPERVISORY AUTHORITY

For Customer: Data protection authority in Customer's EU Member State of establishment

For ticura GmbH: **Der Hessische Beauftragte für Datenschutz und Informationsfreiheit**, Postfach 3163, 65021 Wiesbaden, Germany (https://datenschutz.hessen.de)

ANNEX II TO STANDARD CONTRACTUAL CLAUSES

TECHNICAL AND ORGANISATIONAL MEASURES

Encryption: TLS 1.2+ (transit), AES-256 (at rest), encrypted backups

Access Control: Role-based access control, multi-factor authentication, least privilege, unique credentials, regular access reviews

Network Security: Firewalls, IDS/IPS, network segmentation, VPN for remote access, vulnerability scanning, penetration testing

Application Security: Secure SDLC, code reviews, input validation, OWASP Top 10 protection

Monitoring: Security event logging, centralized log management, SIEM integration, automated alerting

Backup & Recovery: Automated daily backups, encrypted storage, geographically separate locations, disaster recovery procedures, regular restoration testing

Physical Security: 24/7 data center security, restricted access (biometric/badge), environmental controls, secure media disposal and cloud service providers with appropriate measures and certifications (SOCII/III, ISO27001)

Organizational: Designated DPO, security policies, mandatory training, confidentiality agreements, background checks

Incident Response: Documented response plan, dedicated team, breach notification procedures

Vendor Management: Sub-processor due diligence, security assessments, contractual obligations

Testing: regular penetration testing, vulnerability scanning, control reviews

Sub-processors must implement equivalent measures including encryption, access controls, monitoring, incident response, audit rights, and compliance with data protection laws.

ANNEX III TO STANDARD CONTRACTUAL CLAUSES

LIST OF SUB-PROCESSORS

Current list maintained at: **https://ticura.io/privacy** #subprocessor

Specific Sub-processor details available upon request subject to confidentiality restrictions.

END OF DATA PROCESSING AGREEMENT

For questions regarding this DPA, contact:

ticura GmbH
Address: Ludwig-Erhard-Straße 4, 34131 Germany
Email: privacy@ticura.io
Website: https://ticura.io

Version: 1.1 | **Effective:** March 2026