Tricentis Controller to Processor
Data Processing Agreement

DATA PROCESSING AGREEMENT (DPA)

1. Background and Parties

a. This Data Processing Agreement (DPA) supplements the Tricentis General Terms of Use (Terms) accepted between Customer and Tricentis and is an Agreement between Customer and Tricentis and its affiliate group companies.

b. This DPA will be effective on the later of the effective date of the Terms, or the date both parties fully execute this contract according to Section 2 below.

c. This DPA replaces any prior Data Processing Agreements and/or former Standard Contractual Clauses according to Art 46(2)(c) of the GDPR.

d. In the event of a conflict between any provisions of this DPA and the provisions of the Tricentis General Terms of Use or other Agreement between the parties, the provisions of this DPA shall prevail.

e. Processor may be contacted regarding this agreement at

privacy@tricentis.com.
Tricentis Americas Inc.
3711 South MoPac Expressway,
Suite 400, Building 2
Austin, TX 78746

f. Controller may be contacted at

E-mail:

Name and Address:

2. Instructions and Effectiveness

a. This DPA has been pre-signed on behalf Tricentis. To enter into this DPA, Customer must

i. Have signed the Tricentis General Terms of Use

ii. Complete the signature block below

iii. Select the appropriate subprocessor list(s)

iv. Submit the completed and signed DPA to Tricentis: dpasubmissions@tricentis.com

3. Definitions

Definitions used but not defined in this DPA shall have the same meaning as set forth in the Agreement or the Data Protection Laws.

a. "**Data Protection Laws**" means any applicable law or regulation regarding the collection, use, disclosure, sharing, security, integrity, or other processing of personal data, personal information, personally identifiable information, or other similar terms, and includes the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("**GDPR**"), the GDPR as preserved in the United Kingdom following the withdrawal of the UK from European Union ("**UK GDPR**"), the Swiss Federal Data Protection laws, and all applicable legislation protecting the fundamental rights and freedoms of persons who are Data Subjects, as defined in the GDPR and UK GDPR; the California Consumer Protection Act of 2018 ("**CCPA**"), the Virginia Consumer Data Privacy Act (VCDPA), the Colorado Data Privacy Act (CDPA), the Utah Data Privacy Act (UDPA) and other US Federal and state privacy laws; the Canadian Federal Law Personal Information Protection and Electronic Documents Act ("**PIPEDA**"); and the Australian Privacy Act of 1988, as amended.

b. "**Customer Data Subjects**" means the data subjects whose personal data will be Customer Data subject to this DPA.

c. "**Processing Activities**" means processing which Tricentis undertakes with respect to the Customer Data.

d. "**Customer Content**" means any content, code or data provided by you or Users to us in connection with your use of, or resulting from your authorized use of, the Offerings.

e. "**Customer Data**" means any personal data (personally identifying information) contained in "Customer Content" according to the Tricentis General Terms of Use.

f. "**Controller**" has the same meaning as the term defined under GDPR CCDPA, CPA, UCPA and Controller also includes the term "business" as defined under CCPA. The terms "Customer" and "Controller" may be used interchangeably in this DPA.

g. "**Processor**" has the same meaning as the term defined under GDPR CCDPA, CPA, UCPA and "service provider" as defined under CCPA. The terms "Processor" and "Tricentis" may be used interchangeably in this DPA.

h. "**Subprocessor**" means any processor engaged by Tricentis to assist in providing the Offerings pursuant to the Terms where such entity processes Customer Data. Subprocessors may include Tricentis' affiliates or other third parties.

i. **"Terms"** means the contract in place between Customer and Tricentis under the Tricentis General Terms of Use.

4. Processing Activities

a. **Description of Processing Activities**

i. **Subject Matter.** The subject matter of the data processing under this DPA is described in the Product Specific description of processing provided in Exhibit A. The parties acknowledge and agree that the description of processing can be updated by Tricentis from time to time to reflect new features or functionalities comprised within the Offerings.

ii. **Duration.** The duration of the data processing under this DPA is determined by the term of the Customer's contract with Tricentis.

iii. **Purpose.** The purpose of the data processing under this DPA is the provision of the Offerings initiated by the Customer from time to time, communication with the Customer, and other business purposes.

b. **Tricentis's Obligations**

i. Tricentis will process Customer Data only on the written instructions of the Customer;

ii. Tricentis will not process Customer Data for any purpose other than as consistent with any written instructions from Customer and the purposes of the DPA. For the avoidance of doubt, Tricentis will not retain, use, or disclose the personal information for any purpose other than for the specific purpose of providing the Offerings. Tricentis shall not "sell" the Customer Data within the meaning of the CCPA or otherwise; and

iii. Tricentis will notify the Customer promptly if Tricentis receives a legally binding request for disclosure of Customer Data by a law enforcement authority unless otherwise prohibited by law

iv. Tricentis will notify the Customer if Tricentis believes an instruction from the Customer violates Data Protection Laws, unless it is legally prohibited from notifying Company on important grounds of public interest.

c. The Parties agree to limit the collection and processing of Customer Data by Tricentis to only that which is reasonably necessary for the Offerings and/or other business purposes for which the Customer Data was provided to Tricentis.

d. **Restricted Transfers:** The Controller agrees Customer Data that is subject to GDPR, or UK GDPR may be transferred outside the European Union or European Economic Area pursuant to the Standard Contractual Clauses incorporated into this DPA along with the Product Specific description of processing activities and Subprocessor list.

5. Tricentis Employees and Contractors

a. Tricentis shall ensure that all its personnel who have access to Customer Data:

i. Are bound by a duty of confidentiality

ii. Will not process Customer Data except on instructions from the Customer, unless such processing is required by applicable law; and

iii. Are trained with respect to compliance with this DPA and Data Protection Laws generally.

iv. Have undergone a background check prior to their employment.

b. Processor shall not disclose Customer Data to any of its personnel or any third party except:

i. As necessary, consistent with written instructions from the Customer, to provide the Offerings;

ii. To comply with applicable law to which it is subject; or

iii. With the Customer's prior written consent.

c. Tricentis may only subcontract the processing of Customer Data with the specific prior written consent of the Controller. Where the Customer provides such consent to subcontracting, Tricentis shall:

i. Ensure that it has a written contract in place with the relevant subcontractor which meets the requirements of Data Protection Laws and which imposes on the subcontractor the same obligations in respect of processing the Customer Data as are imposed on Tricentis under this DPA and Agreement;

ii. Remain liable to Customer for acts or omissions of the subcontractor under such contract; and

iii. Give the Customer notice prior to changing subprocessors via a message through the Tricentis SupportHub.

iv. Customers may object to any change in subprocessors by submitting an objection in writing to dpasubmissions@tricentis.com within 30 days of the notification of the change.

6. Data Security Measures

Tricentis has implemented and will maintain the technical and organizational measures as identified in the Security Annex of this DPA. In addition, Tricentis will:

i. Notify Customer in writing of any suspected Personal Data Breach (as such term or equivalent term is defined under Data Protection Laws) promptly and within 72 hours of becoming aware of a possible personal data breach.

b. Provide all reasonable assistance to the Customer regarding any Personal Data Breach, including, without limitation, all reasonable assistance in relation to any obligations the Customer may have as a result of the personal data breach to notify applicable governmental entities, regulatory authorities, and/or affected individuals as may be required by Data Protection Laws.

c. Customer acknowledges that Data Security Measures are subject to technical progress and development, and that Tricentis may update or modify the Data Security Measures from time to time, provided that the updates and modifications do not degrade or diminish the overall security of the Offerings.

7. Data Deletion and Retention

Tricentis shall delete or return Customer Data to the Controller within 30 days of the termination of the Agreement, save where it is required to retain such data for compliance with applicable law.

8. Compliance and Monitoring

a. Tricentis shall assist the Customer in complying with any obligations under the Data Protection Laws, including obligations to investigate, remediate, and provide information to applicable governmental entities, regulatory authorities, or affected individuals about personal data breaches, to carry out data privacy impact assessments, and to consult with such governmental entities and/or regulatory authorities as required by applicable Data Protection Laws.

b. Tricentis shall have in place appropriate measures to assist the Customer in complying with its obligations to respond to requests from Customer Data Subjects for exercising individual rights under Data Protection Laws. These requests are known as "Data Subject Requests."

c. Tricentis shall promptly notify the Customer of any Data Subject Requests and shall cooperate with the Customer to execute its obligations under applicable Data Protection Laws with respect to Data Subject Requests.

d. Tricentis shall provide such co-operation as necessary to enable the Customer to monitor and verify Tricentis's compliance with this DPA, the Agreement, and Data Protection Laws.

9. Termination

a. This DPA shall have the same duration as the Tricentis General Terms of Use between Customer and Tricentis.

b. Termination of the Agreement at any time, in any circumstance and for whatever reason does not exempt the Parties from the obligations and/or conditions under this DPA regarding the processing of Customer Data.

10. Standard Contractual Clauses

The Standard Contractual Clauses in Annex 2 are incorporated for any Data Subjects in the EEA.

11. Subprocessor Lists

Subprocessor lists for Tricentis products are included as Annex 1.C. You may indicate here which subprocessor lists are incorporated by reference, and delete the remainder of the subprocessor list pages from this DPA:

- ☐ Tosca
- ☐ Neoload
- ☐ QTest
- ☐ Testim
- ☐ Vera

For Controller

For Tricentis

Customer name (Required): _____

Signature (Required):_____

Name (Required):_____

Title (Optional):_____

Date (Required):_____

EU Representative (Required only where applicable):_____

Contact details:_____

Data Protection Officer (Required only where applicable):_____

Contact details:_____

TRICENTIS

Notwithstanding the signatures below of any other Tricentis affiliates, a Tricentis affiliate is not a party to this DPA unless they are a party to the General Terms of Use for the provisions of the Offerings.

Tricentis GmbH	Signature: DocuSigned by: Nathalie Hutter A15A5C38A66740E... Name: Nathalie Hütter Title: AGC & Geschäftsführer / Director Date: 15-Sep-2022
Tricentis Americas, Inc.	Signature: DocuSigned by: Amanda Borchevsky 87E05CA27061414... Name: Amanda Borchevsky Title: General Counsel and Secretary Date: 15-Sep-2022
Tricentis APAC Pty. Ltd.	Signature: DocuSigned by: 6E6A456EF5074BC... Name: David Owens Title: EVP and GM & Director Date: 15-Sep-2022
Tricentis SGP Pte. Ltd.	Signature DocuSigned by: Nathalie Hutter A15A5C38A66740E... Name: Nathalie Hütter Title: Director Date: 15-Sep-2022
Neotys SAS	Signature: DocuSigned by: Nathalie Hutter A15A5C38A66740E...

	Name: Nathalie Hütter Title: AGC & Directeur général / Director Date: 15-Sep-2022
Testim – Computerized Verifications Ltd	Signature: DocuSigned by: Amanda Borichevsky 87E05CA27061414... Name: Amanda Borichevsky Title: General Counsel & Secretary Date: 15-Sep-2022

Annex 1 Description of the Processing Activities/Transfer

Annex 1.A List of Parties

Data Exporter	**Data Importer**
Names: Customer	Name: Tricentis
Address/Email address: As provided for in the DPA, General Terms, or Order between the Customer and Tricentis	Address/Email Address: As provided for in the DPA
Contact Person's Name, position and contact details: As provided for in the DPA	Contact Person's Name, position and contact details: As provided for in the DPA
Activities relevant to the transfer: See Annex 1.B below	Activities relevant to the transfer: See Annex 1(B) below
Role: See Annex 1.B	Role: See Annex 1(B)

Annex 1.B Description of Processing by Product

Tosca On Premises and QTest on Premises	
Categories of data subjects	Customers' employees,
Categories of personal data transferred	Name, Email address, IP address, telephone number
Controller/Processor roles	Controller (Customer) to Processor (Tricentis)
Sensitive data transferred	None
Frequency of the transfer	Continuous
Nature of the Processing	Providing the Offerings, including: Support for the Offerings: • To authenticate users, and manage access control and user permissions. Training for the Offerings: • To maintain and display user profiles during training, authenticate users, and manage access control and user permissions.
Purpose of the Transfer	Providing the offerings, including: • To allow and maintain proper access controls and user permissions.
Duration of the Processing	Data will be deleted or returned within 30 days of the Termination of the Tricentis General Terms between Customer and Tricentis.

QTest SaaS	
Categories of data subjects	Customers' employees,
Categories of personal data transferred	Name, Email address, IP address, telephone number
Controller/Processor roles	Controller (Customer) to Processor (Tricentis)
Sensitive data transferred	None
Frequency of the transfer	Continuous
Nature of the Processing	Providing the Offerings, including: Support for the Offerings: • To authenticate users, and manage access control and user permissions. Training for the Offerings: • To maintain and display user profiles during training, authenticate users, and manage access control and user permissions. To provide user alerts and messages
Purpose of the Transfer	Providing the offerings, including: • To allow and maintain proper access controls and user permissions. • To communication with customer To provide

Duration of the Processing	Data will be deleted or returned within 30 days of the Termination of the Tricentis General Terms between Customer and Tricentis.

Neoload	
Categories of data subjects	Customers' employees,
Categories of personal data transferred	Name, Email address, IP address, telephone number
Controller/Processor roles	Controller (Customer) to Processor (Tricentis)
Sensitive data transferred	None
Frequency of the transfer	Continuous
Nature of the Processing	Providing the Offerings, including: Support for the Offerings: • To authenticate users, and manage access control and user permissions. Training for the Offerings: • To maintain and display user profiles during training, authenticate users, and manage access control and user permissions. To provide user alerts and messages
Purpose of the Transfer	Providing the offerings, including: • To allow and maintain proper access controls and user permissions. • To communication with customers
Duration of the Processing	Data will be deleted or returned within 30 days of the Termination of the Tricentis General Terms between Customer and Tricentis.

Testim	
Categories of data subjects	Customers' employees,
Categories of personal data transferred	Name, Email address, IP address, telephone number
Controller/Processor roles	Controller (Customer) to Processor (Tricentis)
Sensitive data transferred	None
Frequency of the transfer	Continuous
Nature of the Processing	Providing the Offerings, including: Support for the Offerings: • To authenticate users, and manage access control and user permissions. Training for the Offerings: • To maintain and display user profiles during training, authenticate users, and manage access control and user permissions. To provide user alerts and messages
Purpose of the Transfer	Providing the offerings, including: • To allow and maintain proper access controls and user permissions. • To communication with customer To provide
Duration of the Processing	Data will be deleted or returned within 30 days of the Termination of the Tricentis General Terms between Customer and Tricentis.

Vera	
Categories of data subjects	Customers' employees,
Categories of personal data transferred	Name, Email address, IP address, telephone number
Controller/Processor roles	Controller (Customer) to Processor (Tricentis)
Sensitive data transferred	None
Frequency of the transfer	Continuous
Nature of the Processing	Providing the Offerings, including: Support for the Offerings: • To authenticate users, and manage access control and user permissions. Training for the Offerings: • To maintain and display user profiles during training, authenticate users, and manage access control and user permissions. • To provide user alerts and messages
Purpose of the Transfer	Providing the offerings, including: • To allow and maintain proper access controls and user permissions. • To communication with customer To provide
Duration of the Processing	Data will be deleted or returned within 30 days of the Termination of the Tricentis General Terms between Customer and Tricentis.

Annex 1.C Subprocessor List: You may delete the pages of this Annex section for products which are not part of your agreement.

Tosca Subprocessor List, September 8, 2022				
Processor name	Purpose	Data	Product	Country/region
MS 365 Exchange	Email integrated exchange to ServiceNow	E-mail	Tosca	EU
ServiceNow	Support application for Tricentis supported SAP Partner Products	E-mail and IP address	Tosca	Netherlands
SkillJar	User training platform for Tricentis products	Name, email, phone number, address, IP address	Tosca	US

Neoload Subprocessor List, September 8, 2022:				
Processor name	Purpose	Data	Product	Country/region
MS 365 Exchange	Email integrated exchange to ServiceNow	E-mail	Neoload	EU
ServiceNow	Support application for Tricentis supported SAP Partner Products	E-mail and IP address	Neoload	Netherlands
SkillJar	User training platform for Tricentis products	Name, email, phone number, address, IP address	Neoload	US
Datadog	Data Analytics	Business E-mail	Neoload	US
GainSight	Customer Success and Support	Business contact name Business E-mail	Neoload	US
PagerDuty	Customer notifications	Business E-mail	Neoload	US

QTest Subprocessor List, September 9, 2022				
Processor name	Purpose	Data	Product	Country/region
ServiceNow	Support application for Tricentis supported SAP Partner Products	E-mail and IP address	Neoload	Netherlands
SkillJar	User training platform for Tricentis products	Name, email, phone number, address, IP address	Neoload	US
Datadog	Data Analytics	Business E-mail	Neoload	US
GainSight	Customer Success and Support	Business contact name Business E-mail	Neoload	US
PagerDuty	Customer notifications	Business E-mail	Neoload	US
AWS	Cloud service	Business e-mail, IP address	QTest	Regionalized per user selection (EU or US)
Intercom	Customer Notifications	Business e-mail, IP address	QTest	US
Mailchimp	Customer notification	Business e-mail	QTest on Demand	US
Recurly	Customer billing/license	Business e-mail	QTest	US

Testim Subprocessor List, September 8, 2022				
Processor name	Purpose	Data	Product	Country/region
MongoDBAtlas	Storing test related data	Business email address and customer test data	Testim	USA
FullStory	Recording interactions with product	Business email address	Testim	USA
Zendesk	Customer support	Business e-mail address	Testim	EU (Germany)
Intercom	Customer communication	Business e-mail address	Testim	USA
Mixpanel	Product and user behavioral analytics	Business e-mail address	Testim	USA
AWS	Cloud infrastructure	Business e-mail address	Testim	USA

Vera Subprocessor List, September 8, 2022				
Processor name	Purpose	Data	Product	Country/region
Microsoft Azure	Cloud infrastructure	Business e-mail address	Vera	Regionalized per user selection
Sendgrid	Customer communication	Business e-mail address	Vera	US
MongoDB Atlas	Database	Business e-mail address	Vera	US
GK Arenas Private Limited	Support services	Business contact information	Vera	India

Annex 2: Standard Contractual Clauses

STANDARD CONTRACTUAL CLAUSES: COTROLLER TO PROCESSOER

SECTION I

Clause 1 -Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 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 (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex 1.A (hereinafter each '**data exporter'**), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex 1.A (hereinafter each '**data importer'**)

have agreed to these standard contractual clauses (hereinafter: '**Clauses'**).

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex 1.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 -Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 - Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 - Interpretation

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 - Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 - Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex 1.B.

Clause 7 – Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex 1.A.

(b) Once it has completed the Appendix and signed Annex 1.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex 1.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

The accession of any third Party according to this Clause 7 is subject to the approval of Tricentis and the Controller. Such approval must be made in writing.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 - Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex 1.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex 3 and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex 1.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of

local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter '**personal data breach**'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures specified in Annex 3. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

If imported data includes any Sensitive Data as defined under the Data Privacy laws, the parties shall negotiate an additional Data Privacy agreement to address any specific additional contractual measures.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter '**onward transfer**') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9 - Use of sub-processors

(a) The data importer has the data exporter's general authorization for the engagement of sub-processors from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor. The data importer shall provide the data exporter with the information necessary to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([2]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10—Data Subject Rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex 3 the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11 - Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(d) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

[2] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(i) refer the dispute to the competent courts within the meaning of Clause 18.

(ii) The Parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 - Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 - Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 - Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing

access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved, and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([3]);

(iii) any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 - Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

[3] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 - Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 - Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of **AUSTRIA.**

Clause 18 - Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of **AUSTRIA** (specify Member State).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Competent supervisory authority
Austrian Data Protection Authority (Datenschutzbehörde) Barichgasse 40-42 1030, Vienna

Annex 3: SECURITY ANNEX

TECHNICAL AND ORGANIZATION MEASURES

The security-related technical and organizational measures (TOMs) provided below apply to all standard service offerings provided by Tricentis except where the customer is responsible for the security and privacy TOMs. Evidence of the security measures implemented and maintained by Tricentis may be presented in the form of up-to-date attestations, reports, or extracts from independent bodies upon request from the customer.

1. **Security Program**

Tricentis have implemented and will maintain an information security program that follows generally accepted system security principles embodied in the ISO 27001 standard designed to protect the Customer Data as appropriate to the nature and scope of the Services provided. Tricentis Security & Compliance Team maintaining the information security program includes experienced professionals holding a wide range of certifications in both security and privacy. The information security program includes at least the following elements:

a. Security Awareness and Training

Tricentis will implement and maintain an information security awareness program that is delivered to employees and appropriate contractors at the time of hire or contract commencement and annually thereafter. The awareness program will be delivered electronically and includes a testing aspect with minimum requirements to pass.

b. Policies and Procedures

Tricentis will maintain policies and procedures to support the information security program. Policies and procedures will be reviewed annually and updated as necessary.

c. Change Management

Tricentis will utilize a change management process based on industry standards to ensure that all changes to the Tricentis production environment are appropriately reviewed, tested, and approved.

d. Patching

Tricentis will maintain a documented patch management process. Patching of systems within our environment will be prioritized according to the impact on the business. Patches shall be tested in a controlled environment to verify that the system/ equipment continues to function smoothly after installing the patch. This will be done before deploying the patch in the production environment.

e. Data Protection and Backup

Tricentis will develop and maintain data protection measures through appropriate data classification, using industry-standard encryption mechanisms for data protection. Confidential data will be encrypted in transit and at rest, and acceptable encryption algorithms will be reevaluated as encryption technology changes. Tricentis will create backups of critical Customer Data according to documented backup procedures. Customer Data stored on backup media will be encrypted using industry-standard encryption mechanisms.

f. Vulnerability Scanning and Penetration Testing

Tricentis will conduct internal vulnerability scanning on a regular basis with automated scans and notifications. The scan results will be analyzed to confirm identified vulnerabilities, and remediation scheduled within a timeframe commensurate with the relative risk.

On at least an annual basis, Tricentis will conduct a vulnerability assessment and penetration testing of our hosted products by an independent qualified vendor. Issues identified during the engagement will be appropriately addressed within a reasonable time frame commensurate with the identified risk level of the issue. An executive summary can be made available to customers upon written request and will be subject to non-disclosure and confidentiality agreements.

g. Secure Development Lifecycle

Tricentis will develop and maintain industry-standard secure coding practices, including peer coding review, application vulnerability scanning, and adherence to secure coding techniques. Tricentis will use industry-standard practices to avoid the inclusion of any program, routine, subroutine, or data (including malicious software or "malware," viruses, worms, and Trojan Horses) within Tricentis products.

2. Human Resource Security

a. Employee Handbook

All Tricentis employees must read and agree to the company policies, including the Code of Conduct, Anti Bribery and Anti-Corruption Policy.

b. Acceptable Use Policy (AUP)

Our Acceptable Use Policy outlines requirements around:

- Hardware, Software, Mobile Device, e-mail, and Network use;
- Social Media; and
- Data Classification, Handling, and Ownership.

c. Non-Disclosure Agreement (NDA)

All employees and contractors must sign a Non-Disclosure Agreement or similar obligations of confidentiality prior to employment.

3. Network Security

Tricentis will implement industry-standard network security controls designed to protect Customer Data. Tricentis will implement and maintain a network-based intrusion detection system designed to alert in the event of suspicious activity. Network security measures include firewalls, remote access control via virtual private networks or remote access solutions, network segmentation, and detection of unauthorized or malicious network activity via security logging and monitoring.

4. Physical Security

Tricentis will implement physical security measures for its facilities as well as take precautions against environmental threats and power disruptions. Access to controlled areas within our facilities will be limited by job role and subject to authorized approval.

5. User Access Control

Tricentis will implement and maintain appropriate access controls and the concept of least privilege designed to ensure only authorized users have access to Customer Data.

a. Customer User Access

Customers are responsible for managing user access controls within the application. The customer defines the usernames, roles, and password characteristics (length, complexity, and expiration timeframe) for their users. The customer is entirely responsible for any failure by customer, agents, contractors, or employees (including without limitation all of the customer's users) to maintain the security of all usernames, passwords, and other account information under customer control.

b. Our User Access

Tricentis will create individual user accounts for each of our employees or contractors that have a business need to access systems within our environment. The following guidelines will be followed with regard to our user account management:

i. User accounts are requested and authorized by our management.

ii. User accounts follow the concept of least privilege.

iii. Access to the Tricentis Production environment requires multifactor authentication.

iv. Dormant or unused accounts are disabled after 90 days of non-use.

v. Session time-outs are systematically enforced.

vi. User accounts are promptly disabled upon employee termination or role transfer, eliminating a valid business need for access.

6. Business Continuity and Disaster Recovery

Tricentis will maintain business continuity and disaster recovery plans designed to ensure the continued business operation and provision of services to our customers in the event of a disruption to normal business operations.

7. Security Incident Response

Tricentis will maintain a Security Incident response program based on industry standards designed to identify and respond to suspected and actual Security Incidents involving Customer Data. The program will be reviewed, tested, and, if necessary, updated on at least an annual basis. "Security Incident" means a confirmed event resulting in unauthorized use, deletion, modification, disclosure, or access to Customer Data.

a. Notifications

In the event of a confirmed Security Incident involving the unauthorized release or disclosure of customer data or other security event requiring notification under applicable law, we will notify customers without undue delay where a breach is known or reasonably suspected to affect customer data and will reasonably cooperate so that customers can make any required notifications in connection with such an event unless we are specifically requested by law enforcement or a court order not to do so.

8. Privacy

Tricentis will develop and maintain a privacy program designed to respect and protect Customer Data under our control, and this is located at https://www.tricentis.com/legal-information/privacy-policy/.

Please see next page.

Measure	Description
Measures of pseudonymization and encryption of personal data	Transfer of personal data takes place over secure encrypted channels such as SSL/TLS, and VPN. Customer data in our hosted products are encrypted at rest using industry-standard AES-256 encryption.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Tricentis has policies, standards, and procedures in place for the management of information security systems and people, the ISMS is audited annually to ensure the controls are operating effectively. Tricentis has put in place an access control process to ensure access to customer data is restricted to employees with valid business needs subject to managerial approval. We have documented a Business Continuity Plan to ensure the availability of services we provide to our 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	A Disaster Recovery Plan is documented to ensure the ability to restore our services in the event of disruption with minimal impact on our customers. The Disaster Recovery Plan is tested at least annually and updated as necessary.
Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	Tricentis undergoes annual SOC 2 Type 2, ISO 27001, and ISO 9001 audits to test the technical and organizational controls that we have implemented within the company.
Measures for user identification and authorization	Tricentis has an access controls policy to govern the provision of access to internal systems. Access is provisioned on a need-to-know and least privilege basis. VPN is required for remote access to internal systems, and multi-factor authentication (MFA) is also implemented to provide an additional layer of authentication protection for employees' access to corporate systems.
Measures for the protection of data during transmission	Our information security policy mandates data to be encrypted in transit using industry-standard encryption mechanisms. Transfer of personal data takes place over secure encrypted channels such as SSL/TLS, and VPN.
Measures for the protection of data during storage	Customer data are hosted with industry-leading cloud hosting providers and data centers. Customer data in our hosted products are encrypted at rest using industry-standard AES-256 encryption, customer data are logically segregated so that the actions of one customer cannot compromise the data or service of other customers.
Measures for ensuring physical security of locations at which personal data are processed	Physical security controls in our offices are guided by our physical and environmental security policy which ensures robust physical security is implemented across our environments on-premises and in the cloud. This policy covers areas such as secure working areas, securing our IT equipment wherever it may be, restricting access to our buildings and offices to appropriate personnel, and monitoring physical ingress and egress points.

Measures for ensuring events logging	Tricentis has SIEM in place for logging security events, we have a dedicated security operations center team to monitor and respond to alerts. Our internal processes define how these alerts are triaged, investigated further, and escalated appropriately.
Measures for ensuring system configuration, including default configuration	Tricentis has documented IT change and configuration management standards for ensuring consistency in system configurations. Changes to configurations are documented.
Measures for internal IT and IT security governance and management	Tricentis has a dedicated security department headed by the CISO, the team oversees security governance within the organization. We have structured our policies to cover the domains included in both the ISO 27001 and ISO 9001 standards.
Measures for certification/assurance of processes and products	There are annual SOC 2, ISO 27001, and ISO 9001 certifications for some of our products.
Measures for ensuring data minimization	Data collection is restricted to only what is necessary and sufficient to provide our services to customers
Measures for ensuring data quality	Data access is restricted on a need-to-know basis, employees with access to data must possess valid business justification to access data.
Measures for ensuring limited data retention	Tricentis has a data retention policy that ensures data are not retained longer than required as mandated by legal and compliance regulations we adhere to.
Measures for ensuring accountability	Tricentis has Information Security Management System (ISMS) in place for the management of information within the company. We have a dedicated privacy officer to ensure compliance with relevant privacy regulations.
Measures for allowing data portability and ensuring erasure]	For information, please refer to our privacy policy. https://www.tricentis.com/legal-information/privacy-policy/