TolaData

TolaData GmbH

Data Processing Agreement

Related Policies	TolaData Technical and Organisational Measures (TOMs) TolaData Data Privacy Policy
Relevant legal frameworks	The European Union General Data Protection Regulation (GDPR)
Approved by	Managing Director, Vijay Bhalaki
Last updated	July 2026
Supersedes	Data Processing Agreement of September 2021 and Data Processing Agreement of February 2020. This version covers the migration period from July to December 2026 during which hosting is provided by Hetzner Online GmbH (for clients not yet migrated) or by Amazon Web Services EMEA SARL in the AWS Europe (Frankfurt) Region (for clients from their migration date). It will be superseded by a further version once the migration is complete and Hetzner is retired as a sub-processor.

Section I – Purpose and Scope

1. Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to III are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

2. Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

3. Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, 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 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

4. Hierarchy

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

5. Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

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

Section II – Obligation of the Parties

6. Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

7. Obligations of the Parties

7.1. Instructions

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. Security of processing

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (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 purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit 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 an audit, the controller may take into account relevant certifications held by the processor.

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

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. Use of sub-processors

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

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

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

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

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

7.8. International transfers

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a

transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

8. Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions.

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

- (1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
- (2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
- (3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
- (4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

9. Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant (unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

- (1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- (2) the likely consequences of the personal data breach;
- (3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

- (a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
- (b) the details of a contact point where more information concerning the personal data breach can be obtained;
- (c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

Section III – Final Provisions

10. Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

- (1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
- (2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
- (3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1(b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

ANNEX I – List of parties

Customer (Controller)

Company: _____

Address: _____

Represented by (Name, Position): _____

Place, date: _____

Signature(s): _____

Supplier (Processor)

Company: TolaData GmbH

Address: Wallstraße 15, 10179 Berlin, Germany

Represented by: Vijay Bhalaki

Position: Managing Director (Geschäftsführer)

Place, date: Berlin, _____

Signature: _____

Please sign and send the signed scan via email to info@toladata.com

ANNEX II

1. Description of the processing

Data subjects: Data subjects include the data controller's representatives and end-users including employees, contractors, collaborators, and customers of the data controller. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by the data processor. TolaData acknowledges that, depending on Customer's use of the TolaData Services, Customer may elect to include personal data from any of the following types of data subjects in the personal data at their own responsibility:

- Employees, contractors and temporary workers (current, former, prospective) of data controller;
- Data controller's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Clients (e.g., beneficiaries, customers, clients, patients, visitors, etc.) and other data subjects that are users of data controller's services;
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the data controller via TolaData.io.

Categories of data: The personal data transferred by the controller's representatives and end-users including employees, contractors, collaborators, and customers for the use of TolaData.io includes only contact information and authentication data. TolaData acknowledges that, depending on Controller's use of TolaData.io, Controller may elect to include personal data from any of the following categories in the personal data at their own responsibility:

- Basic personal data (for example place of birth, street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth), including basic personal data about family members and children;
- Authentication data (for example user name, password or PIN code, security question, audit trail);
- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
- Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);
- Pseudonymous identifiers;
- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);
- Commercial information (for example history of purchases, special offers, subscription information, payment history);
- Biometric information (for example DNA, fingerprints and iris scans);
- Location data (for example, Cell ID, geo-location network data, location by start call/end of the call, location data derived from use of wifi access points);
- Photos, video and audio;
- HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location and organizations);
- Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);
- Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);
- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;
- Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural

person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences); or

- Any other personal data identified in Article 4 of the GDPR.

Nature and purpose of the processing: Provision of services by TolaData GmbH (Processor) to the Customer (Controller) under their main contractual agreement.

Duration of the processing: The duration of the processing corresponds to the duration of the main agreement.

2. List of sub-processors for TolaData.io

The controller has authorised the use of the following sub-processor(s). During the migration period (July to December 2026), both hosting providers are engaged: Hetzner hosts client environments that have not yet been migrated; AWS hosts client environments from each client's migration date onward. Each individual client's data is processed by only one hosting provider at any given time — never both simultaneously.

Amazon Web Services EMEA SARL (from each client's migration date)

Address: 38 Avenue John F. Kennedy, L-1855 Luxembourg

Website: https://aws.amazon.com

Nature and purpose of the processing: Cloud hosting infrastructure provider for the TolaData Software. All application data is hosted and processed exclusively in the AWS Europe (Frankfurt) Region (eu-central-1), located in Germany, unless a different AWS Region is agreed in writing with the individual Customer, in which case the applicable hosting location and safeguards are set out in dedicated terms between the Parties. A Data Processing Addendum pursuant to Art. 28 GDPR, incorporating the EU Standard Contractual Clauses, is concluded between TolaData GmbH and Amazon Web Services EMEA SARL.

Hetzner Online GmbH (until each client's migration date; being phased out by December 2026)

Address: Industriestr. 25, 91710 Gunzenhausen, Germany

Website: https://www.hetzner.com

Nature and purpose of the processing: Cloud hosting infrastructure provider for the TolaData Software for clients whose environment has not yet been migrated to AWS. All application data hosted with Hetzner is stored in Germany. A Data Processing Agreement pursuant to Art. 28 GDPR is concluded between TolaData GmbH and Hetzner Online GmbH. Hetzner will be retired as a sub-processor once all clients have been migrated to AWS, expected by the end of 2026, at which point this Annex will be updated to remove the Hetzner entry.

Additional third-party service providers used for website operation, communication and customer support (which do not process data entered into the TolaData Software) are listed in the TolaData Data Privacy Policy: https://www.toladata.com/data-privacy-policy/.

ANNEX III – Technical and Organisational Measures (TOMs)

The technical and organisational measures implemented by the processor pursuant to Article 32 GDPR are set out in the document "TolaData GmbH: Technical and Organisational Measures (TOMs)", version July 2026 (Migration Period, Hetzner / AWS), which is attached to and forms an integral part of this Agreement. That document describes both hosting environments and identifies which measures apply to each client based on their migration date.

Summary of key measures (applicable to both hosting environments unless otherwise noted):

- Hosting of the TolaData application and all client application data within Germany: either at Hetzner Online GmbH data centers (for clients not yet migrated) or in the AWS Europe (Frankfurt) Region (from each client's migration date onward, unless a different AWS Region is agreed in writing with the individual Customer under dedicated terms).
- Independent certification of the hosting environments: Hetzner is certified against ISO/IEC 27001; the AWS Frankfurt Region is certified against ISO/IEC 27001, 27017 and 27018, audited under SOC 1/2/3, and holds a C5 attestation from Germany's Federal Office for Information Security (BSI).
- Replication of application data across two physically separated data centers within Germany at all times (parallel data centers at Hetzner; two Availability Zones at AWS Frankfurt), and automated daily encrypted backups.
- Encryption of data in transit (SSL/TLS) in both environments; encryption at rest (AES-256) including for backups.
- Role-based access controls, individual named accounts, least-privilege permissions and (in the AWS environment) mandatory multi-factor authentication for administrative access; logging of access and administrative activity.
- Logical isolation of the TolaData environment from other customers of the hosting provider; separation of production, testing and development environments.
- Documented incident management plan; any incident or data breach is reported immediately to management and the Data Protection Coordinator (Managing Director, Vijay Bhalaki), who reports to the relevant supervisory authority within 72 hours where required; affected customers are informed immediately.
- Data retention and deletion in line with GDPR: customer data is deleted on the client's request or at the latest two years after the customer is deactivated from the TolaData software.

The full and current TOMs document is available from TolaData upon request and at https://www.toladata.com/.