TolaData

Technical and Organisational Measures (TOMs)

Related contracts and policies	TolaData Terms of Service TolaData Privacy Policy TolaData Data Processing Agreement
Relevant legal frameworks	The European Union General Data Protection Regulation (GDPR)
Approved by	Managing Director, Vijay Bhalaki
Last updated	July 2026
Supersedes	Technical and Organisational Measures (TOMs) of April 2026 (Hetzner-only). This version covers the phased migration to AWS running from July to December 2026.
Applicability during migration	TolaData is migrating its hosting infrastructure from Hetzner Online GmbH to Amazon Web Services (AWS Europe (Frankfurt) Region, Germany) in phases between July and December 2026. Until a client's migration date (as separately notified to them), hosting is provided by Hetzner Online GmbH within Germany. From the migration date onward, hosting is provided by Amazon Web Services EMEA SARL, exclusively in the AWS Europe (Frankfurt) Region in Germany. The technical and organisational measures below apply throughout. Where a measure differs between the two hosting environments, both are described (labelled "Hetzner (pre-migration hosting)" and "AWS (post-migration hosting)"). Measures relating to TolaData's own controls are described once and apply in both environments. Where hosting in a different AWS Region has been agreed in writing with an individual client, the applicable hosting location and safeguards are set out in dedicated terms between the parties.

Data protection, security compliance and assurance and user access model

Summary: Hosting, back up and uptime

- TolaData GmbH is a German company. The TolaData application and the data input by users is hosted in Germany, either by Hetzner Online GmbH (for clients whose migration date has not yet been reached) or by Amazon Web Services EMEA SARL in the AWS Europe (Frankfurt) Region (for clients on or after their migration date). All client application data at rest remains within Germany.
- Hetzner (pre-migration): hosting is compliant with the ISO/IEC 27001 standard, as certified.
- AWS (post-migration): the Frankfurt Region is certified against ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018, audited under SOC 1/2/3, and holds a C5 attestation from Germany's Federal Office for Information Security (BSI).
- In both environments, application data is stored in parallel across two physically separated data centers within Germany, which secures non-loss of data even in case of a hazard at one data center.
- Backups are taken automatically every day and stored in encrypted form within Germany.
- For service availability, we guarantee 99% uptime of our platform.

GDPR and Data retention policy

- The client remains the owner of their data at all times and TolaData GmbH will retain (or at the client's request, delete) the data according to our Terms of Use on our website (https://www.toladata.com/terms-of-use/).
- Under GDPR we are required to delete all personal data we hold on users (names, email addresses etc.) if the client or user requests us to or else latest two years after they cease to be our client.
- This is not the same as the data the client inputs into the TolaData application; it is the client's responsibility to comply with relevant legislation and their own data policies for this data.
- For clients hosted on AWS: a Data Processing Addendum (including EU Standard Contractual Clauses where applicable) is concluded between TolaData GmbH and Amazon Web Services EMEA SARL in accordance with Art. 28 GDPR, and TolaData maintains a Transfer Impact Assessment covering the AWS engagement. Supplementary measures include encryption of data in transit and at rest and the exclusive use of the Frankfurt (Germany) Region for client application data.
- For clients hosted on Hetzner: a Data Processing Agreement in accordance with Art. 28 GDPR is concluded between TolaData GmbH and Hetzner Online GmbH; as processing takes place exclusively within Germany, no third-country transfer arises for this arrangement.
- More details are available in our Data Privacy Policy on our website (https://www.toladata.com/data-privacy-policy/).

1. Confidentiality

Physical Access Control	
Physical Security Measures	**Hetzner (pre-migration hosting):** Servers in secure locations in Germany. Physical security measures include an electronic physical entry control system with log, documented distribution of access media, comprehensive video monitoring, security door interlocking systems, written visitor policies, and high-security perimeter fencing with anti-climbing and anti-tunneling protection around the entire data center park. Hetzner's hosting is compliant with the ISO/IEC 27001 standard, as certified. **AWS (post-migration hosting):** Servers in AWS data centers in Frankfurt, Germany. Physical security measures — independently audited under SOC 2 and ISO/IEC 27001 — include controlled building perimeters with professional security staff on site 24/7, multi-factor authentication for authorized staff entering data center floors, comprehensive video surveillance and intrusion detection systems, strictly limited role-based and time-limited physical access granted on a need basis with all access logged and regularly reviewed, and no physical access for visitors or external parties to data center floors. The AWS Frankfurt Region is certified against ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018, audited under SOC 1, 2 and 3, and holds a C5 attestation (Cloud Computing Compliance Criteria Catalogue) issued under the standards of Germany's Federal Office for Information Security (BSI). TolaData has technical and organizational measures to control access to its premises and facilities, particularly to check authorization. These are: access only with key, key management (key issuance), visitors are accompanied by authorized employees, cabinets and offices are locked when not present.
Hazard Detection System	**Hetzner (pre-migration hosting):** Data centers are equipped with a site-wide early-warning fire system with a direct connection to the local fire and rescue coordination center. Dynamic fire protection measures are in place: fireproof doors separate designated fire-protection areas and close automatically on smoke detection; there is a physical gap between data center buildings; transformers, medium-voltage stations and battery rooms are isolated using

	firewalls and fireproof doors. Hetzner holds regular emergency and fire-protection training. **AWS (post-migration hosting):** Data centers are equipped with automatic fire detection and suppression systems. Smoke sensors are installed in networking, mechanical and infrastructure areas, supported by fire-suppression equipment. Buildings are constructed and operated to withstand environmental risks, with continuous monitoring of mechanical and electrical equipment.
Video Surveillance	**Hetzner (pre-migration hosting):** Continuous video monitoring of all relevant areas including perimeter fencing, access roads, entrances and exits, security airlocks, and server rooms. Footage is recorded, stored and deleted in accordance with Hetzner's GDPR-compliant deletion plan. **AWS (post-migration hosting):** Physical access points to server rooms are recorded by closed-circuit television. Surveillance data is retained and deleted in accordance with AWS's legal and compliance obligations.
Perimeter Protection	**Hetzner (pre-migration hosting):** High-security perimeter fencing with anti-climbing and anti-tunneling features. Data center staff are present on site 24/7 year-round. **AWS (post-migration hosting):** Controlled perimeters with security staff on site 24/7 year-round. Entrances are secured with intrusion detection devices that trigger alarms if doors are forced open or held open.
Key Management	**Hetzner (pre-migration hosting):** Access media (e.g. keys) are issued only to authorized employees, subcontractors and colocation customers, with full documentation for traceability. Distribution is centrally managed and regularly reviewed. **AWS (post-migration hosting):** Physical access media and credentials are issued only to authorized AWS employees and contractors with a legitimate business need, are time-limited, logged, and regularly reviewed and revoked when no longer required. TolaData provides keys only to its employees; access to the office is only available to keyholders.
Supervision of Outside Parties	**Hetzner (pre-migration hosting):** Written policies govern external visitors: registration, authorization, ID requirements, escort by Hetzner staff during the visit, and closeout procedures. Entrance to the data center is only permitted in the company of a Hetzner employee. **AWS (post-migration hosting):** AWS does not permit routine visits to its data centers. Where third-party access is exceptionally required, it must be requested and approved in advance, is limited in scope and time, and such parties are escorted and monitored by authorized AWS personnel. At the TolaData office, visitors are accompanied by authorized employees.
Electronic Access Control	
Data Processing	Formal guidelines and procedures covering the processing of data have been defined, documented and agreed between all data controllers and data processors prior to the commencement of processing activities.
Password Protection	Passwords of TolaData users for accessing the TolaData application are both hashed and salted, and not stored as plain text. At TolaData company, the policy on passwords and authorizations is based on the general provisions regarding the structure of passwords according to best

	practice (such as minimum length, and level of complexity). Furthermore, the company operates a 'clean-desk policy' when it comes to employee passwords and employees are required to use the company's password manager. **Hetzner (pre-migration hosting):** Hetzner has defined minimum requirements for customer account passwords. **AWS (post-migration hosting):** Administrative access to the AWS environment (AWS console and APIs) is protected by individual named accounts, strong password requirements and mandatory multi-factor authentication (MFA).
Encryption	Data transfer between the user and the TolaData application is encrypted using SSL/TLS. **Hetzner (pre-migration hosting):** Automated backups are encrypted. **AWS (post-migration hosting):** Data at rest in the AWS environment, including databases, storage volumes and automated backups, is encrypted using industry-standard AES-256 encryption. TolaData's engineering team accesses the application's servers and databases via encrypted Secure Shell (SSH) connections. For the production database (i.e. the database that holds data entered by clients), the access credentials are shared only with the authorised staff personnel for whom this is required. Emails are generally transmitted by TolaData via TLS, provided that the recipient's email provider supports TLS encryption. If required, emails can also be encrypted and signed using the S/MIME procedure. The IT policy of TolaData GmbH requires employees to encrypt sensitive and customer data on hard drives or external data carriers if storage is essential.
3rd Party Data Processing	The TolaData Data Privacy Policy sets out the third parties with whom the customer data is processed and for what purpose.
Internal Access Control	
Cloud Infrastructure Controls	**Hetzner (pre-migration hosting):** Routine security updates to the underlying cloud infrastructure. Employee access is based on documented roles/rights plans; authorizations are checked regularly, granted only for the required period, and every grant, change or revocation is documented in a complete and traceable manner. (Applies to the cloud infrastructure, not the servers within it.) **AWS (post-migration hosting):** Hosting on AWS follows the AWS Shared Responsibility Model: AWS is responsible for the security of the underlying cloud infrastructure (facilities, hardware, network and virtualization layer), while TolaData is responsible for security in the cloud (operating systems, application, data and access management). AWS employees gain access based on a documented approval process following least-privilege principles; access is time-limited, logged, regularly reviewed and revoked when no longer required. TolaData manages its AWS environment through AWS Identity and Access Management (IAM) with individual named accounts, role-based least-privilege permissions and mandatory MFA.
Role Based Access Controls	The TolaData software has role based access controls with users assigned different roles accessing different functionalities based on the access matrix. These users are authenticated on login based on their assigned roles. For TolaData employees, specific access control rights are allocated to each role (involved in the processing of personal data) following the need-to-know principle. A Client Data Management Policy that governs access is in place.

User Accounts and Permissions	In the TolaData Software, every client has one or more designated Org Admin users that manage invitations for new users and the deactivation of old users. For TolaData company, an access control system is in place that allows creating, approving, reviewing and deleting employees' user accounts and permissions. The use of common user accounts is avoided.
Control of Access to Data/Records	In the TolaData Software, Org Admins grant access permission to each project, and all its associated data, to users. This access can be edit access or view only. In addition, each project has one or more Project Admins who can grant access to other users to that specific project. For TolaData employees, specific access control rights have been allocated following the need-to-know principle. A Client Data Management Policy that governs access is in place.
Management of Privileged Level Accounts	For the TolaData Software, Org Admin accounts are created and controlled by the TolaData User Support team at the request of the client or by the latter on their own. Project Admin accounts are managed by the Org Admin(s). For TolaData company, privileged level accounts (including hosting-provider administrative accounts) are secured by mandatory MFA (where supported by the provider) and a password management system that consolidates all accounts in a centralized vault in a fully encrypted form.
Logging of Server Access	**Hetzner (pre-migration hosting):** Traceable access logs and change logs for customer accounts; login and administrative changes are saved and retained in accordance with Hetzner's deletion plan and the GDPR. **AWS (post-migration hosting):** Administrative access to and changes within the AWS environment are logged in a traceable manner (AWS CloudTrail); logs are retained and deleted in compliance with the GDPR. For the TolaData software infrastructure, an access log (including attempted access) is kept both on server level and database level. A defined timeout is in place for sessions. For TolaData employees, data access is logged in all systems used. Defined timeouts are required to be in place for all sessions.
Isolation Control	
Data retention and disposal	Fully compliant with GDPR. Customer data is stored during the period of their use of the software and is deleted on the client's request or latest two years after the customer is deactivated from the TolaData software or upon their request. Both hosting providers apply defined, audited processes for the secure decommissioning and destruction of storage media at end-of-lifecycle, in line with industry standards.
Environments	**Hetzner (pre-migration hosting):** Data is stored either physically (on separate storage devices) or logically (via permissions systems and virtualization) separately from other customers' data, ensuring that data remains isolated and does not get mixed with other data. **AWS (post-migration hosting):** TolaData's AWS environment is logically isolated from other AWS customers using Amazon Virtual Private Cloud (VPC), private subnets, security groups and network access controls, ensuring that TolaData's data remains isolated and does not get mixed with other customers' data. Furthermore, on our servers we maintain isolation control by separating the different environments (production, testing, development), including the use of

	different databases between the environments. Only authorised staff (where this is needed) have access to the production databases.
Pseudonymisation	
Protection of personal data	The TolaData application does not require the entering of personal data other than upon registration and login. With the Terms of Use, TolaData and the client agree that the client alone is the controller of all (personal) data that the client processes through the Software. Data entered by clients can only be accessed in the software by users as assigned by the client's organisation and permissions for the data of each project are set and managed by the client's Admin users. Ownership and legal responsibility for such data is always with the client. While TolaData cannot control (and thus be held liable) whether a client enters or uploads a file including personal information, we encourage best practices and pseudonymisation for personal data.

2. Integrity

Data Transfer Control	
Data Sharing and Transfer	**Hetzner (pre-migration hosting):** All data transferred to and from the customer interface is encrypted. A defined process for deleting data from storage drives after the contract is completed is in place. **AWS (post-migration hosting):** All data transferred to and from the customer interface is encrypted in transit using SSL/TLS. A defined process is in place for the secure deletion of data from the hosting environment upon contract completion, and AWS applies audited media-destruction procedures for decommissioned storage devices. The TolaData employees access the server and databases remotely and are required to not take local copies or use data carriers of client data. Furthermore employees are required to use only hardware and software that has been officially released by the company, not to print out any sensitive documents and not to forward information to external IT services.
Data Entry Control	
Logging	**Hetzner (pre-migration hosting):** Traceable access logs and change logs for customer accounts; login and administrative changes are saved and retained in accordance with Hetzner's deletion plan and the GDPR. **AWS (post-migration hosting):** Administrative access to and changes within the AWS environment are logged in a traceable manner (AWS CloudTrail); logs are retained and deleted in compliance with the GDPR. For the TolaData software infrastructure, an access log (including attempted access) is kept both on server level and database level. The TolaData software automatically logs additions, edits and deletions of data by the user within the software. For TolaData employees, access to data processing systems is only possible after login, no passing of passwords, a password policy is in place on how to proceed if a password becomes known, automatic logging when entering, changing and deleting data.

3. Availability and resilience

Availability Control	
Data Backup and Restore	**Hetzner (pre-migration hosting):** Application databases are run in parallel in two different data centers in Germany at any time. Data entered by clients is thus stored in two different data centers, ensuring non-loss of data even in case of a hazard at one data center. **AWS (post-migration hosting):** Application data is replicated across two physically separated Availability Zones (data centers) within the AWS Frankfurt (Germany) Region at any time. Data entered by clients is thus stored in two different data centers, ensuring non-loss of data even in case of a hazard at one Availability Zone. In both environments, automated daily database backups are taken and stored in encrypted form. These backups enable the technical team to restore at a certain image point.
Uninterruptible Power Supply	**Hetzner (pre-migration hosting):** An uninterruptible power supply (UPS) and emergency power supply system guarantee a constant, uninterrupted power supply, even during a power outage. **AWS (post-migration hosting):** Fully redundant power systems including uninterruptible power supply (UPS) units and backup generators guarantee a constant, uninterrupted power supply for critical loads. Climate-control systems maintain constant operating temperatures.
Reporting Procedures	TolaData maintains regulated procedures and processes for security patches and has a monitoring system in place for its servers.
Data Breach Incident Management	Isolation control is in place; different environments (production, testing) are run on separate instances. In case of an incident, daily backups can be restored within a few hours and a team is on standby ready to support the data restore and ensure services are reinstated swiftly. **Hetzner (pre-migration hosting):** Hetzner operates an incident response management (IRM) system to react quickly to incidents affecting the underlying infrastructure. **AWS (post-migration hosting):** AWS operates a documented incident response management program, aligned with ISO/IEC 27001 and audited under SOC 2, so that incidents affecting the underlying infrastructure are detected and addressed quickly. At TolaData, an incident management plan is in place: Preparation and response measures are documented, including a list of necessary steps and a clear assignment of roles in the event of a data breach. Any incident or data breach must be reported immediately to management and the Data Protection Coordinator (Managing Director, Vijay Bhalaki). The Data Protection Coordinator will report the incident to the relevant supervisory authority within 72 hours; affected customers or individuals will be informed immediately by TolaData.
Anti-virus	All TolaData machines have antivirus installed. Both hosting providers apply server-level malware protections and hardening measures.
Malware	The antivirus software installed on all TolaData machines protects against malware. Server-level malware protections are in place in both hosting environments.

Anti-spyware	The antivirus software installed on all TolaData machines has anti-spyware capabilities.
Intrusion detection	The TolaData software is monitored and reports are sent immediately in case of any breach or intrusion detected. **Hetzner (pre-migration hosting):** A continuously active DDoS recognition system constantly analyses traffic, recognises attacks early, and automatically filters out malicious traffic before it reaches its target. **AWS (post-migration hosting):** The AWS environment is protected by AWS Shield, a continuously active managed DDoS protection service that constantly analyses traffic, recognises attacks early, and automatically mitigates malicious traffic before it reaches its target.
Firewalls	There are firewalls in place for the network in use in the office and in the TolaData software hosting environment (including, for AWS-hosted clients, VPC security groups and network access control lists).
Vulnerability Scans	**Hetzner (pre-migration hosting):** Hetzner performs routine security updates on the underlying cloud infrastructure to identify and remove potential vulnerabilities. **AWS (post-migration hosting):** AWS performs routine security updates and vulnerability management on the underlying cloud infrastructure. TolaData applies regulated patching procedures for the operating systems and application components it manages.
Rapid Recovery	
Business Continuity / Disaster recovery	Standard procedures are in place for business continuity. This includes: technical expertise on standby at all times to investigate and resolve issues, database-level disaster recovery, replication across two data centers in Germany (both environments) and daily encrypted backups.
Systems Monitoring	The TolaData software is monitored and alerts are sent immediately in case of any kind of breach.
Testing	The data recovery process has been tested. As part of the migration to AWS, restore tests have been performed in the AWS environment.
Recoverability	**Hetzner (pre-migration hosting):** Data replicated in parallel across two different data centers in Germany at any time. **AWS (post-migration hosting):** Application data replicated across two separate Availability Zones within the AWS Frankfurt (Germany) Region at any time. Automated daily database backups are taken in both environments and stored in encrypted form, enabling the technical team to restore at a certain image point.

4. Procedures for regular testing, assessment and evaluation

Data Protection Management	
Data Protection Coordinator	TolaData has not appointed a DPO. The Managing Director, Vijay Bhalaki, has been designated as the Data Protection Coordinator. TolaData ensures that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. This includes documented, mandatory annual security and data protection refreshers for all staff members, including specific

	one-on-one training upon induction. All TolaData employees are asked to review and agree on the security policy of the organization and sign respective confidentiality and non-disclosure agreements.
Incident Response Management	
Incident Management	In case of an incident, daily backups can be restored within a few hours and a team is on standby ready to support the data restore and ensure services are reinstated swiftly. Both hosting providers operate documented incident response programs for the underlying cloud infrastructure.
Data Protection by Design and Default	
GDPR Compliance	TolaData is fully GDPR compliant and data protection is at the forefront of the decision-making process. With this in mind, data protection by design and by default are incorporated into the company's structure and into the application.
Order or Contract Control	
Order Control	TolaData takes all necessary measures to ensure that data processed on behalf of the customer are only processed in accordance with the customer's instruction: TolaData processes the customer's data only for purposes within the scope of the business relationship; all necessary contracts in accordance with GDPR are concluded. Suppliers are carefully chosen and suppliers' employees have only access to the information they need to carry out the order. Suppliers' employees are obliged to comply with the data protection principles of GDPR. Control of the execution of the contract is warranted.
Third Party Data Processing	For the TolaData Software, application data is hosted and processed either by Amazon Web Services EMEA SARL (38 Avenue John F. Kennedy, L-1855 Luxembourg) in the AWS Europe (Frankfurt) Region (eu-central-1) in Germany — from each client's migration date onward — or by Hetzner Online GmbH (Industriestr. 25, 91710 Gunzenhausen, Germany) within Germany, for clients whose migration date has not yet been reached. A Data Processing Agreement / Addendum pursuant to Art. 28 GDPR is concluded with each provider. For the AWS engagement, the AWS DPA incorporates the EU Standard Contractual Clauses; TolaData additionally maintains a Transfer Impact Assessment and applies supplementary technical measures (encryption in transit and at rest, exclusive use of the Frankfurt Region). Hetzner will be phased out as a sub-processor by the end of 2026. Where hosting in a different AWS Region has been agreed in writing with an individual client, the applicable hosting location and safeguards are set out in dedicated terms between the parties. For signing into the software via the company website as well as communication and support of customers, data is shared with a range of third-party data processors who can be found in our Data Privacy Policy: (https://www.toladata.com/data-privacy-policy/). Any third-party data processing takes place in compliance with Art. 28 GDPR, corresponding standards of the GDPR and, where applicable, the BDSG or other data protection laws and guidelines.