TolaData

TolaData GmbH
Data Processing Agreement

Related Policies	TolaData Technical Organisational Measures (TOMs)
Relevant legal frameworks	The European Union General Data Protection Regulation (GDPR)
Approved by	CEO, Jo Bennett
Last updated	September 2021

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 months 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 of 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.

TolaData

ANNEX I

List of parties

Customer (Controller)

Company: _____

Address: _____

_____

Represented by

Name(s): _____ _____

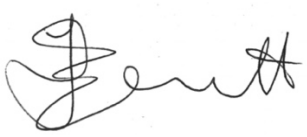
Position(s): _____ _____

Place, date _____ _____

Signature(s) _____ _____

Supplier (Processor)

Company:	TolaData GmbH	
Address:	Ringbahnstraße 32-34	
	12099 Berlin (Germany)	
Represented by		
Names:	Jo Bennett	Linda Kleemann
Positions:	CEO (Geschäftsführerin)	CEO (Geschäftsführerin)
Place, date	Berlin , 28th September 2021	



Digital unterschrieben von Kleemann, Linda
Datum: 2021.09.28 13:13:14 +02'00'

Signatures _____ _____

Please sign and send 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 the 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):

Noris network: Thomas-Mann-Straße 16-20, 90471 Nuremberg, Germany;

Website: https://www.noris.de/

Nature and purpose of the processing: Hosting Provider of TolaData GmbH.

TolaData

ANNEX III

Technical and Organisational Measures (TOMs)

Related contracts and policies	TolaData Terms of Service TolaData Privacy Policy TolaData IT Agreement
Relevant legal frameworks	The European Union General Data Protection Regulation (GDPR)
Approved by	CEO, Jo Bennett
Last updated	March 2021

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 with the German company noris network AG ("the Hosting Provider") within Germany and complies with all EU regulations for data security. This hosting is compliant with ISO 20000-1, ISO/IEC 27001 and ISO 9001 standards.
- The application data is stored in parallel in two different data centers in Germany at any time, which secures uninterrupted availability of data even in case of hazards at one data center.
- Furthermore, historic backups are taken automatically every day.
- 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 last 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.
- 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	The Hosting Provider has servers in secure locations in Germany that have access control limited to authorized personnel. Physical access is controlled according to ISO/IEC 27001 A.11. No public physical access to the data centres is granted. Only parties responsible for the systems have access to the systems. Key authorizations are limited to a minimal group of authorized individuals. All relevant doors are equipped with access control systems; other authorized parties must use access cards or input of a system code. Physical access to the data centres via access cards is logged and is archived by the data centre's director of operations. Regular access is limited with regards to time to the regular business hours of the hosting provider. Outside of business hours, a four-eyes principle is required to gain physical access to the data Centres. 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, cleaning personnel are carefully selected.
Hazard Detection System	Data centers are fitted with hazard detection systems for fire and alarm detection. Multiple silent alarm detection lines as well as smoke detectors are connected to the Hosting Provider's monitoring system and its 24-hour on-call service. The system automatically passes on fire alarms to the respective fire department via the fire alarm control panel.
Video Surveillance	Data centers are monitored by video surveillance at their respective double door security areas and at all relevant doors leading from one zone to another.
Perimeter Protection	Data centers are monitored by security staff.
Key Management	Access rights of employees of the data centers are managed by the human resource department of the Hosting Provider. TolaData provides keys only to its employees; access to the office is only available to keyholders.

Supervision of Outside Parties	No unauthorised personnel have access to the data centers however, in the case when external service providers are needed, relevant security provisions apply. At the TolaData office, visitors are accompanied by authorized employees.
Closed windows and doors	The data centers are windowless and doors close automatically. At the TolaData office, windows and doors are locked when not present.
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	The policy on passwords and authorizations at the data centers 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 Hosting Provider operates a 'clean-desk policy' when it comes to employee passwords. 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.
Encryption	Data transfer between the user and the TolaData application is encrypted using SSL. TolaData's engineering team accesses the application's databases via an encrypted Secure Shell (SSH) connection. 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. Automated backups taken by the Hosting Provider are encrypted. 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 with and for what purpose.
Internal Access Control	
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. An access control policy has been detailed and documented.
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 has been applied that allows creating, approving, reviewing and deleting employee's 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. An access control policy has been detailed and documented.
Management of Privileged Level Accounts	Org Admin accounts are created and controlled by the TolaData User Support team at the request of the client. Project Admin accounts are managed by the Org Admin(s). For the TolaData company, privileged level accounts are secured by an assigned Org admin and a password management system that consolidates all accounts in a centralized vault in a fully encrypted form.

Logging of Server Access	For the TolaData software, in terms of access to the server, the data access log (including attempted access) is conducted in the system log. 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 clients request or latest two years after the customer is deactivated from TolaData software or upon their request.
Environments	There is isolation control where the different environments (production, testing, development) in the Hosting Provider are separated, 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 customer agree that customer alone is the controller of all (personal) data that customer 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 and can provide advice and recommendations in regards to managing personal data based on the specific data, tracking and reporting requirements of each client or project.

2. Integrity

Data Transfer Control

Data Sharing and Transfer	Data transfer is done remotely and there is a log of all personnel who access it from our Hosting Provider. In addition, data is encrypted enroute in order to avoid a breach during sharing/transfer. 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	In the Data Centers, all measures are taken to ensure that it can be subsequently verified and established whether and by whom data has been entered, modified or removed in the data processing system (including automatic access login, password policy, analysis of log files for specific events.) Same applies to the TolaData software which automatically logs additions, edits and deletions of data by the user. Same applies to TolaData employees: access to data processing systems is only possible after login, no passing of passwords, 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	The application databases are run in parallel in two different data centers in Germany at any time (redundancy concept). Data entered by clients is thus stored in two different data centers. Accordingly, even in case of a hazard at one data center, the data is not affected but would continue to be served from the other data center, without interruption. Furthermore, as an additional security measure, our Hosting Provider takes automated daily database backups and stores them in encrypted form. These backups enable the technical team to restore at a certain image point.
Uninterruptible Power Supply	Our Hosting Provider's data centers abide by the 24/7 principle of the power supply for sustainable protection from failure. Redundant climate chambers

	(secured via UPS and diesel generators) ensure that no system failures occur even in case of malfunctions.
Reporting Procedures	Our Hosting Provider maintains regulated procedures and processes for security patches ("patch days") and reported vulnerabilities, and additionally arranges escalations in case of system-relevant security reports from the respective CERT.
Data Breach Incident Management	The Hosting Provider provides isolation control, different environments (production, testing) are run on separate instances with redundancy. 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. The Hosting Provider as well as TolaData company have defined and documented incident response plans with detailed procedures, including a list of possible mitigation actions and clear assignment of roles. Any incident or data breach must be reported immediately to management and the Data Protection Officer. The Data Protection Officer will report the incident to the relevant supervisory authority within 72 hours; affected customers or individuals will be informed immediately by 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.
Anti-virus	All TolaData machines have antivirus installed. Our Hosting Provider also uses antivirus software to ensure that the TolaData application is not compromised where it is hosted.
Malware	The antivirus software installed on all machines protects against malware. Our Hosting Provider also has antivirus software installed to ensure that the software is not compromised with malware.
Anti-spyware	The antivirus software installed on all machines has anti-spyware capabilities. Our Hosting Provider also uses antivirus software that has anti-spyware capabilities.
Intrusion detection	The TolaData software is monitored and there are reports sent immediately in case of any breach or intrusion detected. Our Hosting Provider also has intrusion detection systems in place.

Firewalls	There are firewalls in place for the network in use in the office and in the TolaData software hosting.
Vulnerability Scans	There are automatic antivirus scans on workstations.
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, a disaster recovery on the database level of the application and daily backups. Our Hosting Provider has a disaster recovery plan that is activated in the event of an incident. This includes snapshots for VM products, database backups and archive logs.
Systems Monitoring	The TolaData software is monitored and alerts are sent immediately in case of any kind of breach.
Testing	The recovery process has been tested between our Hosting Provider and the TolaData technical team.
Wireless Networking	There is wireless access in the TolaData offices that have SSIDs and passwords that are changed regularly.
Recoverability	At the data center of our Hosting Provider all systems can be restored via redundant systems, in a highly accessible and geo redundant manner. Comprehensive monitoring (e.g. incident response management according to ISO/IEC 27001 A.16) makes it possible to react to potential failures before they arise.

4. Procedures for regular testing, assessment and evaluation

Data Protection Management	
Data Protection Officer	TolaData has appointed a Data Protection Officer : Susanne Eggers, GFA Consulting Group GmbH, Eulenkrugstraße 82, 22359 Hamburg, Germany. email: susanne.eggers@gfa-group.de, telephone: +49 (40) 60306-105 TolaData ensures that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. This includes structured and regular training programmes for staff, including specific programmes for the induction (to data protection matters) of newcomers.

	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. Furthermore, our Hosting Provider performs incident response management according to ISO/IEC 27001 A.16
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, data is only processed by the German hosting provider noris network AG. 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.