General Terms and Conditions of Use Data Protection AND for order processing in accordance with Art. 28 GDPR of the

This document has been translated, in case of ambiguity the German version is binding!

tecRacer Germany GmbH
Vahrenwalder Straße 156
DE-30165 Hanover

and

tecRacer Switzerland GmbH
(CHE 291.618.844)
Canton of Zurich
Schaffhauserstrasse 429
CH-8050 Zurich

– hereinafter referred to as the contractor –

Subject of the AND

The subject of this AND is the written agreement of data protection matters with the contractor. It applies to all activities that are related to the individual customer contract ("**Main Contract**") and in which employees of the Contractor or persons commissioned by the Contractor process personal data ("**Data**") of the Client ("**Order Processing**").

The detailed processing agreements are defined by the individual customer contract (**main contract**).

This AND applies to the processing of personal data in accordance with the European Union's General Data Protection Regulation (GDPR) and the Swiss Data Protection Act (FADP).

Subject-matter, duration and specification of order processing

1. The subject matter and duration of the contract result from the main contract. The term of this AND shall be based on the term of the contract, unless any additional obligations arise from the provisions of this AND.

2. The **Kind** of the data processed in the context of data processing result from the scope of the individual processing carried out by the customer. (Appendix 1)

3. **Kind** and **Purpose** of the processing result from the scope of the customer's individual processing. (Appendix 1)

4. The **Affected group** of the processing results from the scope of the customer's individual processing. (Appendix 2)

5. The provision of the contractually agreed data processing takes place exclusively in the **Territory of the Federal Republic of Germany**, in a **Member State of the European Union** or in a **Contracting** of the Agreement on the European Economic Area. Any **Relocation to a third country requires the consent of the client** and may only take place if the special requirements of Art. 44 et seq. GDPR are met.

Scope and Responsibility

The Contractor processes personal data on behalf of the Client. This includes activities that are specified in the main contract. Within the framework of this contract, the Client is solely responsible for compliance with the legal provisions of the data protection laws, in particular for the lawfulness of the data transfer to the Contractor and for the lawfulness of the data processing ("Controller" within the meaning of Art. 4 No. 7 GDPR).

Commitment to confidentiality

1. The Contractor confirms that it is aware of the relevant data protection regulations. It undertakes to ensure that the principles of lawfulness, fairness and transparency are complied with in the processing of the Client's personal data in accordance with the contract. He also undertakes to observe the same rules on the protection of secrets as those incumbent on the Client.

2. The Contractor assures that it will strictly maintain confidentiality during processing and has committed the employees employed in the data processing in accordance with the order to confidentiality in writing and has familiarised them with the data protection regulations applicable to them. The Contractor shall monitor compliance with data protection regulations.

3. The duty of confidentiality/secrecy continues even after the end of the assignment.

4. The Contractor undertakes to maintain secrecy about non-generally known, commercially relevant and significant matters of the Client (trade secrets).

5. The Client undertakes to treat confidentially all knowledge of the Contractor's trade secrets and data secrets acquired in the course of the contractual relationship.

Obligations of the Client

1. The client is solely responsible for assessing the permissibility of data processing/collection/use as well as for safeguarding the rights of the data subjects.

2. The Client shall place all orders or partial orders in writing. Changes to the object of processing and changes to the process must be jointly agreed upon and contractually recorded

3. The Client shall inform the Contractor immediately and in full if it discovers errors or irregularities in the results of the contract with regard to data protection regulations.

4. The Client is obliged to treat confidentially all knowledge of the Contractor's trade secrets and data security measures acquired in the context of the contractual relationship.

5. The Client shall designate to the Contractor

a. the contact person for data protection issues arising within the framework of the contract,
b. the persons authorised to issue instructions, and
c. the extent to which these persons are authorised to issue instructions under b).

Technical and organisational measures

1. The Contractor must document the implementation of the necessary technical and organisational measures before the start of processing, in particular with regard to the specific execution of the order, and hand them over to the Client for review. If accepted by the client, the documented measures become the basis of the order. If the examination or an audit by the client reveals a need for adjustment, this must be implemented by mutual agreement.

2. The Contractor must ensure the security of processing in accordance with Articles 28 (3) (c) and 32 GDPR, in particular in conjunction with the principles in accordance with Article 5 (1) and (2) GDPR. Overall, the applicable technical and organizational measures are data security measures and to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. In doing so, the state of the art, the implementation costs and the type, scope and purposes of the processing as well as the different probability of occurrence and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32 (1) GDPR must be taken into account [details in Annex 3]. For this purpose, the Contractor shall provide the Client with a corresponding data security concept as an attachment.

3. The technical and organizational measures are subject to technical progress and further development. In this respect, the contractor is permitted to use alternative adequate measures. The safety level of the defined measures must not be undercut. Significant changes must be documented.

4. The Contractor must carry out a review, evaluation and evaluation of the effectiveness of the technical and organisational measures to ensure the security of the processing if necessary, but at least annually (Art. 32 para. 1 lit. d GDPR).

Obligations of the Contractor

1. The Contractor shall process personal data exclusively within the framework of the agreements concluded and in accordance with the instructions of the Client, unless there is an exceptional case within the meaning of Article 28 (3) (a) GDPR. The Contractor shall inform the Client without delay if it is of the opinion that an instruction violates applicable laws. The Contractor may suspend the implementation of the instruction until it has been confirmed or amended by the Client.

2. The instructions are initially set out in an annex to the main contract and can then be amended, supplemented or replaced by individual instructions (individual instructions) by the Client in written form or in an electronic format (text form) to the body designated by the Contractor (Annex 3). Instructions that are not provided for in the main contract are treated as an application for a change of performance. Oral instructions must be confirmed immediately in writing or in text form.

3. The Contractor shall correct, delete and block personal data if the Client so requests in the agreement or instruction made.

4. The Contractor shall not use the data provided for data processing for any other purpose. Copies or duplicates will not be made without the knowledge of the client.

5. In its area of responsibility, the Contractor will design the internal organisation in such a way that it meets the special requirements of data protection.

   a. The Contractor shall take technical and organisational measures to ensure the confidentiality, integrity, availability and resilience of the systems and services in connection with the processing in the long term.
   b. The Contractor shall keep a record of all categories of processing activities pursuant to Art. 30 (2) GDPR that it carries out on behalf of a controller.
   c. The Client is aware of these technical and organisational measures and is responsible for ensuring that they provide an appropriate level of protection for the risks of the data to be processed.

The Contractor reserves the right to change, further develop or adapt the safety measures taken to technical progress, but it must be ensured that the contractually agreed level of protection is not undercut. Significant changes are documented and the documentation is made available to the client without being asked.

6. If the security measures taken by the Contractor no longer meet the Client's requirements, the Client shall notify the Client immediately. The same shall apply to disruptions, violations by the Contractor or the persons employed by the Contractor against data protection regulations or the stipulations made on behalf of the Contractor,

as well as in the event of suspicion of data protection violations or irregularities in the processing of personal data.

7. The Contractor shall not use the data provided by the Client for any purpose other than that specified in the Service Contract or this AND. Copies or duplicates will not be made without the knowledge of the client.

8. The data carriers provided by the Client or used for the Client are specially marked and are subject to ongoing automated management. Entrance and exit are documented.

9. The Contractor shall, insofar as agreed, support the Client within the scope of its possibilities in fulfilling the enquiries and claims of data subjects in accordance with Chapter III of the GDPR and in complying with the obligations specified in Articles 32 to 36 of the GDPR. For support services that are not included in the main contract or are due to misconduct on the part of the contractor, the contractor may demand remuneration.

10. The Contractor warrants that the employees involved in the processing of the Client's data and other persons working for the Contractor are prohibited from processing the data outside of the instructions. Furthermore, the Contractor guarantees that the persons authorised to process the personal data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality. The duty of confidentiality/secrecy continues even after the end of the assignment.

11. The Contractor shall inform the Client without undue delay if it becomes aware of any breach of the Client's personal data protection. The Contractor shall take the necessary measures to secure the data and to mitigate possible adverse consequences for the data subjects and shall immediately consult with the Client in this regard.

12. Inspection and maintenance work of mobile workstations is permitted under the following additional conditions:

The contractor's employee will carry them out from suitable locations. The aspects of IT security (TOMs Appendix 1) must always be taken into account.

Data protection officer of the contractor

The contact person for data protection questions arising within the scope of the contract is

Mr. Stephan Riepe
NoRisk Datasecurity GmbH
as an external data protection officer
Am Windhügel 17A

DE-59457 Werl
Phone: +49 (0) 2922 / 80 33 70 7
Fax: +49 (0) 321 / 29 22 29 00
E-mail: datenschutz@norisk-datasecurity.com
Internet: http://norisk-datasecurity.com/

A change in the data protection officer will be notified to the client immediately.

Data Protection Coordination Office:
Franziska Höpfner, datenschutz@tecracer.de

Data Subject Requests

1. If a data subject contacts the Contractor with demands for correction, deletion or information, the Contractor will refer the data subject to the Client, provided that an assignment to the Client is possible according to the data subject's information. The Contractor shall forward the application of the data subject to the Client without delay. The Contractor shall support the Client within the scope of its possibilities on instructions to the extent agreed. The Contractor shall not be liable if the request of the data subject is not answered by the Client, or if it is not answered correctly or in due time.

2. In the event of a claim against the Client by a data subject with regard to any claims under Art. 82 GDPR, the Contractor undertakes to support the Client in defending against the claim within the scope of its possibilities. For support services that are not included in the main contract or are due to misconduct on the part of the contractor, the contractor may demand remuneration.

3. In the event of a claim against the Contractor by a data subject with regard to any claims under Art. 82 GDPR, No. 2 shall apply mutatis mutandis.

Proof of obligations

1. Upon request, the Contractor shall prove to the Client that it has complied with the obligations laid down in this contract, in particular the technical and organisational means pursuant to § 3 (2) of this contract, by appropriate means. Proof of the implementation of the technical and organisational measures can be provided by
   a. Data protection certificate (issued by the data protection officer)
   b. Current reports of the Data Protection Commissioner

2. Should inspections by the client or an inspector commissioned by the client be necessary in individual cases, these will be carried out during normal business hours without disruption to the operational process after notification and taking into account a reasonable lead time of at least 4 weeks. The Contractor may make this subject to prior notification with reasonable notice and to the signing of a confidentiality agreement with regard to the data of other customers and the technical and organisational measures put in place.

3. If the auditor commissioned by the client is in a competitive relationship with the contractor, the contractor has a right of objection against the contractor.

4. The contractor may demand remuneration for assistance in carrying out an inspection that is not included in the main contract.

5. The cost of an inspection is generally limited to one day per calendar year for the contractor.

6. If a data protection supervisory authority or another sovereign supervisory authority of the client carries out an inspection, paragraph 2 shall apply mutatis mutandis. It is not necessary to sign a confidentiality agreement if this supervisory authority is subject to professional or statutory secrecy, in which a violation is punishable under the Criminal Code.

Subcontractors (other processors)

1. The contractually agreed services or the partial services described below are carried out with the involvement of the subcontractors listed in Appendix 4.

2. The Contractor shall inform the Client of any intended changes with regard to the involvement or replacement of further Processors. In individual cases, the client has the right to object to the commissioning of a potential additional processor. An objection may only be raised by the Client for important reasons that must be proven to the Contractor. If the Client does not object within 14 days of receipt of the notification, its right of objection with regard to the corresponding assignment expires.

3. The Contractor is obliged to carefully select subcontractors according to their suitability and reliability. When engaging subcontractors, the Contractor shall oblige them in accordance with the provisions of this Agreement and shall ensure that the Client can exercise its rights under this Agreement (in particular its rights of inspection and control) directly vis-à-vis the subcontractors. If subcontractors are to be involved in a third

country, the contractor must ensure that an adequate level of data protection is guaranteed by the respective subcontractor (e.g. by concluding an agreement based on the EU standard data protection clauses). Upon request, the Contractor shall provide the Client with proof of the conclusion of the aforementioned agreements with its subcontractors.

4. A subcontractor relationship within the meaning of these provisions does not exist if the contractor commissions third parties with services that are to be regarded as purely ancillary services. These include, for example, postal, transport and shipping services, cleaning services, telecommunications services with no specific reference to services provided by the contractor for the client and security services. Maintenance and testing services constitute subcontractor relationships requiring approval insofar as they are provided for IT systems that are also used in connection with the provision of services for the Client.

Rectification, deletion, blocking and return of personal data

1. The Contractor shall correct, delete or block the data subject to the contract if instructed by the Client and this is covered by the framework of instructions, and shall keep a record of the deletion or correction.

2. If deletion in compliance with data protection regulations or a corresponding restriction of data processing is not possible,
a. the Contractor undertakes the destruction of data carriers and other materials in accordance with data protection regulations on the basis of an individual order by the Client, or
b. returns these data carriers to the Client, unless already agreed in the contract.

3. If the Contractor incurs costs due to the destruction of data carriers and other materials in compliance with data protection regulations for which the Contractor is not responsible, he may demand remuneration.

4. In special cases to be determined by the client, storage or handover will take place. Remuneration and protective measures for this purpose must be agreed separately, unless already agreed in the contract.

5. After the end of the order, all data, data carriers and all other materials, including processing and usage results, are to be either surrendered or physically deleted at the request of the Client. In the case of test and scrap materials, individual commissioning is not required. If additional costs arise due to deviating specifications in the release or

deletion of the data, these shall be borne by the Client. The deletion or destruction must be documented.

Liability and damages

The client and contractor are liable to data subjects in accordance with the regulation made in Art. 82 GDPR.

Information obligations, written form clause, right of retention, choice of law

1. If the Client's data at the Contractor is endangered by attachment or seizure, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor shall inform the Client thereof immediately. The Contractor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lies exclusively with the Client as the "controller" within the meaning of the General Data Protection Regulation.
1. For ancillary agreements, the written form is required.
2. The objection of the right of retention within the meaning of Section 273 of the German Civil Code (BGB) is excluded with regard to the processed data and the associated data carriers.
3. In the event of any contradictions, the provisions of this Annex on data protection shall take precedence over the provisions of the contract. If individual parts of this system are invalid, this does not affect the validity of the rest of the system.
4. German law applies.

Status of the AND: 01.02.2025

APPENDIX 1 – Type of data, type and purpose of data processing

Type of data	Type and purpose of data processing
• Personal master data of the client's contact persons • Communication data (e.g. telephone, e-mail) with the client's contact persons • Contract master data (contractual relationship, product or contractual interest) of the customer • Customer history of the client • Client's contract, billing and payment data • Planning and control data for the projects with the client • Access data for deliveries, source code storage	Collection and processing of personal data for the purpose of processing contracts for work and services
• Personal master data of the client's contact persons • Communication data (e.g. telephone, e-mail) with the client's contact persons • Contract master data (contractual relationship, product or contractual interest) of the customer • Customer history of the client • Client's contract, billing and payment data • Planning and control data for the projects with the client • Access data for deliveries	Collection and processing of personal data for the provision of standard software
• Personal master data of the client's contact persons	Collection and processing of personal data for the purpose of conducting public training and company training courses.

• Communication data (e.g. telephone, e-mail) with the client's contact persons • Contract master data (contractual relationship, product or contractual interest) of the customer • Customer history of the client • Client's contract, billing and payment data • Planning and control data for the projects with the client • Personal master data of the training participants: name, address, date of birth • Contact details of the training participants (e-mail, telephone number). • Professional data of the trainees: employer, position, department, professional qualifications. • Training participant participation data: Information about participation in training courses, such as registration data, attendance lists, certificates. • Student performance data: results of tests or assessments, feedback and comments. • Participant communication data: emails, chat logs, or other forms of communication related to the training.	

ANNEX 2 - Categories of data subjects

Categories of data subjects
• Employees of the client
• Client's customers
• Interested parties of the client
• Subscribers of the Client
• Employees of the client
• Suppliers and service providers of the client
• Commercial agent of the client

Appendix 3: Description of the technical and organizational measures – data backup measures (TOM)

The technical and organisational measures to ensure data protection and data security are set out below, which the Contractor must at least set up and maintain on an ongoing basis. The aim is to guarantee in particular the confidentiality, integrity, resilience and availability of the information processed on behalf of the company.

Access

Hanover location:

Visitor logging: Visitors are logged and provided with visitor badges. There is a guideline for accompanying and marking guests in the office buildings.

Chip cards: transponder locking system The floor rooms in the building are accessible with a chip card, which are personalised and centrally managed. Only employees and permanent visitors have a chip card that can be used for an unlimited period of time and space. Floor doors have an automatic door closer.

Locking system: Use of a locking system Access to the building is possible during business hours. Outside business hours, the building is automatically locked. Access during this time is only possible by selected employees by key.

Key management: There is a guideline for handling building keys / chip cards and the issuance is documented.

Security service: An external security service checks the building at regular intervals at night.

Location Hamburg:

Access app: Access to the business premises is only possible with a personalized access app or token. Only employees have a personalized access app/token. The cleaning company also has a personalized access app/token for the office space.

Locking system: Access to the building is open during business hours. Outside business hours, the building is automatically locked. During the locking, access is only possible with personalized tokens. The personalized token is issued only to employees of the facility management.

Duisburg location:

Manual locking system: access to the business premises is only possible with a key. Only employees have a key. The same applies to the cleaning company, caretaker and property management.

Locking system: Access to the building is locked during business hours and only accessible to resident companies with a key. The key is only issued to them.

Frankfurt location:

Manual locking system: access to the business premises is only possible with a key. Only employees have a key. We are subtenants on this floor, the landlord still has access to the floor, our rooms are manually locked by us in the evening by the employees

Locking system: Access to the building is open during business hours. Outside business hours, the building will be locked. During locking, access is only possible by key. The keys are owned by 2 employees and employees of the local companies.

Munich location:

Access app: Access to the business premises is only possible with a personalized access app. Only employees have a personalized access app. The cleaning company also has a personalized access app for the offices.

Locking system: Access to the building is open during business hours. Outside business hours, the building is automatically locked. During the locking, access is only possible with a personalized access app. The personalized access app is only issued to employees.

Location: Lisbon

Access code: Access to the business premises is only possible with an access code. This is only issued to employees and is changed at regular intervals.

Locking system: Access to the building is only possible with an access code. This is owned by all employees, as well as employees of the local company. The code is changed at regular intervals.

Location: Berlin

Coworking/open space with small dedicated 2-person office

Visitor logging: Visitors must be registered in advance, are checked at the entrance (airport level: with person/pocket scanner) and receive a visitor badge that must be carried. Visitor badges contain a barcode that can be used to leave/enter the building

(lock) without further checks. However, the visitor passes are never activated for the separately lockable office!

Chip card: Only employees belonging to the Berlin location have a chip card that can be used for an unlimited period of time and space. This can be used to enter the building (lock) and to enter the separately lockable office.

Locking system: The building can only be entered through a lock (chip card). The separately lockable office is secured with an electronic lock that can be unlocked by the chip card.

Other accesses: Separate security guards, cleaning staff, coworking managers, etc. will have access to the building/office (to carry out their respective activities).

Physical access control

Anti-virus software: Server systems and laptops are equipped with anti-virus software and are monitored centrally.

Authentication with user + password: Login to work devices and applications is done with personalized access data or biometric data of the employees.

- **AWS specific measures:** All employees are created in a special TR Management AWS account. Employees are authenticated with username, password and mandatory multi-factor authentication.

User permissions: User permissions are assigned according to the principle of least privilege and are checked regularly.

Clean Desk: There is a guideline for a tidy workplace and blank screen

Firewall: The network is protected by a hardware next-gen firewall (AV, IPS, IDS, DPI, ATP, Sandstorm detection). The firewall's firmware and signatures are updated regularly. The firewall's logs are regularly checked for unusual activity.

Network isolation: Networks are separated by demilitarized zones, and access to resources is restricted to the services/ports they need. Access to internal network resources from the public Internet is encrypted via the firewall appliance. VPN authentication is carried out via personalized username and password combination as well as a one-time password. When using an IPSec connection, a pre-shared key is requested instead. Access to the networks is restricted to the corresponding services/ports.

On offboarding: An on-/offboarding process exists, which includes, for example, the blocking of all systems when an employee leaves.

Password policy: A password manager is used throughout the company to securely manage and create passwords. There is a guideline for assigning passwords.

Inactivity locking: Work devices are automatically locked after 5 minutes of inactivity (using MDM).

Blocking of user accounts: User accounts are temporarily blocked and logged after multiple incorrect logins and/or ask for an additional captcha entry.

Locked work equipment: Work equipment is stored safely in a safe unless it is taken home.

Locked server rooms: Server rooms are not designated and are closed with a non-slip door. The door can only be opened using a personal code.

Encryption of data carriers: Work devices are encrypted with Bitlocker (Windows OS) or FileVault (Mac OS) (use of MDM). Data carriers for backups of work devices are encrypted.

Central access data management: The access data in an AzureAD directory or in the application itself is managed centrally by internal IT. Initial passwords are changed by the employee when they log in for the first time.

Access control

Authorization concept: Least privilege principle System/content authorizations are granted exclusively by internal IT via group memberships.

- **AWS specific measures:** A role concept exists for access to the client's corresponding AWS accounts.

Data deletion: Data carriers that are no longer needed or old are regularly disposed of in accordance with DIN66399.

Use of service providers: Business documents are regularly destroyed in compliance with the statutory retention period in accordance with DIN66399.

Event Log: Events are logged accordingly by the server or the application used.

Least privilege: Least privilege principle System/content authorizations are made exclusively by internal IT via group memberships. Authorization for administrators is only granted when appropriate need / necessity and is regularly reviewed.

Password light lines: There is a guideline for assigning passwords.

Safe storage: Work equipment is stored safely in a safe unless it is taken home.

Encryption of data carriers: Work devices are encrypted with Bitlocker (Windows OS) or FileVault (Mac OS) (use of MDM). Data carriers for backups of work devices are encrypted.

Transmission/transport control

VPN tunnels: Setup of VPN tunnels for dialing into the network from the outside.

Pseudonomyation

Pseudonomization policy: Personal and other data relevant from a data protection point of view are anonymized during development, testing or bug fixing or modified in such a way that the data cannot be assigned to specific persons without the use of additional information (e.g. by using pseudonyming scripts). If unchanged data must be used, the corresponding instructions of the client will be obtained and documented before the processing begins. Excluded from this regulation are data for the purpose of general commercial tasks such as accounting, bookkeeping and others. There is an internal policy to anonymize / pseudonymize personal data as far as possible in the event of disclosure, use for development / testing purposes or even after the expiry of the statutory deletion period.

- **AWS Specifics:** Pseudonymization on its own systems must be ensured by the client himself.

Separation requirement

Logical client separation: The master data of a client, its contact persons and the technical documentation of its projects are logically separated from other data.

Production and test systems: There is a separation between development, test and production systems, in which these systems are stored and executed on different virtual environments or different physical environments.

Regular auditing: Access and authorizations are managed by internal IT and regularly checked. Access and authorizations are managed by internal IT or the database owner and regularly checked.

AWS specifics: The separation takes place in dedicated AWS accounts.

Encryption

Transmission: Use of SMIME/PGP at appropriate locations if necessary. The transfer and communication of personal data or other data relevant from a data protection point of view is carried out in encrypted form, for example through encryption protocols, VPN and others. If supported by the systems used, system/application logging takes place. Communication with all SaaS systems used is always encrypted.

Access data: Documented processes are used to anonymize, archive or delete the data after the deadline, request or termination of the order in accordance with the deletion concept. Access data and passwords are never transmitted unencrypted to the Client or other third parties authorised by the Client, but are always separated from each other via different communication channels.

Input control

Crypto concept: There is a cryptography method for encrypted information.

Personalized usernames: Traceability of entry, modification and deletion of data through individual usernames (not user groups) and logging.

Logging: Technical logging of the input, modification and deletion of data is carried out in the corresponding applications.

Logging: Traceability of entry, modification and deletion of data through individual user names (not user groups) and logging. Rights to enter, change and delete data are assigned by internal IT.

Access rights: Traceability of input, modification and deletion of data through individual user names (not user groups) and logging.

AWS specifics: AWS-specific measures: Configuration changes in all AWS accounts are automatically recorded and logged using appropriate tools.

Availability check

Antivirus software: Server systems and laptops are equipped with anti-virus software and are centrally monitored.

Outsourcing data backup: Backups of internal systems are backed up daily in a data center in Germany.

Backup and recovery concept: There is a data backup concept. Mission-critical systems are backed up daily.

Fire alarm systems: The server room is equipped with an alarm system and alerts in the event of moisture, temperature rise and smoke development.

Fire extinguishers: Fire extinguishers are located near the server room.

Air conditioning: The server room is air-conditioned. In the event of an air conditioning failure, an automatic reporting process is carried out.

Temperature monitoring: The server room is equipped with an alarm system and alerts in the event of humidity, temperature rise and smoke development.

Uninterruptible power supply: There is an uninterruptible power supply. Servers shut down automatically in the event of a power failure.

AWS specifics: If the client has not booked a corresponding tecRacer Managed Service, it can check the availability of its AWS resources itself via https://status.aws.amazon.com/ and via the AWS CloudWatch Service. The client's AWS accounts use multi-redundant systems on AWS. AWS data centers are correspondingly redundantly secured with several power and Internet suppliers and with corresponding emergency power generators.

Recoverability

Data Recovery: Regular data recovery tests and logging of results are performed.

AWS specifics: If the Client has booked a corresponding tecRacer Managed Service, the data in the Client's AWS accounts can be backed up in the Client's AWS accounts on multi-redundant AWS systems via a central backup solution used by tecRacer (in accordance with the contractual scope of services). The backups created in this way can be restored via an explicit disaster recovery process. If the client has not booked a corresponding tecRacer Managed Service, he is responsible for this himself.

Order control

Selection: The subcontractors are carefully selected.

Data processing contract: Contracts for order processing are concluded with subcontractors in accordance with Art. 28 GDPR.

Data secrecy: The employees of the subcontractors are obliged to data secrecy.

Suppliers: In the case of subcontractors with processing in third countries, EU standard contractual clauses are used to ensure the level of data protection. There is a supplier management process.

Handling of unchanged data: If unchanged data has to be processed, the instructions of the client are obtained and documented before the processing begins.

Instruction management: Data of the client is processed exclusively according to the instructions of the client. The instructions of the client are documented. The Client legitimises himself by means of a specified procedure, e.g.: - by his customer password in the case of telephone notification, - by a self-created ticket in the ticket system after corresponding login in the ticket system or - by e-mail, whereby the Contractor sends a confirmation to the reply address

Description of the data protection management system

Audits: The level of awareness of data protection is evaluated at annual intervals.

DPO: The data protection officer has appropriate training, professional know-how, personal aptitude. As a staff unit, it is integrated into the organizational structure and free of conflicts of interest. He has adequate resources and support at his disposal.

Incident Response System: Incident response system for the traceability of security breaches and problems.

Information security management system: Information security management system (e.g. based on ISO 27001 or VdS 3473)

Training: Annual training on data protection is conducted, see Data Protection Instruction for Employees. The training courses on data protection are evaluated at biennial intervals and updated if necessary. The training presentations are reviewed and checked for adaptation, expansion and improvement.

Software-based tools: Use of software-supported tools to comply with data protection requirements (e.g. audatis MANAGER)

Obligation: Obligation to maintain confidentiality in accordance with Art. 28 para. 3 sentence 2 lit. b, Art. 29, Art. 32 para. 4 GDPR

Appendix 4: Subcontractors of the Contractor

Status of the listing	01 March 2023	
Subcontractors	Address	Service
Amazon Web Services EMEA SARL	5 Rue Plaetis, L-2338 Luxembourg	Provision of cloud services
Anycloud A/S	Hedegaardsvej 88, DK-2300 Copenhagen S, Denmark	MS365 Backup
Atlassian Pty Ltd, Atlassian Inc.	1098 Harrison Street, 94103 San Francisco, California, USA	Provision of wiki and Jira ticket system
Atlassian Pty Ltd.	Level 6, 341 George Street Sydney NSW 2000, Australia	Bitbucket (code management), Confluence (knowledge management), Jira (project management), Jira Service Management (ticket system)
AutoTask GmbH	Landwehrstraße 6, 80336 Munich	Provision of TicketTool, billing
HubSpot Inc.	25 First Street, 2nd Floor, 02141 Cambridge, MA, USA	Deployment CRM
Hubspot, Inc.	HubSpot Ireland Limited, HubSpot House, One Sir John Rogerson's Quay, Dublin 2, Ireland	CRM
Microsoft GmbH	South County Business Park, 18, One Microsoft Place, Carmanhall and Leopardstown, D18 P521 Dublin, Ireland	File Storage, Collaboration, Office365 Email
Rewind Software Inc.	333 Preston Street, Suite 200, Ottawa, Ontario, K1S 5N4	Atlassian Data Protection
SEMCO Software Engineering GmbH	Ellimahdstr. 40, 89420 Höchstädt	Provision of seminar management
KMpro	Tax advisor	https://kmpro-muc.de/
ClickMeeting	Ul. Arkońska 6, bud. A4, 80-387 Gdansk, Poland	Webinar Software ClickMeeting is connected to HubSpot via an interface, so registered attendees are automatically created as contacts in HubSpot.
Gilmore Global Logistics Services	120 Herzberg Rd. Kanata, Ontario K2K 3B7	Purchase of the AWS electronic scripts and send the links to the participants via the subcontractor Gilmore Global Logistics Services
EasyBill	Düsselstraße 21, 41564 Kaarst	Datev order processing and the SaaS product Easybill are used as

		billing tools. The SaaS product Easybill is purchased from the supplier Easybill.
CoffeeCup GmbH	CoffeeCup GmbH Hohenzollernststrasse 81 80796 Munich	Project Time Tracking
Audatis Services GmbH	Luisenstr. 1, 32052 Herford	Data protection management system
Lucid Software Inc.	10355 S Jordan Gateway STE 150, 84095 South Jordan, UT, USA	Lucidchart Enterprise
Slack Technologies, Inc	500 Howard Street, San Francisco, CA 94105, United States of America	Communication platform internally and externally
Zoho Corporation	4141 Hacienda DrivePleasanton, CA 94588USA	IT monitoring platform Site24x7
CloudCheckr Inc.	342 North Goodman StreetRochester, NY 14607USA	Cloud Cost and Security Management

Appendix 5: Recipients of instructions at the contractor

Name	Contact details	Range	Area of Command / Powers
Torsten Höpfner		Contracts for work and services Service Agreements	Completely
Eva Ramuschkat		Software Solutions	Completely
Dr. Felix Grelak		Training	Completely

Appendix 6: Deletion concept

Personal data of the Client for the commercial processing of the data at the Contractor:

The company master data and the contact details of the respective contact persons of the Client shall be stored by the Contractor in the following systems:

- Atlassian (Confluence, Jira Software) for project documentation

o When a contractual relationship is terminated, all project documentation is archived.

o At the explicit request of the client, the data of the contact persons can be deleted or anonymised with NN.

- Datev for Accounting

o When a contractual relationship is terminated, the company master data is retained in the system, as it serves as a reference for the invoices created. At the explicit request of the client, the data of the contact persons can be deleted or anonymised with NN.

- Microsoft 365 (Exchange, Sharepoint, MS Teams)

o Upon termination of a contractual relationship, the communication data of the client's contact persons will be retained in Microsoft 365.

- Hubspot

o When a contractual relationship is terminated, the company master data is retained in the system, as it serves as a reference for the offers created. At the explicit request of the client, the data of the contact persons can be deleted or anonymised with NN.

- Anycloud (Backup MS365)

o Data retention is set at 10 years. In accordance with Art. 17 (3) GDPR, we store the data to comply with other legal obligations.

- Rewind (Backup Atlassian)

o Data storage is set for one year. After that, the data will be permanently deleted.

Personal data of the client and its customers in software development projects:

- Atlassian for project documentation

o The communication data of the client's contact persons in Jira and Confluence will be retained as long as the project is in the warranty phase and/or a valid maintenance contract exists. At the explicit request of the client, the data of the contact persons can be deleted or anonymised with NN.

- Personal data of the Client and its customers in the Amazon AWS infrastructure provided by the Contractor

- The contractor makes the infrastructure requested by the customer available on Amazon AWS.

- The Contractor is not responsible for the storage/processing/deletion of personal data of the Client or its customers, as this takes place within the Client's applications on the Amazon AWS infrastructure provided.

- This Amazon AWS infrastructure may be managed accordingly by a separate managed service with the contractor contract at the request of the client. As part of this support, the Contractor shall also perform data backups in the Client's Amazon AWS infrastructure to corresponding storage resources in the Client's Amazon AWS infrastructure.

- On the instructions of the Client, the Contractor shall delete corresponding historical data backups. Amazon AWS ensures that Amazon AWS resources deleted by the contractor are actually physically deleted (Amazon AWS has been audited accordingly for this purpose: https://aws.amazon.com/de/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/)

- Individual data records from a data backup cannot be selectively deleted, but are only deleted when the entire data backup is deleted.

Personal data of the Client, its employees and its customers for public training and company training:

The company master data, the contact details of the respective contact persons and the training participants of the Client shall be stored by the Contractor in the following systems:

- SemcoSoft Seminar Administration

o Contact persons of customers and training participants can be deleted at any time via functionalities provided by SemcoSoft if a contact person explicitly requests this.

- To do this, this contact person must then also be deleted in HubSpot, as training participants in particular are imported into HubSpot