Agreement on Data Processing
in accordance with Article 28 General Data Protection Regulation

Table of Contents

Section **Page**

SUBJECT MATTER OF AGREEMENT

1.1 According to the General Terms and Conditions of Hanseaticsoft GmbH (hereinafter **"Processor"**) for "Software as a Service" as well as the quote of the Processor (hereinafter collectively **"Main Agreement"**) the Processor makes available software products (hereinafter **"Software**") for use via internet to the customer designated in the Main Agreement (hereinafter **"Controller"**). The Processor and the Controller are hereinafter individually or, as applicable, collectively also referred to as **"Party"** or **"Parties"**. The Processor operates the Software through a data processing service provider (also known as "Software as a Service" model). This Agreement on Data Processing (hereinafter **„Agreement"**) specifies the Parties' duties regarding data protection laws. The Agreement applies to all services which relate to the commissioned data processing where the Processor or its personnel may get in contact with personal data, which are provided to the Processor by the Controller.

1.2 The type of processed data and categories of data subjects, and the nature, purpose and subject matter of processing of personal data by the Processor on behalf of the Controller and the categories of data subjects are defined in **Annex 1**.

2. TECHNICAL AND ORGANIZATIONAL MEASURES

2.1 The Processor shall establish measures in accordance with Art. 28 Para. 3 Point c, and Art. 32 GDPR in particular in conjunction with Art. 5 GDPR. The measures to be taken are measures of data security and measures that guarantee an appropriate data protection level taking account of risks for confidentiality, integrity, availability and resilience of systems. The state of the art, implementation costs, the nature, scope and purposes of processing as well as the probability of occurrence and the severity of the risk for the rights and freedoms of natural persons within the meaning of Art. 32 Para. 1 GDPR must be taken into account.

The measures taken by Processor are specified in **Annex 2**.

2.2 The technical and organizational measures are subject to technical progress and further development. In this respect, the Processor may implement alternative adequate measures. However, the security level of the defined measures shall not be reduced. Substantial changes must be documented.

2.3 The Processor regularly controls the internal processes as well as the technical and organizational measures in order to ensure that the data processing which lies within

his responsibility is carried out in accordance with the applicable data protection laws and to ensure the protection of the rights of the data subjects.

3. RECTIFICATION, RESTRICTION AND ERASURE OF DATA

3.1 The Processor may not on its own authority modify or delete the data that is being processed on behalf of the Controller, or restrict the processing such data, but only on documented instructions from the Controller. In the event that a data subject contacts the Processor directly concerning a modification or deletion of data, or restriction of processing, the Processor shall immediately forward the data subject's request to the Controller.

3.2 The Processor shall assist the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's 'right to be forgotten', and rights to rectification, data portability and access. The Processor may request payment of fees for assistance which is not owed under the Main Agreement.

4. QUALITY ASSURANCE AND OTHER DUTIES OF THE PROCESSOR

4.1 The Processor entrusts only such employees with the data processing outlined in this Agreement who have been bound to confidentiality. Unless required by law to process the data, the Processor shall not process the data except as on instructions from the Controller, which includes the processing allowed under this Agreement and the Main Agreement.

4.2 The Processor shall assist the Controller in complying with the obligations concerning the security of personal data, reporting of data breaches, data protection impact assessments and prior consultations, as stipulated in Articles 32 through 36 of the GDPR. These include:

4.2.1 The obligation to report a personal data breach immediately to the Controller,

4.2.2 The duty to assist the Controller with regard to the Controller's obligation to provide information to the data subject and to immediately provide the Controller with all relevant information in this regard.

4.2.3 Supporting the Controller with its data protection impact assessment.

4.2.4 Supporting the Controller regarding prior consultation with the supervisory authority.

4.3 Processor may charge a fee for support which is not included in the description of services in the Main Agreement or which is caused by a misconduct of the Controller.

5. SUBCONTRACTING

5.1 Subcontracting for the purpose of this Agreement is to be understood as services which relate directly to the provision of the principal service. This does not include ancillary services, such as telecommunication services, postal / transport services, maintenance and user support services or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing equipment. The Processor shall, however, be obliged to make appropriate and legally binding contractual arrangements and take appropriate inspection measures to ensure the data protection and the data security of the Controller's data, even in the case of outsourced ancillary services.

5.2 The Controller herewith agrees that Processor engages Microsoft Ireland Operations Ltd. based in Ireland (“Microsoft Ireland”) as a subcontractor for the collection, processing and use of data. The Processor may in particular use the infrastructure and platform services of the Windows Azure platform, e.g. for providing server and computing capacities, data storage and database services (collectively “Windows Azure Services”). The Processor uses Windows Azure Services in accordance with Microsoft Ireland’s general terms of use (http//www.windowsazure.com/de-de/support/legal) and security measures (http://www.windowsazure.com/en-us/support/trust-center/compliance/).

5.3 The Processor notifies the Controller of any intended change with respect to the addition of, or replacement by, any other processors. The Controller may object to such change by giving notice within 14 days as of receipt of the notification of change. If the Controller does not oppose within such term, the change shall be deemed approved. The Controller may not oppose without having an own legitimate interest which overrides the interests of the Processor.

5.4 If a sub-processor provides processing outside of the EU or the EEA, the Processor shall ensure compliance with data protection laws by taking appropriate measures.

6. SUPERVISORY RIGHTS OF THE CONTROLLER

6.1 The Controller has the right, after consultation with the Processor, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. The Controller has the right to convince itself in the Processor's business premises of the Processor's compliance with this Agreement by means of random checks, which are, as a rule, to be announced in good time.

6.2 The Processor shall ensure that the Controller is able to verify compliance with the obligations of the Processor in accordance with Art. 28 GDPR. The Processor undertakes to give the Controller the necessary information on request and, in particular, to demonstrate the execution of the technical and organizational measures.

6.3 Evidence of such measures may be provided by

6.3.1 Compliance with approved codes of conduct pursuant to Art. 40 GDPR;

6.3.2 Certification according to an approved certification procedure in accordance with Art. 42 GDPR;

6.3.3 Current auditor's certificates, reports or excerpts from reports provided by independent bodies (e.g. auditor, data protection officer, IT security department, data privacy auditor, quality auditor);

6.3.4 A suitable certification by IT security or data protection auditing (e.g. according to BSI-Grundschutz (IT baseline protection certification developed by the German Federal Office for Security in Information Technology (BSI) or ISO/IEC 27001).

6.4 The Processor may claim remuneration for enabling Controller inspections.

7. AUTHORITY OF THE CONTROLLER TO ISSUE INSTRUCTIONS

7.1 The Controller shall immediately confirm oral instructions (at the minimum in text form).

7.2 The Processor shall inform the Controller immediately if he considers that an instruction violates data protection laws. The Processor shall then be entitled to suspend the execution of the relevant instructions until the Controller confirms or changes them.

8. DELETION AND RETURN OF PERSONAL DATA

8.1 Copies or duplicates of the data shall not be created without the knowledge of the Controller, with the exception of (i) backup copies as far as they are necessary to ensure appropriate data processing, and (ii) retention of data required to meet statutory data retention laws.

8.2 After conclusion of the contracted work, or earlier upon request by the Controller, at the latest upon termination of the rendering of IT-services, the Processor shall hand over to the Controller or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the contract that have come into its possession, in a data-protection compliant manner. The same applies to any and all connected test, waste, redundant and discarded material. The log of the destruction or deletion shall be provided on request. The Processor's obligations under this Section 8.2 do not apply to the extent that Union or EU Member State law requires storage of the personal data.

8.3 Documentation which is used to demonstrate data processing in accordance with the Agreement shall be stored beyond the contract duration by the Processor in accordance with the respective retention periods. The Processor may hand such documentation over to the Controller at the end of the contract duration to relieve the Processor of this contractual obligation.

9. TERM OF PROCESSING; TERMINATION

The duration of this Agreement corresponds to the term of the Main Agreement and includes the term after termination of the Main Agreement until full return of deletion of the personal data which have been provided by the Controller to the Processor in connection with the performance with the Main Agreement. This does not affect the right to terminate the Agreement with good cause.

10. GENERAL PROVISIONS

10.1 This Agreement shall be governed by and construed in accordance with German law. Place of performance and jurisdiction is Hamburg, Germany.

10.2 Any amendments or additions to this Agreement, including this Section 10.2, require written form.

10.3 Should individual provisions of this Agreement be invalid or unenforceable for actual or legal reasons, without rendering the continuity of the remaining provisions unreasonable as a whole for a Party, this shall not affect the validity of the remaining provisions. The same shall apply in the event of a contractual gap. In lieu of the invalid or unenforceable provisions or to close any contractual gap, the Parties shall agree to a provision that comes closest to fulfilling the economic purpose intended by the Parties.

Exhibits:

Annex 1: Nature and Purpose of Processing, Subject Matter of Processing, Type of Data, Categories of Data Subjects

Annex 2: Technical and Organizational Measures

ANNEX 1: NATURE AND PURPOSE OF PROCESSING, SUBJECT MATTER OF PROCESSING, TYPE OF DATA, CATEGORIES OF DATA SUBJECTS

Categories of data subjects	In particular: • users of Software (particularly personnel of customers, ship managers and crewing agents) • crews/member of crews of vessels managed through the software • data of personnel of business partners of the customer (e.g. contractual partners of charter agreements)
Type of data	Depending on the modules licensed, the following categories of personal may be collected, processed and used: • Contact data of users of software (e.g. name, address, contact details, birthday, certificates, CV/experiences, body height, marital status, agency • Contract data of crew members (e.g. position, remuneration, age supplement, travel data, presence, responsibilities, performance evaluation) • Other data of crew members on vessels (e.g. travel information, travel documents, availability, information and documents regarding fitness and vital status, information on specific events on vessels • Contact data of business contacts, e.g. ship managers and crewing agents • Data on the use of the Software (protocol data) The data may include personal data within the meaning of Art. 9 GDPR, Section 22 of the German Federal Data Protection Act (BDSG) (special categories of personal data, e.g. fitness/vital status, illness, origin of crew members
Recipients	Processor and subprocessor
Nature and purpose of processing	Making available of Software together with storage via the internet; rendering of IT services, in particular support services

ANNEX 2: TECHNICAL AND ORGANIZATIONAL MEASURES

Preliminary remark: Within the sope of this Agreement Hanseaticsoft GmbH (hereinafter **„Hanseaticsoft“**) solely processes personal data for the purpose of meeting its service and support obligations under the Main Agreement. All data are processed on the Microsoft Azure platform (cf. Section 5.3 of the Agreement; hereinafter **„Microsoft Azure Server“**). Hanseaticsoft accesses the data through its personnel which is entrusted with the provision of the services (hereinafter **“Support Personnel**”) via laptops or desktops provided for the aforementioned purpose (hereinafter **„Support Computers**“). The applications used by the Support Personnel are hosted on the Office 365 platform (hereinafter **„Office 365 Server**“). In case of certain support incidents it may be required that Support Personnel transfers data from the Microsoft Azure Server in an Office 365 application, where Support Personnel may use such data. Hanseaticsoft has entered into agreements with Microsoft Ireland Operations Limited on the use of the services Microsoft Azure and Office 365. The technical and organizational measures undertaken by Microsoft Ireland Operations Limited for these services are specified in the Microsoft Online Services Terms (http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31). The following describes the technical and organizational measures undertaken by Hanseaticsoft.

1. Confidentiality (Art. 32 Parapraph 1 Point b GDPR)

1.1 Physical Access Control

No unauthorized access to Support Computers:

The Support Computers of the Support Personnel are exclusively kept in the business premises of Hanseaticsoft in the office building Possmoorweg 2, 22301 Hamburg, Germany. Access to the office building and to the business premises of Hanseaticsoft are at any time secured through locks. The main entrance of the building is equipped with a video supported intercom, and the access to the office premises of Hanseaticsoft is equipped with a viewing panel. If a person requests from Hanseaticsoft access to the office building or the Hanseaticsoft office premises, then Hanseaticsoft examines such person’s authorization. Hanseaticsoft does not grant access without such authorization.

1.2 Data Carrier Contol

No unauthorized reading, copying, modification or deletion of data carriers:

Hanseaticsoft does not use own data carriers, which store data of the Controller.

1.3 Access, Process and User control

The Support Computers serve the exclusive purpose of meeting Hanseaticsoft's service and support obligations.

Access to the Support Computers is protected through a qualified password, which consists of at least 8 characters, including at least one special character and one number.

The password is regularly changed on a six monthly basis. Moreover, the password is changed without undue delay if it gets known to an unauthorized person or in the event of an actual suspicion of such knowledge.

In case of the absence of personnel from the Support Computer the password lock will be activated within 15 minutes.

Only the Support Personnel has access to the Support Computers as well as access to the Microsoft Azure Server as required for providing support services, and access to any data which are processed on the Office 365 Server in relation to the commissioned data processing. This is ensured by user accounts of Support Personnel, which use require the entry of a user name and password.

1.4 Severability

The separate processing of data, which is collected for different purposes:
Each customer of Hanseaticsoft has access to its own database, which does not have any link to the databases of other customers. It is not possible that one customer may view the data or user administration of another customer. Accordingly, in case of a support incident the Support Personnel does only have access to the data of the customer which are subject of the respective support incident. The Support Personnel processes the Controller's data separate from the other customers' data at any time.

1.5. Pseudonymisation (Art. 32 Para. 1 Point a GDPR; Art. 25 Para. 1 GDPR)

The processing of personal data in such a manner, that the data cannot be associated with a specific data subject without the assistance of additional information, provided that this additional information is stored separately, and is subject to appropriate technical and organizational measures:
Hanseaticsoft does not analyze personal data. In particular does Hanseaticsoft not generate user profiles.

2. Integrity (Art. 32 Para. 1 Point b GDPR)

2.1 Data Transport Control

No unauthorized reading, copying, modification or deletion in case of electronic transmission or transport:

Any transmission/transport of data is encrypted
Any transmission/transport of data is logged
Any transmission/transport of data is only done for the purpose of backups or data processing in accordance with this Agreement and the Main Agreement

2.2 Data Entry Control

Verification, whether and by whom personal data is entered into a data processing system, is modified or deleted:

Only Support Personnel is entrusted with the processing of personal data within the scope of the commissioned data processing.
Log data are generated for each data entry, modification or deletion; such log data include information on the author of the processing.
Each support incident is logged. Edited protocols are made available to the Controller upon the Controller’s request.

2.3 Data Integrity

No damage to data due to system failures:

Subject to technical possibilities the Support Computers are maintained so there is no damage or loss of data.

Each database is mirrored three times. The data are backed up regularly.
The data are hosted on a SQL server platform, on which server connections, data and stored procedures are encrypted.

3. Availability and Resilience (Art. 32 Para. 1 Point b GDPR)

3.1 Availability Control

Protection against accidential or wilful destruction or loss:

The Support Computers include virus protection and a firewall, which are constantly updated.
Regarding data backups see above, 2.3.
Modern hardware which is regularly maintained ensures an uninterruptable power supply of the Support Computers and the availability of data.

3.2 Rapid Recovery (Art. 32 Para. 1 Point c GDPR)

Upon a malfunctioning of a Support Computer all system components are examined for errors without undue delay to assess whether data has been damaged.
In the event of a damage or loss of data, such data will be restored from a backup.
A report on the scope and the correction of the malfunctioning will be maintained for future reference.

3.3 Reliability

Availability of all functions of the system and error reports:

All Support Computers are updated, checked for errors and maintained regularly.
It is regularly checked whether the systems used comply with the then current technical standards.

4. Procedures for regular testing, assessment and evaluation (Art. 32 Para. 1 Point d GDPR; Art. 25 Para. 1 GDPR)

4.1 Data Protection Management

The data protection officer of Hanseaticsoft reports, provides consulting to, and controls Hanseaticsoft, to ensure data protection compliance at Hanseaticsoft. The duties assumed by the data protection officer include the following:

- Training and providing consulting to Hanseaticsoft and its employees regarding obligations and requirements under data protection laws
- Control of data protection law compliance and the strategies for the protection of personal data, the raising of awareness and training of the employees of Hanseaticsoft, and the respective audits and controls thereof
- Consulting with respect to the data protection impact assessment
- Contact for and cooperation with the supervisory authority

All employees of Hanseaticsoft receive advice on data protection law issues and are bound to data protection compliance.
The management of Hanseaticsoft regulary examines by itself or through qualified employees, whether the internal procedures meet data protection law requirements, and undertakes adequate measures to ensure such compliance.
The management of Hanseaticsoft regularly receives lawyer's advice with regards to data protection law issues.

4.2 Incident Response Management

In case of a security incident, which could have an impact on the Support Computers or the data processing systems of the providers engaged by Hanseaticsoft, the Hanseaticsoft employees inform the management of Hanseaticsoft immediately. If the security incident may have an impact on the Controller's data, Hanseaticsoft shall inform the Controller without undue delay.

4.3 Data Protection by Design and Default (Art. 25 Para. 2 GDPR);

When choosing the hardware and software used for the performance of services under the Main Agreement Hanseaticsoft takes account of such hardware's and software's compliance with the principle of data minimisation.
When processing the data Hanseaticsoft refrains from using components which are not required for the processing of the data and which may impair the data of the Controller.

4.4 Order Control

Hanseaticsoft is under the contractual obligation to process the Controller's data in accordance with the Controller's instructions.
The rights of Hanseaticsoft are clearly and comprehensively set forth in a contract. Orders and support requests are documents in text form in order to document such orders and support requests for future references.