

Licence Terms for ASP-Software Softship.SAPAS

User:

Softship GmbH
Notkestrasse 15
22607 Hamburg, Germany
(“Softship”)

§ 1 Subject matter of the Agreement

1. The subject matter of these terms is the provision of the software Softship.SAPAS (“**Software**”), which allows port agents to better coordinate and administer their daily duties in the sector of „Port Call Handling“. This software consists of the program code and the related user documentation in electronic form.
2. With the option of accessing the software within the scope of the Application-Service-Providing (“**ASP**”) the customer receives the non-exclusive right to use the software. Access is limited in time to the period of use respectively acquired by credits (see § 5 para. 2 of these terms), independent of the period of the contract.
3. All other rights to the software, in particular the right to conduct changes to the software, to sell the software and/or to use the software for other purposes, as well as all rights to the brand Softship.SAPAS, the business secrets or other intellectual property to the software remain with Softship.
4. The customer shall not be entitled to assignment, transfer or sub-licencing without the prior written approval from Softship.

§ 2 Terms for Software provision via ASP

1. As the customer is provided with the software within the scope of the ASP, he will receive access to the software environment, in which the software is installed, via the Internet-Browser. Softship does not assume any guarantee with regard to the software being suitable or applicable for use in locations other than the stated software environment.
2. The customer shall receive both read and write access to the software environment in which the software is installed. For this purpose, Softship will provide storage space in appropriate scope according to its own discretion.
3. Softship will conduct a backup of the customer data once a day and will use state-of-the-Art hardware for this purpose. The customer is responsible for the storage periods under commercial and tax law.
4. Softship will provide the contractual services with an availability of 97%. This availability is calculated on the basis of the time allocated to the respective calendar month less the maintenance work defined in the following. During business hours, the performance may be interrupted at maximum for 30 minutes in total per day. Business hours are all work days in the time from 8.30 a.m. to 5.00 p.m. CET, decisive is the registered office of Softship in Hamburg.
5. Softship is entitled to temporarily suspend or restrict the availability of the contractual performances outside of business hours (“Downtimes”), to be able to conduct maintenance work or improvements of the system. Softship will inform the customer on time in text form of the start and duration of the

maintenance work. The downtimes within the maintenance window may, however, not exceed 10 hours per month. Every commenced quarter of an hour will be calculated as a full quarter of an hour. Times during which the system is not available in the agreed access times are also deemed to be downtimes.

§ 3 Obligations of the customer

1. The customer shall be obliged to prevent unauthorised third party access to the software environment through suitable precautions. In particular access data (user name, passwords) may never be made accessible to unauthorised third parties and only ever to the employees who have to work with the software. These employees must be instructed about the prohibition of disclosure of access data to unauthorised third parties.
2. Softship will not actively process the data entered by the customer (“**Customer data**”). Insofar, the customer is responsible for these data and their accuracy himself, as far as he does not prove that the processing algorithms of the software have conducted such a processing themselves and without control by the customer.
3. The technical connection to the Softship computer centre is the responsibility of the customer. The transfer point for the software is therefore the router output of the computer centre. Softship is therefore not responsible for the quality of the required customer hardware and software nor the telecommunications connection between the customer and Softship up to the transfer point.
4. In as far as the customer does not expressly point out in advance, Softship may assume that all customer data it may come into contact with, are backed up before the initial import into the system.
5. The customer grants Softship the right to read and check the user data imported by the customer or its employees, when Softship must assume for prudent considerations that all or a part of the data are linked to unlawful acts. Above and beyond this, the customer shall grant Softship the right to access all user data stored on the servers used by the customer, when this access is required within the scope of correct administration of the software environment.
6. In as far as actions by the customer (as well as his employees) or data entered by the customer, resp. its employees violate legal regulations or third party rights (e.g. copyrights), the customer shall release Softship from liability in full and shall reimburse Softship all costs the latter incurs from these (e.g. costs for lawyer). There is agreement that Softship is not obliged to check data transferred from customer systems for possible legal violations.

§ 4 Software Maintenance

1. Softship will constantly monitor the functioning of the software and will remove any software errors which become known.
2. Softship will also monitor the functioning of the software environment and its link to the data networks. Identified faults will receive immediate response and will be rectified as quickly as possible.

§ 5 Remuneration

1. The use of the software in its basic functions is free of charge. The customer shall pay a remuneration for the use of certain software functions, the amount can be found in the respectively valid price list which is enclosed with these terms with the status 01.07.2022 and which can also be viewed at any time on the website at this link. The listed prices are exclusive of the currently valid 19% VAT.
2. The above Annex 1 also contains the concrete regulations for the purchase of the “Credits” required for the use of the software.
3. Softship may adjust its prices in accordance with the following regulations at its reasonable discretion, if the overall costs for the subject matter of the Agreement change due to circumstances which occur after conclusion of the Agreement, were not foreseeable and which are not within the discretion of Softship. Hereafter, Softship may increase the prices once per calendar year when

the above overall costs rise. The customer shall be informed in text form about the price increase at least six weeks prior to the coming into force. Here, special mention will be made of a possible right to termination with its periods and legal consequences. If the price increase is more than 5% of the previous price, the customer shall be entitled to terminate the Agreement in writing within a period of four weeks after receipt of the notification about the increase, effective as per the date of coming into force. On the other hand, Softship will lower the prices when the above overall costs drop. The price cut shall correspond to the amount of the overall cost reduction.

§ 6 Changing these Licence Terms

Softship is entitled to change these Terms at any time. Changes become effective when the customer agrees to these expressly or they were brought to customer's notice in text format, if the customer does not object within a period of 10 days. If the customer does object, the Licence Agreement shall terminate as per the next possible date of termination in accordance with § 9 of these Terms while maintaining the contractual contents.

§ 7 Warranty

1. The software and its performance are known to the customer. It has been developed under consideration of scientific diligence and the recognised engineering standards, in particular accepted programming rules.
2. In as far as the functions of the software deviate from the contractually specified purpose and/or demonstrate these defects, the customer must make a complaint forthwith in writing. Softship will then rectify these – possibly through third parties. Claims for damages remain unaffected.
3. A desistance from the Agreement, resp. right to extraordinary termination of the contract only comes into question if the continuation of the contractual relations is unreasonable or a not inconsiderable violation of contractual duties continues despite warning, resp. setting of a deadline. A warning is not necessary if the violation of contractual duties is so grave that a warning does not seem suitable to terminate the breach of duty and/or to re-establish trust. Before such a termination of the contract, Softship shall be regularly entitled to two attempts at rectifying the defects related to the respective defect.
4. The customer is aware that Softship does not operate an own network and does not provide the customer with Internet access. For this reason, Softship does not accept any responsibility for the functioning of the respective access to the Internet.
5. The legal warranty claims apply for the remainder

§ 8 Liability

1. In all cases of contractual and non-contractual liability, Softship will pay damages exclusively in accordance with the following limits:
 - a. Upon premeditation in the full amount, also in the absence of a characteristic which Softship has guaranteed;
 - b. Upon gross negligence only in the amount of the foreseeable damage which was to be prevented by the violated obligation;
 - c. in other cases: only from violation of an essential contractual obligation, when the contractual purpose is endangered by this, however only ever in the amount of the foreseeable damage;
 - d. above and beyond this: in as far as Softship is insured against the occurred damages, within the scope of the insurance cover for the public liability insurance in the amount of EUR 2.5 million.



WISETECH GLOBAL GROUP

2. The limitations of liability in accordance with clause 1 do not apply to the liability for personal injuries and liability according to the product liability law.
3. Softship reserves the right of defence of contributory fault. In the case of a breach of duty which does constitute a defect, the customer may only rescind or terminate when Softship is responsible for the breach of duty. A free right of termination of the customer (in particular pursuant to §§ 651, 649 BGB (German Civil Code)) is excluded. The legal prerequisites and legal consequences apply for the remainder.

§ 9 Period

1. The contractual relationship will begin when the contract is concluded and will be concluded for an indeterminate period. The provision of the performances will start from the agreed point of time.
2. The contractual relationship may be terminated in writing by both parties with a period of notice of one month.
3. The extraordinary termination because of, or in connection with a breach of duty is only possible after a preceding written warning with appropriate deadline of not less than 14 working days. If the party authorised to terminate has more than 14 working days knowledge of the circumstances justifying the extraordinary termination, he can no longer base the termination on these circumstances.

§ 10 Legal consequences on termination of the Contract, Expiry of the acquired Credits

1. With termination of the contractual relations, Softship is obliged, upon wish of the customer, to provide the data stored by the latter on a common data carrier or by way of remote data transmission. The customer may demand that the above data shall be handed over to a third party nominated by it. The customer is obliged to reimburse Softship for the necessary and proven costs incurred by the surrender.
2. After the surrender, Softship shall be entitled to delete all customer data stored in the software environment. Before that, the customer shall be informed in text form with a term of notice of at least 14 days.
3. **In as far as the customer still owns funds from acquired credits at the end of the contract, (§ 5 para. 2), this credit balance shall be forfeited.**

§ 11 Data Protection

1. The parties shall observe the legal provisions for data protection, in particular the EU-data-protection-regulation (GDPR), the Telemedia Act as well as the Federal Data Protection Act. The customer shall obligate the employees appointed in connection with the contract and its execution to observe data secrecy pursuant, in as far as these have not already been obligated. In addition, all employees with access rights shall provide their consent in writing to collect and transmit their – necessary for using the software – personal data to Softship servers (name, first name, e-mail address, telephone number, street, place of residence, date of birth), to the extent required by law.
2. If the customer collects, processes or uses personal data, he is also responsible for being entitled to do this according to the applicable, especially data protection provisions, and shall release Softship from any third party claims in the case of a violation. As far as the data to be processed are personal data, there is a case of contractual processing and Softship shall observe the legal requirements for contractual processing and instructions of the customer (e.g. compliance with deletion and blocking obligations, see Art. 28 DSGVO / GDPR. The instructions must be notified on time and in writing or textual form. The contractual contents for contract data processing are regulated in **Annex 2**.
3. Softship shall undertake the technical and organisational safety precautions and measures pursuant to Art. 32 GDPR / DSGVO. Softship shall protect, in particular, the services and systems which are within its access as well as the user data stored on the server by the customer or concerning the customer



WISETECH GLOBAL GROUP

and possibly other data, against unauthorised information, storage, change or other non-authorized access or attacks - be this through technical measures, viruses or other malicious programs or data or through physical access – by employees of Softship or third parties, no matter in which way these take place. He shall undertake the suitable and usual measures which are offered according to state-of-the-art technology, in particular virus protection and protection against similar malicious programs, as well as other security of his facilities including protection against burglary.

4. Softship shall collect and use customer-related data only in the scope as required for the execution of this contract. The customer shall agree to the collection and use of such data in this scope.
5. The obligations according to para. 2 to 4 exist as long as user data are within the sphere of influence of Softship, including beyond the end of the contract. The obligation according to para. 4 also exists beyond the end of the contract for an indeterminate period.
6. In as far as Softship conducts data processing in a non-member state of the EU as well as EEA or transfers these there, it will announce this in advance in writing or textual form to the customer. If the customer agrees to the transfer, the standard contractual clauses II for the transfer of personal data from the community into third countries (Decision 2004/915/EG by the Commission of 27.12.2004) or other types of warranties according to Art. 46 GDPR / DSGVO shall apply.
7. Requests for information, enquiries and contradictions against the data processing or notices for the correction of customer data can be addressed directly to the following customer data with specification of name, address and possibly customer number:

Cargowise GmbH
Attn. Mr. Dirk Selter
Notkestrasse 15
22607 Hamburg
Dirk.Selter@wisetechglobal.com

The customer can also direct advertising contractions to Softship at:

Telephone +49 40 89 06 8-0
Dirk.Selter@wisetechglobal.com

§ 12 Blocking

Softship will block customer access after expiry of the period of use earned by credits (§ 5 para. 2). Softship shall notify the customer of such an expiry on time and in text form and recommend an extension through the purchase of further credits. Blocking access to the server is also permissible, if the customer falls behind with other payment obligations and was warned unsuccessfully in advance in writing with an appropriate payment period and threat of the blocking. Blocking is also possible when a.) there is a threat to the facilities of Softship – in particular the relay system (e.g. through responses from end systems) – or public safety. b.) the customer uses servers and/or software for illegal purposes (e.g. storage of copyright infringing contents) or c.) the customer gives reason for instant termination of the contract.

§ 13 Secrecy

1. The customer will maintain silence about all confidential information which he has gained knowledge of within the scope of these contractual relations, resp. will use this vis-à-vis third parties – no matter for which purpose – only in the previously determined written consent by Softship. Information to be treated confidentially includes information expressly determined as confidential by Softship and such information where confidentiality results from the circumstances of the transfer.

2. The obligations according to para. 1 can be dropped for such information or parts thereof for which the customer can prove that these
 - were made accessible rightfully by third parties without obligation of confidentiality or
 - became known or generally accessible to the public after the date of receipt without the information-receiving party being responsible for this.
3. Public declarations by the parties about a cooperation will only be made with prior mutual agreement.
4. The obligations according to para. 1 shall exist beyond the end of the contract for an indeterminate period, and this as long as an exemption according to para. 2 has not been proven.

§ 14 Conclusion of Contract

1. The conclusion of the contract in accordance with the provision can be carried out via the Internet. For this purpose the customer must proceed as follows:
2. The customer has to first register in a registration form ("Registration"). Here, the customer enters the name of the company, email of the user and a password to be selected. A registration by private persons without specification of a company is not possible. The Softship.SAPAS offer is solely directed at companies, insofar the regulations for distance selling do not apply. The customer will be informed about this again before sending the form.
3. The customer can change his entries before sending the registration form.
4. To send the registration form, a confirmation of these Licence Terms, the data protection declaration as well as the entrepreneurial status is necessary by clicking on the existing box. The customer does not enter into a payment obligation by sending the form because the later purchase of credits (§ 5 para.2) is necessary for the use.
5. The system then sends a confirmation to the specified email address with a link, which in turn must be clicked on by the email recipient. By activating the link, the customer reaches the Softship Website which concludes the registration and thereby conclusion of the contract.
6. By entering the email address and password, the customer can now use the software and create individual users.
7. The customer can view these Licence Terms at any time in the current version on the Softship website and store these in a reproducible form. They are provided in the German and English languages. On the other hand, the concrete contractual text assigned to the customer will not be stored.

§ 15 General Provisions

1. Where legally permissible, the place of fulfilment and exclusive place of jurisdiction is Hamburg.
2. The present Licence Terms as well as all agreements concerning this matter between Softship and the customer are subject to German law. The application of the UN Sales Convention (CISG) is excluded.
3. Should one provision be or become invalid or void, the validity of the remaining provisions shall not be affected by this. In this case, the invalid or void provision shall be replaced by a reliable agreement which comes closest to the economic purpose of the original, invalid or void provision.

Annexes:

1. Price list, issued 01.07.2022
2. Data Processing Agreement (DPA)

Annex 1: Price List

1. Acquisition of Credits

The customer can request for credits by sending an e-mail to sales@softship.com by stating the company name of the customer and the requested number of credits. The customer will receive an offer from Softship by e-mail. After the customer has accepted the offer Softship will send an invoice for the accepted offer. After the funds have been received from the customer Softship will add the paid credits to the customers Softship.SAPAS account.

2. Forms of Payment

Softship exclusively offers the following forms of payment:

- Giro
- Telegraphic transfer

The invoice will be sent to the customer via email.

3. Prices

Use of the software in its basic functions is free of charge for the customer. However, when making use of certain functions, it is necessary to honour credits subject to a charge. The following credits will be deducted from the clients credit balance:

- **Offer:** 5 Credits
- **Port Call:** 50 Credits
- **Port Call based on Offer:** 45 Credits

4. Discount campaigns

Softship can conduct discount campaigns. In such cases the customer will receive a certain number of credits on top of his acquired credits, depending on the campaign, without any further costs.

Annex 2: Data Processing Agreement (DPA)

This Data Processing Agreement (**DPA**) is effective on the Effective Date made between Softship GmbH, Notkestrasse 15, D-22607 Hamburg, Germany (**Softship**) and **Customer**, each as defined on the Execution Page and each a **Party** and together the **Parties**.

This DPA replaces any prior terms and conditions on the same subject matter that have been agreed between the Parties.

For the purpose of this DPA, the Customer is the data controller and Softship is the data processor.

Clause 1

Subject matter and duration of the Processing

The subject matter of the processing results from the contract. The duration of this DPA corresponds to the duration of the contract.

Clause 2

Specification of the Processing Details

- (a) Nature and purpose of processing of personal data by SOFTSHIP for the Customer are defined in the contract.
- (b) The processing of personal data shall be carried out exclusively within a Member State of the European Union (EU) or within a Member State of the European Economic Area (EEA). Each and every transfer of personal data to a state which is not a Member State of either the EU or the EEA requires the prior agreement of the Customer and shall only occur if the specific conditions of Articles 44 et seqq. GDPR have been fulfilled.
- (c) The categories of personal data and the categories of data subjects concerned are set forth in **Annex I**.

Clause 3

Technical and Organisational Measures

- (a) Before the commencement of processing, SOFTSHIP shall document the execution of the necessary Technical and Organisational Measures, and shall present these documented measures to the Customer for inspection. Upon acceptance by the Customer, the documented measures become the foundation of the DPA. Insofar as the inspection/audit by the Customer shows the need for amendments, such amendments shall be implemented by mutual agreement.
- (b) SOFTSHIP shall establish the security in accordance with Article 28 Paragraph 3 Point c, and Article 32 GDPR in particular in conjunction with Article 5 Paragraph 1, and Paragraph 2 GDPR. The measures to be taken are measures of data security and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the 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 to the rights and freedoms of natural persons within the meaning of Article 32 Paragraph 1 GDPR must be taken into account. The details are set forth in **Annex II**.
- (c) The Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for SOFTSHIP to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

Clause 4

Rights of the data subjects

- (a) SOFTSHIP shall support the Customer within its area of responsibility and as far as possible by means of appropriate technical and organisational measures in responding to requests from data subjects. SOFTSHIP must not on its own discretion respond to data subject requests concerning access to data, portability, rectification, erasure or the restriction of processing of data being processed on behalf of the Customer, but only on documented instructions from the Customer. Insofar as the data subject contacts SOFTSHIP directly, SOFTSHIP will immediately forward the data subject's request to the Customer.

- (b) Insofar as it is included in the scope of services, the erasure policy, 'right to be forgotten', rectification, data portability and access shall be ensured by SOFTSHIP in accordance with documented instructions from the Customer without undue delay.

Clause 5

Quality assurance and other duties of SOFTSHIP

In addition to complying with the rules set out in this DPA, SOFTSHIP shall comply with the statutory requirements referred to in Articles 28 to 33 GDPR; accordingly, SOFTSHIP ensures, in particular, compliance with the following requirements:

- (a) Appointed Data Protection Officer who performs his duties in compliance with Articles 38 and 39 GDPR: Dr Volker Wodianka, LL.M> (IT&T), CEO, zertifizierter Datenschutzbeauftragte , volker.wodianka@privacy-legal.de .The Customer shall be informed immediately of any change of Data Protection Officer.
- (b) Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. SOFTSHIP entrusts only such employees with the data processing outlined in this DPA who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. SOFTSHIP and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Customer, which includes the powers granted in this DPA and the contract, unless required to do so by law.
- (c) Implementation of and compliance with all Technical and Organisational Measures necessary for this DPA in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR.
- (d) The Customer and SOFTSHIP shall cooperate, on request, with the supervisory authority in performance of its tasks.
- (e) The Customer shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this DPA. This also applies insofar as SOFTSHIP is under investigation or is party to an investigation by a competent authority in connection with infringements to any Civil or Criminal Law, or Administrative Rule or Regulation regarding the processing of personal data in connection with the processing of this DPA.
- (f) Insofar as the Customer is subject to an inspection by the supervisory authority, an administrative or summary offence or criminal procedure, a liability claim by a data subject or by a third party or any other claim in connection with the data processing by SOFTSHIP under this DPA, SOFTSHIP shall make reasonable efforts to support the Customer.
- (g) SOFTSHIP shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within its area of responsibility is in accordance with the requirements of applicable data protection law and the protection of the rights of the data subject.
- (h) Verifiability of the Technical and Organisational Measures conducted by the Customer as part of the Customer's supervisory powers referred to in Clause 7 of this DPA.

Clause 6

Sub-processing

- (a) SOFTSHIP may commission sub-processors (additional contract processors) only after prior explicit written or documented consent from the Customer. The contractual agreement shall be presented to the Customer at the Customer's request, with the exception of business clauses not related to data protection.
- (b) The transfer of personal data to the sub-processor and the sub-processor's commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved. Compliance with and implementation of the technical and organisational measures at the sub-processor shall be inspected by SOFTSHIP in advance of the processing of personal data, taking into account the risk at the sub-processor, and then on a regular basis.
- (c) SOFTSHIP shall make the inspections' results available to the Customer upon request. SOFTSHIP shall also ensure that the Customer can exercise its rights under this contract (in particular its inspection rights) directly against the sub-processors. If the sub-processor provides the agreed service outside the EU/EEA, SOFTSHIP shall ensure compliance with EU Data Protection Regulations by appropriate measures.
- (d) The sub-processors listed in **Annex III** have been approved by the Customer.

Clause 7

Supervisory powers of the Customer

- (a) The Customer has the right, after consultation with SOFTSHIP, to carry out inspections or to have them carried out by an auditor to be designated in each individual case. It has the right to convince itself of the compliance with this

agreement by SOFTSHIP in its business operations by means of random checks during business hours, which are to be announced in good time.

- (b) SOFTSHIP shall ensure that the Customer is able to verify compliance with the obligations of SOFTSHIP in accordance with Article 28 GDPR. SOFTSHIP undertakes to give the Customer the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.
- (c) Evidence of such measures, which concern not only the specific DPA, may be provided by
 - Compliance with approved Codes of Conduct pursuant to Article 40 GDPR;
 - Certification according to an approved certification procedure in accordance with Article 42 GDPR;
 - 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)
 - 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).
- (d) The Supplier may claim remuneration for enabling Client inspections.

Clause 8

Communication in the case of infringements by SOFTSHIP

- (a) SOFTSHIP shall assist the Customer in complying with the obligations concerning the security of personal data, reporting requirements for data breaches, data protection impact assessments and prior consultations, referred to in Articles 32 to 36 of the GDPR. These include:
 - Ensuring an appropriate level of protection through Technical and Organizational Measures that take into account the circumstances and purposes of the processing as well as the projected probability and severity of a possible infringement of the law as a result of security vulnerabilities and that enable an immediate detection of relevant infringement events
 - The obligation to report a personal data breach immediately to the Customer
 - The duty to assist the Customer with regard to the Customer's obligation to provide information to the data subjects concerned and to immediately provide the Customer with all relevant information in this regard
 - Supporting the Customer with its data protection impact assessment
 - Supporting the Customer with regard to prior consultation of the supervisory authority
- (b) SOFTSHIP may claim compensation for support services which are not included in the description of the services and which are not attributable to failures on the part of SOFTSHIP.

Clause 9

Authority of the Customer to issue instructions

- (a) The Customer shall immediately confirm oral instructions (at the minimum in text form).
- (b) SOFTSHIP shall inform the Customer immediately if it considers that an instruction violates Data Protection Regulations. SOFTSHIP shall then be entitled to suspend the execution of the relevant instructions until the Customer confirms or changes them.

Clause 10

Deletion and return of personal data

- (a) Copies or duplicates of the data shall not be created without the knowledge of the Customer, with the exception of back-up copies as far as they are necessary to ensure orderly data processing, as well as data required to meet regulatory requirements to retain data.
- (b) After conclusion of the contracted work, or earlier upon request by the Customer, at the latest upon termination of the contract, SOFTSHIP shall hand over to the Customer or – subject to prior consent – destroy all documents, processing and utilization results, and data sets related to the DPA 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.



WISETECH GLOBAL GROUP

- (c) Documentation which is used to demonstrate orderly data processing in accordance with the DPA shall be stored beyond the contract duration by SOFTSHIP in accordance with the respective retention periods. SOFTSHIP may hand such documentation over to the Customer at the end of the contract duration to relieve SOFTSHIP of this contractual obligation.

Execution Page

Signed as an agreement.

Executed on behalf of **SOFTSHIP** by:

Signature of authorised signatory

Name

Name of authorised signatory (print)

Job title

Job title (print)

8-Jul-22

Execution date

Declaration by the Customer's signatories to this document

By signing this document, each authorised signatory, director or company secretary of the Customer represents and warrants that they have read this document, are a duly authorised representative of the Customer with full power and authority individually (in the case of a single signatory) or jointly (in the case of two signatories) to execute this document and bind the Customer to the terms of this document.

Executed by [**Insert name of Customer (Tax Number – eg ABN/VAT/GST or foreign equivalent)**] (Customer)
by:

its first or only authorised signatory/director:

its second authorised signatory/director (if required):

Signature

Signature

Name (print)

Name (print)

Job title (print)

Job title (print)

Execution date

Execution date

ANNEX I

DESCRIPTION OF TRANSFER

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

- Customers
- Potential Customers
- Subscribers
- Employees
- Suppliers
- Authorised Agents
- Contact Persons
- Other: Equipment related information; Attributes such as operating system, hardware version, equipment settings, browser type, language, time zone and IP-address; Log data: details about the type and manner how you have used our services; Cookies and similar technologies

Categories of data

The personal data transferred concern the following categories of data:

- Personal Master Data (Key Personal Data)
- Contact Data
- Key Contract Data (Contractual/Legal Relationships, Contractual or Product Interest)
- Customer History
- Contract Billing and Payments Data
- Disclosed Information (from third parties, e.g. Credit Reference Agencies or from Public Directories.
- Other: Employees of the Customer; Employees of Customers' customers (e.g. ship's crew); Other persons who travel on the concerned ships.

Nature and Purpose of the Processing operations

As set forth in the contract between the parties, as well as any appendices thereto.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Unless an alternate period is required by applicable local law or regulation, upon the earlier of: 1) the termination of the contract; or 2) the Customer providing written confirmation (text form is sufficient) to SOFTSHIP that the Customer no longer requires the data to be retained.

ANNEX II

Technical and organisational measures including technical and organisation measures to ensure the security of the data.

Description of the technical and organisational security measures implemented by the data importer:

(a) Confidentiality (Article 32 Paragraph 1 Point b GDPR)

- Physical Access Control
No unauthorised access to Data Processing Facilities, e.g.: magnetic or chip cards, keys, electronic door openers, facility security services and/or entrance security staff, alarm systems, video/CCTV Systems
- Electronic Access Control
No unauthorised use of the Data Processing and Data Storage Systems, e.g.: (secure) passwords, automatic blocking/locking mechanisms, two-factor authentication, encryption of data carriers/storage media
- Internal Access Control (permissions for user rights of access to and amendment of data)
No unauthorised Reading, Copying, Changes or Deletions of Data within the system, e.g. rights authorisation concept, need-based rights of access, logging of system access events
- Isolation Control
The isolated Processing of Data, which is collected for differing purposes, e.g. multiple Client support, sandboxing;
- Pseudonymisation (Article 32 Paragraph 1 Point a GDPR; Article 25 Paragraph 1 GDPR)
The processing of personal data in such a method/way, 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 organisational measures.

(b) Integrity (Article 32 Paragraph 1 Point b GDPR)

- Data Transfer Control
No unauthorised Reading, Copying, Changes or Deletions of Data with electronic transfer or transport, e.g.: Encryption, Virtual Private Networks (VPN), electronic signature; and
- Data Entry Control
Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted, e.g.: Logging, Document Management.

(c) Availability and Resilience (Article 32 Paragraph 1 Point b GDPR)

- Availability Control
Prevention of accidental or wilful destruction or loss, e.g.: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning; and
- Rapid Recovery (Article 32 Paragraph 1 Point c GDPR) (Article 32 Paragraph 1 Point c GDPR).

(d) **Procedures for regular testing, assessment and evaluation (Article 32 Paragraph 1 Point d GDPR; Article 25 Paragraph 1 GDPR)**

- Data Protection Management;
- Incident Response Management;
- Data Protection by Design and Default (Article 25 Paragraph 2 GDPR); and
- Order or Contract Control.
- No third party data processing as per Article 28 GDPR without corresponding instructions from the Client, e.g.: clear and unambiguous contractual arrangements, formalised Order Management, strict controls on the selection of the Service Provider, duty of pre-evaluation, supervisory follow-up checks.

(e) **Security measures**

- Data importer/sub-processor has implemented and shall maintain a security program in accordance with industry standards.
- More specifically, data importer/sub-processor's security program shall include:

Access Control of Processing Areas

Data importer/sub-processor implements suitable measures in order to prevent unauthorised persons from gaining access to the data processing equipment (namely telephones, database and application servers and related hardware) where the personal data are processed or used, including:

- Establishing security areas;
- Protection and restriction of access paths;
- Establishing access authorisations for employees and third parties, including the respective documentation;
- All access to the data centre where personal data are hosted is logged, monitored, and tracked; and
- The data centre where personal data are hosted is secured by a security alarm system, and other appropriate security measures.

Access Control to Data Processing Systems

Data importer/sub-processor implements suitable measures to prevent their data processing systems from being used by unauthorised persons, including:

- Use of adequate encryption technologies;
- Identification of the terminal and/or the terminal user to the data importer/sub-processor and processing systems;
- Automatic temporary lock-out of user terminal if left idle, identification and password required to reopen;
- Automatic temporary lock-out of the user ID when several erroneous passwords are entered, log file of events, monitoring of break-in-attempts (alerts); and
- All access to data content is logged, monitored, and tracked.

Access Control to Use Specific Areas of Data Processing Systems

Data importer/sub-processor commits that the persons entitled to use their data processing system are only able to access the data within the scope and to the extent covered by their respective access permission (authorisation) and that personal data cannot be read, copied or modified or removed without authorisation. This shall be accomplished by various measures including:

- Employee policies and training in respect of each employee's access rights to the personal data;
- Monitoring capability in respect of individuals who delete, add or modify the personal data;
- Release of data only to authorised persons, including allocation of differentiated access rights and roles; and
- Use of adequate encryption technologies; and control of files, controlled and documented destruction of data.

Availability Control

Data importer/sub-processor implements suitable measures to ensure that personal data are protected from accidental destruction or loss, including:

- Infrastructure redundancy; and
- Backup is stored at an alternative site and available for restore in case of failure of the primary system.

Transmission Control

Data importer/sub-processor implements suitable measures to prevent the personal data from being read, copied, altered or deleted by unauthorised parties during the transmission thereof or during the transport of the data media. This is accomplished by various measures including:

- Use of adequate firewall, VPN and encryption technologies to protect the gateways and pipelines through which the data travels; and
- As far as possible, all data transmissions are logged, monitored and tracked.

Input Control

Data importer/sub-processor implements suitable input control measures, including:

- An authorisation policy for the input, reading, alteration and deletion of data;
- Authentication of the authorised personnel;
- Protective measures for the data input into memory, as well as for the reading, alteration and deletion of stored data;
- Utilisation of unique authentication credentials or codes (passwords);
- Providing that entries to data processing facilities (the rooms housing the computer hardware and related equipment) are kept locked;
- Automatic log-off of user sessions that have not been used for a substantial period of time;
- Proof established within data importer/sub-processor's organization of the input authorisation; and
- Electronic recording of entries.

Separation of Processing for different Purposes

Data importer/sub-processor implements suitable measures to ensure that data collected for different purposes can be processed separately, including:

- Access to data is separated through application security for the appropriate users;
- Modules within the data importer/sub-processor's data base separate which data is used for which purpose, i.e. by functionality and function;
- At the database level, data is stored in separate databases for each customer with credentials that only access individual databases; and
- Interfaces, batch processes and reports are designed for only specific purposes and functions, so data collected for specific purposes is processed separately.

Documentation

Data importer/sub-processor will keep documentation of technical and organizational measures in case of audits and for the conservation of evidence. Data importer/sub-processor shall take reasonable steps to ensure that persons employed by it, and other persons at the place of work concerned, are aware of and comply with the technical and organizational measures set forth in this Appendix 2.

Monitoring

Data importer/sub-processor shall implement suitable measures to monitor access restrictions to data importer/sub-processor's system administrators and to ensure that they act in accordance with instructions received. This is accomplished by various measures including:

- Individual appointment of system administrators;
- Adoption of suitable measures to register system administrators' access logs to the infrastructure and keep them secure, accurate and unmodified for at least six months;
- Yearly audits of system administrators' activity to assess compliance with assigned tasks, the instructions received by the data importer/sub-processor and applicable laws;
- Keeping an updated list with system administrators' identification details (e.g. name, surname, function or organizational area) and tasks assigned and providing it promptly to data exporter upon request.

ANNEX III

List of Sub-Processors

Company	Address	Service description	Duration of processing
Affiliates of the Data Importer listed in Internal sub-processors data centre(s) table below	Refer Internal sub-processors data centre(s) table below	Data centres	For the term of Maintenance and License Agreement and the Product & Services Agreement and until tear down of Data Exporter's databases is complete
Microsoft Ireland Operations Limited Microsoft Pty Ltd	C/o Microsoft Operations Pte Ltd Dept. 551, Volume Licensing, 82 Cecil Street, #13-01 Frasers Tower, Singapore 069547 Republic of Singapore 1 Epping Road, North Ryde NSW 2113, Australia	Exchange - email SharePoint – collaboration tools Microsoft Teams – collaboration tools Defender ATP – threat protection Azure -IaaS, PaaS, SaaS	For the term of Maintenance and License Agreement and the Product & Services Agreement and until tear down of Data Exporter's databases is complete
Proofpoint Inc.	892 Ross Drive, Sunnyvale, CA 94085, USA	Email Filtering/quarantine	For the term of Maintenance and License Agreement and the Product & Services Agreement and until tear down of Data Exporter's databases is complete, however, duration of retention of any particular email is two weeks following receipt of each quarantined email
Microsoft Ireland Operations Limited	South County Business Park, One Microsoft Place, Carmanhall and Leopardstown, Dublin, D18 P521, Ireland	Off Site Storage	For the term of Maintenance and License Agreement and the Product & Services Agreement and until expiry of retentions period required thereafter
Aryaka Networks, Inc.	1800 Gateway Drive, Suite 200, San Mateo, CA 94404, USA	Network acceleration services over the public internet	For the term of Maintenance and License Agreement and the Product & Services Agreement and until tear down of Data Exporter's databases is complete

Internal Sub-Processors

Company Name	Country	Address
WiseTech Global Limited	Australia	Unit 3a, 72 O’Riordan Street, Alexandria NSW, Australia
WiseTech Global (US) Inc.	USA	1051 East Woodfield Road, Schaumburg IL 60173, USA
CargoWise GmbH	Germany	c/o Softship GmbH, Notkestraße 13-15, 22607, Hamburg, Germany
Equinix (Germany) GmbH	Germany	Vierenkamp 1, Hamburg, DE, 22453

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised):
 Processing on behalf of SOFTSHIP in accordance with the contract and prevailing privacy and data protection laws and regulation.