Data Processing Agreement

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 supplements the Master Service Agreement (**MSA**) between Softship and Customer.

This DPA replaces any prior terms and conditions on the same subject matter that have been agreed between the Parties, including any terms contained in the MSA or PSA.

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 PSA. The duration of this DPA corresponds to the duration of the PSA.

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 PSA.

(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**.

Clause3

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 PSA, 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 PSA, 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.

(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

Detlef Müller, Managing
Director

Name of authorised signatory (print) Job title

Hamburg 12. May
2022

Place 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 (**Customer**):

____

Address:

____

VAT-ID, Register No:

____

By its first or only authorised signatory/director:

By 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: (Please specify) N/A

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: (Please specify) N/A

Nature and Purpose of the Processing operations

As set forth in the PSA 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 PSA; 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: access 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: (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: 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: 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: Encryption, Virtual Private Networks (VPN), electronic signature

- Data Entry Control

  Verification, whether and by whom personal data is entered into a Data Processing System, is changed or deleted: Logging, Document Management.

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

- Availability Control

  Prevention of accidental or wilful destruction or loss: Backup Strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS), virus protection, firewall, reporting procedures and contingency planning

- 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: 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**

i. Data importer/sub-processor has implemented and shall maintain a security program in accordance with industry standards.

ii. 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, 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 (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, Irland	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
PlusServer GmbH (under condition of hosting services)	Hohenzollernring 72, 50672 Köln, Germany	Housing of the hosted systems	For the term of Maintenance and License Agreement and the Product & Services Agreement

			and until tear down of Data Exporter’s databases is complete
Atlassian. Pty Ltd	Level 6, 341 George Street Sydney NSW 2000 Australia	Product knowledge database	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 MSA and prevailing privacy and data protection laws and regulation.