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 01.08.2017 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 par 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.

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 extend 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 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:

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

The customer can also direct advertising contractions to Softship at:

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

Softship GmbH
Issued: 25.03.2019

Annexes:
1. Price list, issued 01.08.2017
2. Agreement for Contract Data Processing

Annex 1: Price List

1. Acquisition of Credits

The customer can acquire credits at any time via the software shop system. The price for one credit is € 0.45 net. Exclusively parcels in the following sizes can be acquired:

- 100 Credits = € 45.00
- 200 Credits = € 90.00
- 500 Credits = € 225.00
- 1,000 Credits = € 450.00
- 2,000 Credits = € 900.00

2. Forms of Payment

Softship exclusively offers the following forms of payment:

- PayPal
- Credit card (MasterCard, Visa, American Express)

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 prices apply:

- **Offer**: 5 Credits = € 2.25 (preparing an offer)
- **Port Call**: 50 Credits = € 25.00 (processing a port call)
- **Port Call based on Offer**: 45 Credits = € 20.25 (processing a port call which was generated from a preceding offer)
- **Support enquiry**: 25 Credits per unit of 15 minutes commenced = € 11.25 per unit of 15 minutes commenced (enquiry to Service Desk, solution finding by Softship)

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: Agreement for Contract Data Processing in accordance with Article 28 General Data Protection Regulation (GDPR)

between

- Principal -

and

Softship GmbH, Notkestrasse 15, 22607 Hamburg, Germany

- Contractor -

Both hereinafter also called “Party” or jointly “Parties”.

Preamble

This Agreement specifies the obligations of the contractual parties regarding data protection, which result from the Licence Agreement for the use of the software Softship.SAPAS (hereinafter “Contract”). It will be applicable for all activities which are in connection with the contract and where employees of the Contractor or representatives of the Contractor could come into contact with personal data of the Principal.

1. Subject matter and duration of the Contract Data Processing

(1) The subject matter, duration of the order, as well as the scope and type of data collection, processing or use arise from the contract.

2. Specification of the Order or Contract Details

(1) Purpose of data collection, processing or use

- Mapping of the business processes (of the user) within the application.
- Improvement of Softship.SAPAS:
  - Optimisation of user friendliness
  - Performance analyses
  - Usage behaviour
- Communication
  - Marketing
  - Changes with regard to guidelines and conditions
  - Display and measuring of advertisements and services.
- Promotion of safety
  - Investigation of suspicious activities or infringements of conditions, resp. guidelines

The undertaking of the contractually agreed Processing of 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 Data to a State which is not a Member State of either the EU or the EEA requires the prior agreement of the Client and shall only occur if the specific Conditions of Article 44 et seq. GDPR have been fulfilled.

(2) Type of data

The Subject Matter of the processing of personal data comprises the following data types/categories

- Customer and employee data: company, name, first name, address, telephone, e-mail, fax
- Business partners: company, name, first name, address, telephone, e-mail, fax; in the case of crew handling also the date and place of birth.
- 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

(3) Categories of Data Subjects

The Categories of Data Subjects comprise:

- Employees of the Principal
- Employees of Principal's customers (e.g. ship's crew)
- Other persons who travel on the concerned ships.

3. Technical and Organisational Measures

(1) Before the commencement of processing, the Supplier shall document the execution of the necessary Technical and Organisational Measures, set out in advance of the awarding of the Order or Contract, specifically with regard to the detailed execution of the contract, and shall present these documented measures to the Client for inspection. Upon acceptance by the Client, the documented measures become the foundation of the contract. Insofar as the inspection/audit by the Client shows the need for amendments, such amendments shall be implemented by mutual agreement.
(2) The Supplier 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.
(3) The Technical and Organisational Measures are subject to technical progress and further development. In this respect, it is permissible for the Supplier to implement alternative adequate measures. In so doing, the security level of the defined measures must not be reduced. Substantial changes must be documented.

4. Rectification, restriction and erasure of data

(1) The Supplier may not on its own authority rectify, erase or restrict the processing of data that is being processed on behalf of the Client, but only on documented instructions from the Client.
Insofar as a Data Subject contacts the Supplier directly concerning a rectification, erasure, or restriction of processing, the Supplier will immediately forward the Data Subject's request to the Client.
(2) 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 the Supplier in accordance with documented instructions from the Client without undue delay.

5. Quality assurance and other duties of the Supplier

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

a) Appointed Data Protection Officer, who performs his/her duties in compliance with Articles 38 and 39 GDPR. His/Her current contact details are always available and easily accessible on the website of the Supplier in the area "Imprint".
b) Confidentiality in accordance with Article 28 Paragraph 3 Sentence 2 Point b, Articles 29 and 32 Paragraph 4 GDPR. The Supplier entrusts only such employees with the data processing outlined in this contract who have been bound to confidentiality and have previously been familiarised with the data protection provisions relevant to their work. The Supplier and any person acting under its authority who has access to personal data, shall not process that data unless on instructions from the Client, which includes the powers granted in this contract, unless required to do so by law.

c) Implementation of and compliance with all Technical and Organisational Measures necessary for this Order or Contract in accordance with Article 28 Paragraph 3 Sentence 2 Point c, Article 32 GDPR [details in Appendix 1].
d) The Client and the Supplier shall cooperate, on request, with the supervisory authority in performance of its tasks.
e) The Client shall be informed immediately of any inspections and measures conducted by the supervisory authority, insofar as they relate to this Order or Contract. This also applies insofar as the Supplier 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 Order or Contract.
f) Insofar as the Client 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 Order or Contract data processing by the Supplier, the Supplier shall make every effort to support the Client.
g) The Supplier shall periodically monitor the internal processes and the Technical and Organizational Measures to ensure that processing within his 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 Client as part of the Client's supervisory powers referred to in item 7 of this contract.

6. Subcontracting

(1) Subcontracting for the purpose of this Agreement is to be understood as meaning 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 Supplier 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 Client's data, even in the case of outsourced ancillary services.

(2) The Principal agrees that the Contractor subcontracts third parties for the fulfilment of its contractually agreed services. This applies in particular for supporting services (e.g. computer centre, support, etc.).

The Client agrees to the commissioning of the following subcontractors on the condition of a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR:

- PlusServer GmbH, Hohenzollernring 72, 50672 Cologne (Webhosting)
- Pixelcreation GmbH, Jordanstraße 26a, 30173 Hannover (Concept, Webdesign und TYPO3-Realisation)

Changing the existing subcontractor are permissible when:

- The Supplier submits such an outsourcing to a subcontractor to the Client in writing or in text form with appropriate advance notice; and
- The Client has not objected to the planned outsourcing in writing or in text form by the date of handing over the data to the Supplier; and
- The subcontracting is based on a contractual agreement in accordance with Article 28 paragraphs 2-4 GDPR.

(3) The transfer of personal data from the Client to the subcontractor and the subcontractors commencement of the data processing shall only be undertaken after compliance with all requirements has been achieved.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the Supplier shall ensure compliance with EU Data Protection Regulations by appropriate measures. The same applies if service providers are to be used within the meaning of Paragraph 1 Sentence 2.

(5) Further outsourcing by the subcontractor requires the express consent of the Supplier (at the minimum in text form); all contractual provisions in the contract chain shall be communicated to and agreed with each and every additional subcontractor.

7. Supervisory powers of the Client

(1) The Client has the right, after consultation with the Supplier, 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 the Supplier in his business operations by means of random checks, which are ordinarily to be announced in good time.
(2) The Supplier shall ensure that the Client is able to verify compliance with the obligations of the Supplier in accordance with Article 28 GDPR. The Supplier undertakes to give the Client the necessary information on request and, in particular, to demonstrate the execution of the Technical and Organizational Measures.
(3) Evidence of such measures, which concern not only the specific Order or Contract, may be provided by compliance with approved Codes of Conduct pursuant to Article 40 GDPR;
(4) The Supplier may claim remuneration for enabling Client inspections.

8. Communication in the case of infringements by the Supplier

(1) The Supplier shall assist the Client 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:

a) 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.
b) The obligation to report a personal data breach immediately to the Client
c) The duty to assist the Client with regard to the Client's obligation to provide information to the Data Subject concerned and to immediately provide the Client with all relevant information in this regard.
d) Supporting the Client with its data protection impact assessment
e) Supporting the Client with regard to prior consultation of the supervisory authority

(2) The Supplier 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 the Supplier.

9. Authority of the Client to issue instructions

(1) The Client shall immediately confirm oral instructions (at the minimum in text form).
(2) The Supplier shall inform the Client immediately if he considers that an instruction violates Data Protection Regulations. The Supplier shall then be entitled to suspend the execution of the relevant instructions until the Client confirms or changes them.

10. Deletion and return of personal data

(1) Copies or duplicates of the data shall never be created without the knowledge of the Client, 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.
(2) After conclusion of the contracted work, or earlier upon request by the Client, at the latest upon termination of the Service Agreement, the Supplier shall hand over to the Client 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.
(3) Documentation which is used to demonstrate orderly data processing in accordance with the Order or Contract shall be stored beyond the contract duration by the Supplier in accordance with the respective retention

periods. It may hand such documentation over to the Client at the end of the contract duration to relieve the Supplier of this contractual obligation.

Annex to the ADV Agreement:

Technical and organisational Measures
of
Softship GmbH

---

1. Confidentiality (Article 32 Paragraph 1 Point b GDPR))
Access control
The following implementations have taken place, resp. are taking place, to control access by unauthorised persons to the data processing system used to process the personal data:

Computer Centre (CC)

1. The CC building, the surrounding premises and the accesses to the building are secured against unauthorised entry.
2. Access to the CC is only possible with an electronic security card and after a check by security personnel.
3. The accesses to the CC building are – with exception of the main entrance – always locked.
4. Security areas are permanently monitored.
5. Every visitor must register himself/herself.
6. All accesses to the CC building are under video surveillance. The cameras record every person entering the building.
7. There is a burglar alarm which automatically monitors possible accesses into the CC building (e.g. entrance doors, emergency exits, roof windows etc.) and reports break-ins and break-in attempts.

Offices

1. Alarm system
2. Manual locking system to the office
3. Light barriers / Motion detectors
4. Key provisions (Key issue book)
5. Identity check at reception
6. Careful selection of cleaning personnel
7. Security locks
8. Careful selection of security personnel

Access control
The following implementations have taken place so that data processing systems cannot be used by unauthorised persons.

1. Assignment of user rights
2. Individual issue of passwords
3. Authentication with user name / password
4. Use of central smartphone administration software (e.g. for external deletion of data)
5. Recording of system users
6. Use of VPN technology
7. Use of Intrusion-Detection-Software in the case of unauthorised system access
8. Application of a hardware firewall
9. Application of a software firewall
10. Preparation of user profiles
11. Use of anti-virus software
12. Assignment of user profiles to IT systems

Access control
The following points guarantee that the person authorised to use a data processing system can only access the data subject to its access rights, and that personal date cannot be read, copied, changed or removed unauthorised during processing, use and after storage.

1. Use of a system-internal authorization concept.
2. Number of administrators reduced to a “Minimum”.
3. Recording of accesses to applications, in particular when entering, changing or deleting data.
4. Administration of rights by system administrator.
5. Password guideline for the internal system incl. password length, password change.

Separation requirement
The following points guarantee that data collected for different purposes can be processed separately.

1. Physically separated storage on separate systems or data carriers
2. Use of an authorization concept
3. Provision of data sets with function attributes/data fields
4. Logical client separation (by software)
5. Separation of productive and test system
6 Determination of database rights

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.

2. Integrity (Article 32 Paragraph 1 Point b GDPR

The following points ensure that personal data cannot be read, copied, changed or removed unauthorized during electronic transfer or during their transport or storage on data carriers, and that it can be checked and determined at which point a transfer of personal data is intended through facilities for data transmission.

1. Use of dedicated lines and/or VPN tunnels
2. Encryption of data carriers, also on Laptops/Notebooks
3. Documentation of recipients of data and the time frames of the planned handover resp. agreed deletion periods
4. During physical transport: careful selection of transport personnel and vehicles.
5. Transfer of data where possible only in anonymized or at least pseudonymized form
6. Physical deletion of data carriers before re-use
7. With physical transport: secure transport containers/packaging
8. All employees are bound to data confidentiality pursuant to § 53 BDSG-new (Federal Data Protection Act)

Input control

It can be determined subsequently whether and by whom personal data were entered in data processing systems, were changed or removed.

1. Recording of input, change or deletion of data.
2. Traceability of input, change and deletion of data through individual user names (not user groups)
3. Assignment of rights for input, change and deletion of data on the basis of the authorization concept
4. Use of an overview, which shows with which applications which data can be input, changed or deleted.

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

The following positions ensure that personal data are protected against accidental destruction or loss.

1. Uninterruptible power supply (UPS)
2. Storage of data security at a safe, outsourced location
3. Fire and smoke detector systems
4. Alarm messages upon unauthorized access to server rooms
5. Testing of data recovery
6. Use of anti-virus software, which corresponds at least to state-of-the-art technology
7. Air-conditioning in server rooms
8. Protective socket board in server rooms
9. Fire extinguishing equipment in server rooms
10. Backup & Recovery concept
11. Emergency plan

.

Rapid Recovery (Article 32 Paragraph 1 Point c GDPR);

Detailed description:
The Contractor can recover data, data sets and virtual machines from data backups within short time.

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

- Data protection management;

Detailed description:
Implementation of latest patches and security instructions of the manufacturers as well as regular internal audit for revision and evaluation.

- Incident response management;

Detailed description:
A ticket based, electronic incident management tracking system is in use.

- Data Protection by Design and Default (Article 25 Paragraph 2 GDPR);

Detailed description:

Data access for support purposes only for qualified and carefully selected personnel.

5. Order 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.

1. Selection of the subcontractor under due care aspects (in particular with regard to data security)
2. Written instructions to the Contractor (e.g. through contract data processing contract) within the meaning of § 11 para. 2 BDSG
3. Subcontractor has ordered data protection officer
4. Effective control rights agreed vis-a-vis the Contractor
5. Prior check and documentation of the security measures agreed with the subcontractor
6. Employees' obligation in respect of data confidentiality pursuant to § 53 BDSG-new (Federal Data Protection Act)
7. Ongoing monitoring of the Contractor and its activities

Date

DIRK SELTER
Responsible Contractor (in block letters)

Signature Principal