Licence Terms
for ASP-Software
Softship.SAPAS

User:
Softship AG
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 pe-riod 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 calculat-ed 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 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 to § 5 BDSG (Federal Data Protection Act), 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).
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 contract data processing and Softship shall observe the legal requirements for contract data processing and instructions of the customer (e.g. compliance with deletion and blocking obligations, see § 11 BDSG = Federal Data Protection Act). The instructions must be notified on time and in writing. 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 the Annex to § 9 BDSG. 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 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) 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 AG
Attn. Mr. Dirk Selter
Notkestrasse 15
22607 Hamburg
Dirk.Selter@Softship.com

The customer can also direct advertising contractions to Softship at: Telephone:

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 AG
Status: 01.08.2017

Annexes:
1. Price list status 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 cots.

Annex 2: Agreement for Contract Data Processing

between

- Principal -

and

Softship AG, 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, Duration and Specification 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. In particular the following data are an essential part of data processing:

a) Type of data
- 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

b) 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

c) Circle of parties concerned
- Employees of the Principal
- Employees of Principal’s customers (e.g. ship‘s crew)
- Other persons who travel on the concerned ships.

(2) The term of this Annex depends on the term of the contract, provided that obligations above and beyond this do not result from the provisions of this Annex.

(3) The Contractor shall be entitled to process and use the Principal‘s data in anonymized form for own purposes and to combine these with other anonymous data, provided it is ensured that the combination cannot result in references for persons for the data.

§ 2 Application Area and Responsibility

(1) The Contractor processes personal data for order of the Principal. This comprises activities, which are clearly specified in the contract and the service description. Within the scope of this contract, the Principal is solely responsible for compliance with the legal requirements of the data protection acts, in particular for the legality of the data transfer to the Contractor, as well as for the legality of the data processing ("responsible authority" in the intentions of § 3 para. 7 BDSG = Federal Data Protection Act).

(2) The instructions are initially determined by the contract and can thereafter be changed, modified or replaced by the Principal in written form or text form by individual instructions (individual instruction). Instructions which go beyond the contractually agreed services, will be treated as application for change of service.

§ 3 Duties of the Contractor

(1) The Contractor may collect, process or use date of concerned persons only within the scope of the contract and the Principal's instructions.

(2) The Contractor shall design the internal organisation within his area of responsibility so that it satisfies the special requirements of data protection. He shall undertake technical and organisational measures for appropriate protection of Principal's data which satisfy the requirements of the Federal Data Protection Act (Annex to § 9 BDSG). These measures are determined in **Annex 1** to this Agreement. A change of the adopted security measures shall be reserved to the Contractor, however it must be ensured that the contractually agreed protection level is not fallen short of.

(3) Upon request, the Contractor shall supply Principal the information necessary for the overview pursuant to § 4g para. 2 sentence 1 BDSG (Federal Data Protection Act), if he cannot procure these himself.

(4) The Contractor guarantees that the employees engaged with the processing of Principal's data and other persons working for the Contractor are forbidden by obligation to collect, process or use the data unauthorized, (data confidentiality pursuant to § 5 BDSG = Federal Data Protection Act). Data confidentiality shall continue after termination of the order.

(5) The Contractor shall inform the Principal forthwith in the case of serious violations by Contractor or the persons employed by him within the scope of the order of the regulations for the protection of personal data of Principal or the specifications laid down in the contract. He shall undertake the necessary measures to secure the data and to reduce possible adverse consequences of those concerned and will agree on this with the Principal forthwith. The Contractor shall support the Principal with fulfilment of the duties on information pursuant to § 42a BDSG (Federal Data Protection Act).

(6) The Contractor shall give Principal the name of the contract partner for any data protection questions arising within the scope of the contract.

(7) The Contractor shall guarantee to comply with his duties pursuant to §§ 4f, 4g BDSG (§ 11 para. 2 No. 5 in conjunction with § 11 para. 4 BDSG Federal Data Protection Act), such as, e.g. his duty to appoint a data protection officer as prescribed by law.

(8) The Contractor shall not use the provided data for purposes other than fulfilment of the contract.

(9) The Contractor shall correct, delete or block contractual data when the Principal instructs this. The Contractor shall take on the destruction of data carriers and other materials conform to data protection, provided this is not already agreed in the contract. In special cases to be determined by Principal, such materials will be stored, resp. handed over.

(10) Data, data carriers as well as all other materials shall either be surrendered or deleted after end of the contract and upon Principal's request. If additional costs are incurred through deviating guidelines during the surrender or deletion of the data, the Principal shall be responsible for this; § 10 of the Licence Terms applies in this respect.

§ 4 Duties of the Principal

(1) The Principal shall inform Contractor forthwith and in full when he determines errors or irregularities regarding data protection regulations in the order results.

(2) The obligation to keep the public procedure index (index for everyone) pursuant to § 4g para. 2 sentence 2 BDSG lies with the Principal.

§ 5 Enquiries by Parties concerned

(1) If, due to applicable data protection laws, the Principal is obliged vis-à-vis an individual person, to issue information for the collection, processing or use of this person's data, the Contractor shall assist Principal with providing this information. This prerequisites that the Principal has requested the Contractor in writing or in text form for this purpose, and that the Principal will reimburse the Contractor the costs incurred through this support. The Contractor will not answer any requests for information and refer the concerned person to the Principal in this respect.

(2) If a concerned person makes requests for correction, deletion or blocking to the Contractor, the Contractor shall refer the concerned person to the Principal.

§ 6 Control Obligations

(1) The Principal shall convince himself, prior to taking up the data processing and thereafter regularly, of the technical and organizational measures of the Contractor and shall document the result. For this purpose he can, e.g.
- Gather information from Contractor,
- Have a possibly existing certificate from an expert submitted
- Or, after on-time agreement, have an expert third party obligated to professional secrecy, conduct a check during usual business hours and without interfering with operations, provided tis expert is not in a competitive relationship with the Contractor.

(2) The Contractor shall agree, upon written request by the Principal, to provide Principal all information and evidence which is necessary to execute the control within an appropriate period.

§ 7 Subcontractors

(1) 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 Contractor is obliged to inform the Principal in text form, with a period of at least two weeks ahead of commencement of activities, about new subcontractors and their activities.

(2) At the time of concluding this contract, the companies listed in the following are working as subcontractors for subservices for the Contractor and in this context process and/or use the Principal's data directly. For these subcontractors the consent for conducting these activities is deemed as issued.

- PlusServer GmbH, Welserstraße 14, 51149 Cologne (Webhosting)
- Pixelcreation GmbH, Jordanstraße 26a, 30173 Hannover

(3) If the Contractor issues orders to subcontractors, it is the duty of the Contractor to transfer his obligations from this contract to the subcontractors. Sentence 1 applies in particular to requirements in regard to confidentiality, data protection and data security between the contractual partners of this contract. A possible control by the Principal at the subcontractor will only be conducted in agreement with the Contractor. By written request, the Principal shall be entitled to receive information from the contractor about the data protection-relevant obligations of the subcontractor, if necessary through inspection of the relevant contractual documents.

(4) A duty of information about new subcontractors does not exist, when the Contractor, within the scope of supplementary work, assigns third parties to a main service, such as for example in the case of external personnel, postage or dispatch services or maintenance. The Contractor shall make agreements with this third party in the required scope to guarantee appropriate data protection.

§ 8 Information Requirements, Written Form Clause, Choice of Law

(1) Should Principal's data be endangered at Contractor's through seizure or confiscation, as a result of insolvency or composition proceedings or through other events or third party measures, the Contractor shall inform the Principal forthwith about this. The Contractor shall inform all those responsible forthwith that the sovereignty and ownership of the data lie exclusively with the Principal as "responsible authority" within the meaning of the Federal Data Protection Act.

(2) Changes and supplements to this Annex and all its components – including any assurances from the Principal – require a written agreement and the express reference that it is a change, resp. supplement of these provisions. This also applies to the waiver of this form requirement.

(3) In the case of any contradictions, the regulations of this Annex for data protection shall have precedence over the regulations of the contract. Should individual sections of this Annex be invalid this does not affect the effectiveness of the Annex for the remainder.

(4) German law applies.

	Softship AG
- Principal -	- Contractor -

Annex to the ADV Agreement:

Technical and organisational Measures
of
Softship AG

---

1. 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. CC is located in an unmarked building.
2. The CC building, the surrounding premises and the accesses to the building are secured against unauthorised entry.
3. Access to the CC is only possible with an electronic security card and after a check by security personnel.
4. The accesses to the CC building are – with exception of the main entrance – always locked.
5. Security areas are permanently monitored.
6. Every visitor must register himself/herself.
7. All accesses to the CC building are under video surveillance. The cameras record every person entering the building.
8. 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

2. 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

3. 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.

4. Transfer control

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 § 5 BDSG (Federal Data Protection Act)

5. 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.

6. Order control

It is insured that personal data, which are processed on behalf of third parties, can only be processed corresponding to instructions from the Principal.

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
5. Prior check and documentation of the security measures agreed with the subcontractor
6. Employees’ obligation in respect of data confidentiality pursuant to § 5 BDSG (Federal Data Protection Act)

3. Subcontractor has ordered data protection officer
4. Effective control rights agreed vis-a-vis the Contractor
7. Ongoing monitoring of the Contractor and its activities

7. Availability control

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

.

8. 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

Date

Responsible for the preparation (in block letters)

Signature of responsible person