NoSpamProxy Cloud Service Usage Agreement

Version: April 01, 2023

Subject of the Agreement

NoSpamProxy Cloud is a service from Net at Work GmbH that automatically processes incoming and outgoing e-mail sent to a mail domain and provides security functions. Depending on the contractually agreed scope, the service offers

- Spam and malware protection

- E-mail encryption

- Secure transmission of large files

- automatic attachment of mail signature and disclaimer texts

The respective scope of functions of the NoSpamProxy software, which Net at Work is using to provide the NoSpamProxy Cloud service, can be found in the current feature matrix or product sheet. The scope of functions described is not binding, but may change due to technical developments. In particular no right to use certain functions of the NoSpamProxy software is included in this usage agreement for NoSpamProxy Cloud.

Customer will buy and obtain the right to use our service for a certain number of mailboxes, as long as there is no other written agreement. Every e-mail-adress, including so-called function-addresses, to which a mailbox is assigned in the customers e-mail-system-will count as one mailbox. Mailboxes with multiple e-mail-addresses will count as one mailbox.

These terms and conditions apply to the contractual relationship between Net at Work and the Customer for use of the NoSpamProxy Cloud service. Use of the service is only permitted if the Customer has accepted these terms and conditions.

Conclusion of contract

The contract for the use of NoSpamProxy Cloud is concluded when the customer places an order with Net at Work, which can be in text form or online. If the Customer uses the service to provide services for his customers (end customers), he is obliged to agree the terms of this usage agreement with his customers as well.

Services provided by Net at Work

1. Net at Work operates NoSpamProxy Cloud to process the customer's incoming and outgoing mails on a cloud platform hosted in a German data center.

2. NoSpamProxy Cloud will analyze and evaluate emails according to the rule set selected by the customer and, depending on the result, forward them to the customer's mail infrastructure or reject them, encrypt or decrypt them and, if necessary, place mail attachments in quarantine folders.

3. the customer will get access data for a web interface. This provides access to functions with which he can search for processed mails, view metadata and manage mails in a customary, practice-oriented way.

4. Net at Work guarantees mail processing 24 hours a day, 7 days a week (7x24) with an availability of 99.9% calulated for a calendar year. This does not include announced service interruptions to a reasonable extent for maintenance purposes and interruptions due to extraordinary events beyond Net at Work's control such as natural disasters, earthquakes, large-scale power failures or Internet failures.

Net at Work regularly updates the Service with new versions to provide up-to-date protection against emerging cyber threats.

6. service limitation - per mailbox the sending of mails is limited to 480 recipients per hour and 8.000 recipients in 24 hours. The receiving of mails per mailbox is limited to 3,600 mails per hour. If this value is exceeded, Net at Work limits outgoing mail to this value and rejects all emails exceeding the value.

Obligations of the customer

1. the customer assures not to misuse the service (e.g. for sending spam mails, malware, viruses, links to harmful content) and to take reasonable measures in his IT infrastructure to ensure IT security (updated virus scanners, regular updates/patches of operating systems, use of firewalls, ...) If mails that are classified as harmful or spam are detected in the Customer's outgoing mail flow, Net at Work may stop processing of mails or take other suitable measures of its own choice to prevent damage to the Customer and the NoSpamProxy Cloud platform (e.g. blocklists of IP addresses).

2. order data processing - By using the NoSpamProxy Cloud service, the Customer agrees to the corresponding data processing agreement for NoSpamProxy Cloud and appoints Net at Work as contractor for mail processing.

3. Managed Certificates - If the Customer uses the Managed Certificates option, the Customer authorizes Net at Work to order and manage certificates for the Customer's employees at affiliated trust centers on the Customer's behalf, to perform required validations and to enter on behalf of the Customer into contractual terms and conditions specified by the respective trust center. The Customer will make sure to comply with the respective terms of use for certificates.

General Terms and Conditions of Business (AGB)

Upon conclusion of a contract for the use of NoSpamProxy Cloud, the General Terms and Conditions of Net at Work shall apply in addition to the provisions made here and in the version valid at the time of conclusion of the contract. Deviating provisions confirmed in writing by Net at Work when the order is placed shall take precedence over this usage agreement and the General Terms and Conditions.

The English translation of this agreement is only for the purpose of convenience. In doubt, the German version of this agreement shall prevail.

Data Processing Agreement

between

the customer designated in the order of NoSpamProxy Cloud software service

(Responsible person within the meaning of the DS-GVO, hereinafter referred to as "**Client**")

and

Net at Work GmbH

Am Hoppenhof 32 A

33104 Paderborn

(data processor within the meaning of the DS-GVO, hereinafter referred to as **"Contractor"**)

Preamble

This data processing contract (AV contract) specifies the data protection obligations of the contracting parties.

§ 1 Definitions

The definitions according to Art. 4 DS-GVO, § 2 UWG and § 2 TMG as well as § 2 BDSG (neu) apply. In case of contradicting regulations in the articles or paragraphs, the definitions in the order of DS-GVO, UWG and TMG shall apply. The following definitions also shall apply:

1. **Anonymisation**:

Process in which personal data are irreversibly altered, either by the data controller alone or in cooperation with another party, in such a way that the data subject cannot be identified either directly or indirectly afterwards. (Source: DIN EN ISO 25237)

2. **Subcontractors**:

A service provider contracted by the Contractor, whose services and/or work are required by Contractor in order tor provide the services described in this contract to the Client.

3. Contracted Data Processing:

Contracted Data Processing shall mean the processing of personal data by a contractor on behalf of the Client.

4. Instruction:

Instruction shall refer to a written instruction by the Client to the Contractor to handle personal data in a specific manner (e.g. anonymization, blocking, deletion, publication). The instructions are initially set out in a main contract and may subsequently be amended, supplemented or replaced by the Client in writing by individual instructions (individual instruction).

§ 2 Subject of the Contract

- Analysis of incoming and outgoing e-mails from employees of the Client to detect spam, malware and other security risks, as well as the encryption and decryption of e-mails - preamble extend.

The Contractor shall be granted access to the following personal data (by the fact that the Customer shall have the incoming e-mails delivered to him by disclosing an IP address of the Contractor and shall send him outgoing e-mails from his mail server) and the Customer shall allow the Contractor to process the following personal data respectively:

- Name

- E-mail address

- Subject

- Content of e-mails and attachments

- Date of dispatch and receipt

- Encryption and signing status of the e-mail

- IP-addresses

- additional e-mail metadata for 32Guards

- Certificates (only NoSpamProxy Managed Certificates)

- Files attached to e-mails which can contain person-related data (only NoSpamProxy Sandbox)

Affected groups of individuals:

- All employees of the organisations with E-Mail-account or access to E-Mail-accounts

- All persons sending e-mails to the organisation of the Client

Client is aware that the NoSpamProxy SaaS service is a largely standardized check of mails for viruses, malware and spam, encryption and other forms of checking and conversion. This is carried out in accordance with the state of the art using a set of rules agreed with the Client. The data is stored for a period of 3 months, used exclusively for analysis purposes and automatically and permanently deleted after this period. When using the Sandbox option, the content of ile attachments is transferred for analysis and then immediately deleted. There is no frequent or individual access to data of the Client by the Contractor. Instructions of the Client regarding individual mails or groups of

mails are not supported due to the large volume and the customary market nature of the service. The statutory right of the Client to instruct the Contractor remains unaffected. The expenses incurred by the Contractor from Client instructions shall be remunerated separately to the Contractor by the Client at market conditions.

§ 3 Responsibility

1. Within the framework of this contract, Client is responsible for compliance with the statutory provisions, in particular for the lawfulness of data processing (while maintaining data secrecy (Art. 28 DS-GVO) ("responsible party" in the sense of Art. 4 No. 7 DS-GVO)

2) The contents of this Data Processing Agreement shall apply accordingly if test or maintenance of automated procedures or data processing equipment is carried out by Contractor and access to personal data cannot be excluded.

3. Client as well as the Contractor must ensure that the persons authorised to process personal data are bound by adequate confidentiality agreements or are subject to an appropriate statutory duty of secrecy. For this purpose, all persons who can access personal data of the client according to the contract must be bound to data secrecy and instructed about their data protection obligations. Each party is responsible for the obligation of its own personnel. In addition, the persons employed must be informed that the data secrecy will continue to exist after the termination of their employment.

The Customer and the Contractor shall be responsible for compliance with the relevant data protection laws with regard to the data to be processed.

§ 4 Duration of the contract

1. the term of this Data Processing Agreement shall be based on the term of the existing agreements between Client and Contractor, unless the provisions of this Agreement state otherwise.

2. the contracting parties are aware that without a valid DP agreement, e.g. at the end of the present contractual relationship, no (further) processing may be carried out.

3. the right to terminate without notice for good cause remains unaffected.

4. notices of termination require to be in text form to be effective

§ 5 Client‘s Right to Issue Instructions

1. Data is handled exclusively within the framework of the agreements made and, if necessary, in accordance with the documented instructions of the Client. Excluded from this are circumstances in which the Contractor is required to process the data otherwise for legal reasons. In such situations, the Contractor shall, to the extend possible, inform the Client of any enforcement or ruling before processing begins. Within the scope of the description of data processing in this agreement, the Client reserves the right to issue comprehensive instructions on the type, scope and procedure of data processing, which he can concretize by means of individual instructions.

2. Client's instructions must be issued in text form and have to be documented by the Client. The Client shall pay separately for the time and effort required to implement the instructions at market conditions.

3. Changes to the object of processing and procedural changes are covered by the Client's Right to issue instructions and must be documented accordingly. In case of a substantial change of the Data Processing, Contractor has the right to object. If the Client insists on the change despite the Contractor's objection, the Contractor shall be entitled to a regular right of termination with regard to the DP agreement affected by the instruction and the components of the corresponding main contract affected by the DP agreement. If the Contractor refuses to implement the change, the Client shall also be entitled to an ordinary right of termination. If the contract is terminated, the Contractor must continue to provide the contractually agreed services for the remaining term of the contract.

§ 6 Place of Data Processing

1. The Contractor shall provide the contractual services in the European Union (EU) or the European Economic Area (EEA). In the case of service provision that is carried out in parts by subcontracted processors in a third country, the Contractor shall guarantee compliance with the relevant requirements of the GDPR and provide evidence of this upon request (conclusion of the EU standard contractual clauses).

§ 7 Obligations of the Contractor

1. Contractor may only collect, process or use data within the scope of the order and the instructions of the Client.

2. Contractor will design the internal organisation within his area of responsibility in such a way that it meets the special requirements of data protection. He will take technical and organizational measures to adequately secure the Customer's data against misuse and loss, which comply with the requirements of the relevant data protection regulations; the Contractor must provide evidence of these measures to the Customer and, if necessary, to supervisory authorities upon request. This proof includes in particular the implementation of the measures resulting from Art. 32 DSGVO. The technical and organisational measures are subject to technical progress and further development. In this respect, the contractor is permitted to implement alternative, demonstrably adequate measures. It must be ensured that the contractually agreed level of protection is not undercut. Significant changes must be documented. A description of these technical and organisational measures is provided in Annex 2 to this contract.

3. the contractor shall provide the customer on his request with a meaningful and up-to-date data protection and security concept for this order processing.

4. the contractor himself keeps a list of the processing activities taking place at his premises for the processing in the sense of Art. 30 DS-GVO. Upon request, he shall provide the principal with the information necessary for the overview in accordance with Art. 30 DS-GVO. Furthermore, he shall make the list available to the supervisory authority on request.

5. Contractor shall support Client assessing data protection impacts (Datenschutzfolgeabschätzung) with all the information available to him in return for remuneration in line with market conditions. If prior consultation of the competent supervisory authority is necessary, the Contractor shall also support the Client in this respect.

6. Contractor is obliged to treat confidentially all knowledge of foreign secrets or a trade or business secret as well as data security measures of the customer obtained within the scope of the contractual relationship.

7. Contractor shall inform the Client immediately in the event of violations by the Contractor or the persons employed by him within the scope of the agreement against regulations for the protection of personal data of the customer or the stipulations made in the contract. He shall take the necessary measures to secure the data and to minimise possible adverse consequences for the persons concerned and shall consult with the Client without delay. Alerts will be done via E-Mail and sent to the address communicated by Client in the service order and stored in the Contractor's CRM system. The Contractor shall support the Client in fulfilling the information obligations towards the relevant competent supervisory authority or those affected by a violation of the protection of personal data in accordance with Art. 33, 34 DS-GVO. Contractor is not authorized to inform relevant supervisory authorithies without prior consent of the Client.

If a person affected should contact the Contractor directly for the purpose of correcting or deleting his data, the Contractor shall forward this request to the Client without delay.

9. if the Client is obliged to provide information to a data subject under applicable data protection laws with regard to the collection, processing or use of data of this person, the Contractor shall support the Client in providing this information, provided the Client has requested the Contractor to do so in writing.

The Contractor shall inform the Client immediately of any checks and measures by the supervisory authorities or if a supervisory authority investigates the Contractor.

11. the Contractor shall immediately inform the Client if, in his opinion, an instruction issued by the Client violates statutory provisions. The Contractor is entitled to suspend the execution of the relevant instruction until it is confirmed or amended by the Client.

12. if the data of the Client are endangered at the Contractor by seizure or confiscation, by insolvency or composition proceedings or by other events or measures of third parties, the contractor has to inform the customer immediately. The Contractor shall immediately inform all persons responsible in this connection that the sovereignty and ownership of the data lie exclusively with the Customer as the person responsible within the meaning of the DS-GVO.

The Contractor shall not use the data provided for any purposes other than the performance of the contract and shall not use any means of processing that have not been approved by the Customer in advance.

14. Contractor does not store any patient data on systems which are outside the authority of the Client or which are not subject to the protection against seizure.

15) If the Contractor is obliged by Union or national law to process the data in any other way, the Contractor shall notify the Client of these legal requirements prior to processing. The notification shall be omitted if the relevant national law prohibits such notification by reason of an important public interest.

16) The fulfilment of the above-mentioned obligations shall be controlled and documented by the Contractor and shall be proven in a suitable manner to the Client upon request.

§ 8 Obligations of the Client

1) The Client alone is responsible for assessing the permissibility of data processing and for safeguarding the rights of the persons concerned. Within his area of responsibility, the Client shall ensure that the legally necessary conditions are created (e.g. by obtaining declarations of consent for the processing of the data) so that the Contractor can provide the agreed services without infringing the law.

2. the Client must inform the Contractor immediately and completely if he discovers errors or irregularities with regard to data protection regulations when checking the results of the order.

3. the Client is responsible for data protection law with regard to the procedures used by the Contractor and approved by the Client for the automated processing of personal data and - in addition to the Contractor's own obligation - also has the obligation to keep a register of processing activities.

4. Client is obliged to inform the supervisory authority or the persons affected by a violation of the protection of personal data pursuant to Art. 33, 34 DS-GVO.

5. Client shall determine the measures to be taken to delete the stored data after completion of the contract, either by contract or by instruction.

6. Client is obliged to treat as confidential all knowledge of company secrets and data security measures of the Contractor acquired within the framework of the contractual relationship.

7. Client ensures that the requirements resulting from Art. 32 DS-GVO regarding the security of processing are complied with on his part. This applies in particular to remote accesses by the Contractor to the customer's databases.

8) If the Client issues individual instructions that go beyond the contractually agreed scope of services, the client shall bear the costs incurred as a result. If the agreed scope of services is exceeded, a separate written agreement must be made in advance.

§ 9 Rights of Control of the Client

1. Client has selected the Contractor because he is providing sufficient guarantees that he will carry out appropriate technical and organisational measures in such a way that the processing is carried out in accordance with the requirements of the DSGVO and ensures the protection of the rights of the data subject. He shall document the result of his selection. For this purpose, he may, for example, take into account data protection-specific certifications or data protection seals and test marks, obtain written information from the contractor, have an attestation from an expert presented to him, or, after registering in good time during normal business hours without disrupting operations, convince himself personally or through a competent third party, who may not be in a competitive relationship with the contractor, of compliance with the agreed regulations.

2. If the Contractor or the persons employed by him within the scope of the data processing violate regulations for the protection of personal data of the Client or the stipulations made in the contract, related examination can also be carried out without timely notification. Any disruption of the Contractor's operations should also be avoided as far as possible.

3. The Contractor shall support controls by means of regular checks by the Client with regard to the execution or fulfilment of the contract, in particular of compliance with and, if necessary, the necessary adjustment of regulations and measures for the execution of the order. In particular, the Contractor agrees to provide the Client on written request within a reasonable period of time with all

information required to carry out a check. The expenses incurred by the Contractor to perform such a check shall be remunerated separately by the Client at market conditions.

Client shall inform the Contractor immediately and in full if the Client discovers errors or irregularities with regard to data protection regulations during the check.

§10 Subcontractors

1. Contractor provides the service using an internationally recognized hyperscaler (computing service provider). The Contractor is entitled to make use of other subcontractors without the prior explicit written or general written approval of the Customer, provided that this does not violate any assurances from this contract, in particular §§ 6 and 7. Upon request, the Contractor shall provide the Customer with a list of current subcontractors.

The following provisions shall apply accordingly to the subcontractor as well as to all other subcontractors subsequently employed.

In the event of general written approval, Contractor shall always inform the Client of any intended change in the use or replacement of subcontractors, which shall give the Client the opportunity to object to such changes. If the Client refuses to give its approval for reasons other than good cause, the Contractor may terminate the agreement at the time of the intended use of the subcontractor.

4. Client agrees that the Contractor may use affiliated companies of the Contractor to perform his services. In this case, however, each subcontractor (affiliated company) must be notified to the Client in writing prior to the assignment, so that the Client can prohibit the assignment if there are important reasons.

At the time of conclusion of this Agreement, the companies listed in Annex 1 to this Agreement shall act as subcontractors for partial services for the Contractor and shall also directly process and/or use the Client’s data in this connection. Such subcontractors shall be deemed to have given their consent to act.

6. Contractor must conscientiously select subcontractors in particular with regard to their suitability to fulfill the technical and organisational measures agreed between Client and Contractor.

7. Where, for the purposes of this Agreement, Contractor is authorised to use the services of a subcontractor in order to carry out certain processing activities on behalf of the Client, the same obligations shall be imposed on that subcontractor by way of a contract as are laid down in this Agreement between Client and Contractor, in particular with regard to the requirements of confidentiality, data protection and data security between the parties to this Agreement and the Client's rights of control and inspection as described in this DP Agreement Furthermore, sufficient guarantees must be provided that the appropriate technical and organisational measures are carried out in such a way that the processing is carried out in accordance with the requirements of the DS-GVO.

8. By written request, the Client shall be entitled to obtain information from the Contractor about the subcontractor's obligations relevant to data protection, if necessary also by inspecting the relevant contractual documents.

9. If the subcontractor does not comply with his data protection obligations, the Contractor shall be liable to the Client for compliance with the obligations of that subcontractor.

§ 11 Correction, Restriction of Processing, Deletion of Data

1. During the contract period, the Contractor shall correct, delete or block the data subject to the contract only upon instruction of the Customer.

2. After completion of the contractual work - or earlier upon request by the Customer - the Contractor shall delete or destroy data files in accordance with data protection regulations upon instruction by the Customer, unless there is a legal obligation to retain the data. The record of the deletion shall be submitted upon request.

3. If additional costs are incurred after termination of the contract due to the release or deletion of the data, these shall be borne by the Customer.

4. The Contractor shall retain documentation that serves as evidence of the proper processing of data in accordance with the order in accordance with the respective retention periods beyond the end of the contract. The Contractor may hand them over to the Customer at the end of the contract in order to relieve the Customer.

5. The Customer may at any time, i.e. both during the term and after termination of the Agreement, request the correction, deletion, restriction of processing (blocking) and surrender of data by the Contractor, as long as the Contractor has the possibility to comply with this request.

6. The Contractor shall correct, delete or block the data subject to the contract if the Customer so instructs. Insofar as a data subject should contact the Contractor directly for the purpose of correcting or deleting his/her data, the Contractor shall forward this request to the Customer without delay.

7. If it is not possible for the Customer to take back the data, the Customer shall inform the Contractor in writing in due time. The Contractor shall then be entitled to delete personal data on behalf of the Customer.

8. In the case of test and reject materials, an individual order regarding deletion is not required, these must be deleted.

§ 12 Right of Retention

The right of retention, for whatever legal reason, of the contractual data as well as of any existing data carriers is excluded.

§13 Liability

Client and Contractor are jointly liable for damages caused by processing not in accordance with the DSGVO to the affected person.

2 The Contractor is exclusively liable for damage caused by a processing carried out by him in which

a. he has not complied with the obligations resulting from the DSGVO and specifically imposed on contract data processors or

b. he acted in disregard of the lawfully given instructions of the Client; or

c. he has acted against the lawfully given instructions of the Client.

3. insofar as the Client is obliged to pay damages to the person affected, Client reserves the right to claim damages against the Contractor.

4. However, in the internal relationship between Client and Contractor, the Contractor shall only be liable for the damage caused by processing if 1. he has not complied with his obligations specifically imposed on him by the DS-GVO or 2. he has acted in disregard of the client's lawfully issued instructions or in contravention of such instructions.

5. further liability claims according to the general laws remain unaffected.

§ 14 Written form clause

Amendments and supplements to this agreement and all of its components - including any assurances given by the contractor - require a written agreement and the express indication that these regulations are to be amended or supplemented. The written form requirement also applies to the waiver of this formal requirement.

§ 15 Choice of Law, Place of Jurisdiction, Translation

1. This agreemend shall be governed under German law.

2. Place of jurisdiction is Paderborn.

3. The English translation of this agreement is only for the purpose of convenience. In doubt, the German version of this agreement shall prevail.

Annex 1 to the Data Processing Agreement

Net at Work has contracted the following sub-processors under the above DP relationship:

Sub-Processor : Bitdefender SRL.

Data transferred	Purpose	Place of processing
Metadata of e-mails and files	Detection of Spam and Malware in e-mails	EU and USA under application of EU Standard Contractual Clauses

Unterauftragnehmer: Amazon Web Services Inc. (AWS)

Data transferred	Purpose	Place of processing
Metadata of e-mails and files	Detection of Spam and Malware in e-mails	EU

Annex 2 to the Data Processing Agreement

General technical and organizational measures

Technical and organizational measures, subcontractors

1. The Contractor and the Customer agree on the specific technical and organizational security measures set forth in paragraph (5) in accordance with Section 64 BDSG (new).

2. The Contractor shall be entitled to replace these measures with adequate alternatives, provided that the security level of the measures set forth in paragraph (5) is not undercut in the process. Significant changes shall be documented.

3. Upon request, the Contractor shall provide the Customer with the information required to comply with its obligation to control the order and shall make the relevant evidence available. Due to the Customer's control obligation prior to the start of data processing and during the term of the order, the Contractor shall ensure that the Customer can satisfy itself of compliance with the technical and organizational measures taken. For this purpose, the Contractor shall provide the Customer with evidence of the implementation of the technical and organizational measures pursuant to Section 64 BDSG (new) upon request. Proof of the implementation of such measures, which do not only relate to the specific order, can also be provided by submitting a current audit certificate, reports from independent bodies (e.g. auditors, auditing, data protection officers, IT security department, data protection auditors) or a suitable certification by IT security or data protection audit (e.g. according to BSI Grundschutz).

4. The Customer may, after written notification by a third party bound to professional secrecy, inspect the adequacy of the measures for compliance with the technical and organizational requirements of the data protection laws relevant to the commissioned data processing at the Contractor's business premises during normal business hours at any time without disrupting operations.

5. The following specific technical and organizational measures shall apply:

   a. Physical Access control

   Unauthorized persons shall be denied access to data processing systems with which personal data are processed or used.

   b. System Access control

   Data processing systems are prevented from being used by unauthorized persons. Access can only be gained via an access control system. In addition, other technical security devices such as firewalls are used in the communication chain. Where technically possible and economically justifiable, suitable encryption technologies are used for this purpose.

c. Data Access control

Those authorized to use a data processing system can only access the data subject to their access authorization, and personal data cannot be read, copied, modified or removed without authorization during processing, use or after storage. Where technically possible and economically justifiable, suitable encryption technologies shall be used for this purpose.

d. Transfer control

Personal data cannot be read, copied, altered, or removed without authorization during electronic transmission or while being transported or stored on data media, and it is possible to verify and determine to which entities personal data is intended to be transmitted by data transmission equipment. Where technically possible and economically justifiable, suitable encryption technologies shall be used for this purpose.

e. Input control

It is possible to check and establish retrospectively whether and by whom personal data have been entered into data processing systems, modified or removed.

f. Order control

Personal data processed on behalf of a client can only be processed in accordance with the client's instructions. The data submitted for processing shall be processed in accordance with the statutory provisions only within the framework of the instructions of the respective client and, in particular, shall not be disclosed to unauthorized third parties. The framework of instructions is clearly specified in particular by the contract for data processing on behalf of the client, taking into account the mandatory contents pursuant to Section 62 (5) BDSG, and furthermore by the application description of the service programs. The same shall apply to order-related information; it shall be provided exclusively to the Customer or within the scope of the Customer's instructions. Exceptions to the specific instruction framework apply to processing for technical reasons, e.g. for internal data backup.

g. Availability control

Personal data is protected against accidental destruction or loss.

Numerous data security measures ensure that personal data and other data worthy of protection are protected against accidental destruction or loss. In addition, uninterruptible power supply facilities are available to the data centers in the event of a power outage.

h. Separation Control

Data collected for different purposes can be processed separately.

The principle of separation of functions is in place in all key areas; this means that all departments involved in data processing are functionally, organizationally and spatially separated. The principle of functional separation is also largely implemented within the organizational units; data worthy of protection is only made available to employees to the extent that it is absolutely necessary for the assigned lawful performance of tasks. To ensure this, defined rights profiles are assigned to the various functional areas and administered centrally.

6. The Contractor shall only award contracts to subcontractors with the prior express written approval of the Customer. Services which the Contractor uses from third parties as an ancillary service to support the execution of the order, for example telecommunications services and maintenance, shall not be deemed to be services provided by subcontractors within the meaning of this provision. However, the Contractor shall be obligated to enter into appropriate and legally compliant contractual agreements and to take control measures to ensure the protection and security of the Customer's data even in the case of externally contracted ancillary services.

7. f the Contractor engages subcontractors, it shall ensure that the contractual agreements with the subcontractor are designed in such a way that the level of data protection at least corresponds to the agreement between the Customer and the Contractor and that all legal and contractual obligations are observed.

8. Upon written request of the Contractor, the Customer shall be entitled to receive information about the essential content of the contract and the implementation of the data protection-relevant obligations of the subcontractor.