Data Processing Agreement according to Art. 28 GDPR

between

BMS Büro & Marketing – Service e.K., Königstraße 80 in 70173 Stuttgart (Data Processor - hereinafter referred to as **Processor**) and the

Customer (Controller - hereinafter referred to as **Controller**) (collectively hereinafter referred to as "**the Parties**")

1. Subject and Duration of the Contract

The Processor performs, on behalf of the Controller, the processing of personal data for the duration of the contract period based on the main contract.
The subject of the processing is defined in the main contract and in Annex 1 Service Agreement to this DPA.
The scope of services resulting from the main contract may – depending on the services booked – include one or more of the processing operations listed in Annex 1 Service Agreement, without thereby redefining the service obligations.

The duration of this contract corresponds to the term of the service agreement. The termination periods of the office services contract apply.

2. Specification of the Contract Content

(1) Nature and purpose of the intended data processing/type of data/categories of data subjects

The nature and purpose of the processing, the type of personal data, and the categories of data subjects are specified in Annex 1 Service Agreement

3. Technical and Organizational Measures

(1) The Contractor must document the implementation of the technical and organizational measures outlined prior to the award of the contract and necessary for the processing, especially regarding the specific contract execution, before the start of processing and submit them to the Client for review. Upon acceptance by the Controller, the documented measures become the basis of the contract. If the Controller 's examination/audit reveals a need for adjustment, it shall be implemented by mutual agreement.

(2) The Contractor must ensure security according to Art. 28 para. 3 lit. c, 32 GDPR, especially in conjunction with Art. 5 para. 1, para. 2 GDPR. Overall, the measures to be taken are security measures to ensure an appropriate level of protection

regarding confidentiality, integrity, availability, and resilience of the systems. In this regard, the state of the art, implementation costs, the nature, scope, and purposes of processing, as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR, must be considered. Details see Annex 2 technical and organizational measures.

(3) The technical and organizational measures are subject to technological progress and further development. In this respect, the Processor is permitted to implement alternative adequate measures. However, the security level of the defined measures must not be undercut. Significant changes must be documented.

4. Correction, Restriction, and Deletion of Data

(1) The Processor may not independently correct, delete, or restrict the processing of data processed on behalf, but only in accordance with documented instructions from the Controller. If a data subject directly contacts the Processor regarding this matter, the Processor shall promptly forward this request to the Controller.

(2) If included in the scope of services, deletion concept, right to be forgotten, correction, data portability, and information must be ensured by the Processor directly in accordance with documented instructions from the Controller.

(3) The Controller grants the Processor - deviating from (1) of this paragraph 4 - permission, where applicable and concerning telephone services, to store and, within the scope of the service agreement, modify or process the caller data recorded by the Processor, as necessary to properly provide the desired services.

5. Quality Assurance and Other Obligations of the Processor

In addition to complying with the provisions of this contract, the Processor ensures compliance with legal obligations according to Art. 28 - 33 GDPR; in this regard, it guarantees compliance with the following requirements:

a) The Processor undertakes to appoint a data protection officer or, if not legally obligated, another contact person responsible for data protection matters. The Processor ensures that the person possesses the necessary qualifications and expertise. The contact details of the data protection officer or another responsible person can be found in Annex 3 Data Protection Officer

b) Maintaining confidentiality according to Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR. The Processor only employs personnel bound to confidentiality when performing the work, who have been familiarized with the relevant data protection provisions. The Processor and any person subordinate to the Processor who has access to personal data may process this data exclusively in accordance with the Controller's instructions,

including the powers granted in this contract, unless they are legally obligated to process it.

c) Implementation and compliance with all technical and organizational measures required for this contract according to Art. 28 para. 3 sentence 2 lit. c, 32 GDPR. Details see Annex 2 technical and organizational measures.

d) The Controller and the Processor cooperate with the supervisory authority in fulfilling their tasks upon request.

e) Promptly informing the Controller of inspection activities and measures of the supervisory authority relating to this contract. This also applies if a competent authority investigates the processing of personal data by the Processor in the context of order processing.

f) If the Controller is subject to an inspection by the supervisory authority, an administrative or criminal proceeding, the liability claims of an affected person or a third party, or any other claim related to order processing by the Processor, the Processor shall support the Controller to the best of its ability.

g) The Processor regularly monitors internal processes as well as technical and organizational measures to ensure that processing within its area of responsibility complies with the requirements of applicable data protection law and ensures the protection of the rights of the data subject.

h) Demonstrability of the technical and organizational measures taken to the Controller within the framework of its control rights according to paragraph 7 of this contract.

6. Subcontracting Relationships

(1) Subcontracting relationships within the meaning of this provision are those services directly related to the provision of the main service. Excluded from this are ancillary services that the Processor may use, such as telecommunications services, postal/transport services, maintenance and user 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 systems. However, the Processor is obliged to take appropriate and legally compliant contractual agreements and control measures for outsourced ancillary services to ensure data protection and data security of the Controller's data.

(2) The Processor may only engage subcontractors (further data processors) with the prior express written or documented consent of the Controller.

a) ☐ Subcontracting is prohibited.

b) ☐ Outsourcing to subcontractors or

☒ Changing the existing subcontractor

is permissible, provided that:

- the Processor notifies the Controller of such outsourcing to subcontractors in writing or in text form sufficiently in advance and
- the Controller does not object to the planned outsourcing in writing or in text form to the Processor by the time the data is handed over, and
- a contractual agreement is based on Art. 28 para. 2-4 GDPR.

(3) The transfer of personal data of the Controller to the Subcontractor and its initial activities are only permitted once all conditions for subcontracting are met.

(4) If the subcontractor performs the agreed service outside the EU/EEA, the Processor ensures data protection compliance through appropriate measures. The same applies if service providers within the meaning of point (1) sentence 2 are to be used.

(5) Any further subcontracting by the Subcontractor requires the explicit consent of the main Processor (at least in text form); all contractual arrangements in the contractual chain must also be imposed on the further Subcontractor.

(6) Subcontractors engaged by the Processor are listed in Annex 4 Subcontractors.

7. Audit Rights of the Controller

(1) The Controller has the right, in consultation with the Processor, to conduct audits or have them carried out by an auditor to be named in individual cases. The Controller has the right to verify compliance with this agreement by the Processor in its business operations through spot checks, which are usually to be announced in good time.

(2) The Processor ensures that the Controller can verify compliance with the Processor's obligations under Article 28 GDPR. The Processor undertakes to provide the necessary information to the Controller upon request and to demonstrate the implementation of the technical and organizational measures.

(3) Proof of such measures, which do not only concern the specific order, can be provided by:

☐ Compliance with approved codes of conduct pursuant to Art. 40 GDPR;

☐ Certification under an approved certification procedure pursuant to Art. 42 GDPR;

☒ Current attestations, reports or excerpts from reports from independent entities (e.g., auditors, audit departments, data protection officers, IT security departments, data protection auditors, quality auditors);

☐ Suitable certification by IT security or data protection audit (e.g., according to BSI basic protection).

(4) For facilitating audits by the Controller, the Processor may claim compensation. The compensation claim must be agreed with the Controller upon notification of audits.

8. Notification of Breaches by the Processor

(1) The Processor shall support the Controller in complying with the obligations regarding the security of personal data as mentioned in Art. 32 - 36 of the GDPR, including obligations for data breach notifications, data protection impact assessments, and prior consultations. This includes, among other things:

a) Ensuring an appropriate level of protection through technical and organizational measures that consider the circumstances and purposes of processing, as well as the predicted likelihood and severity of a potential breach due to security vulnerabilities and enable the immediate identification of relevant breach incidents.

b) Obligation to promptly report personal data breaches to the Controller.

c) Obligation to support the Controller in fulfilling its obligation to inform data subjects and to provide all relevant information to the Controller immediately in this context.

d) Supporting the Controller in conducting data protection impact assessments.

e) Assisting the Controller in prior consultations with the supervisory authority.

(2) The Processor may claim remuneration for support services under point (1) d) and e), as well as support services not included in the service description or not attributable to misconduct by the Processor.

9. Controller's Authority to Issue Instructions

(1) The Controller shall promptly confirm verbal instructions upon request (at least in text form).

(2) The Processor shall immediately inform the Controller if it believes that an instruction violates data protection regulations. The Processor is entitled to suspend the implementation of the corresponding instruction until it is confirmed or changed by the Controller.

(3) In the event of a change or long-term impediment of the Controller, the Controller shall promptly notify the Processor of a successor or representative authorized to issue instructions.

10. Deletion and Return of Personal Data

(1) Copies or duplicates of the data shall not be created without the knowledge of the Controller. Exceptions to this are backup copies, to the extent necessary to

ensure proper data processing, as well as data required to comply with legal retention obligations.

(2) Upon completion of the contractually agreed work or earlier upon request by the Controller - at the latest upon termination of the service agreement - the Processor shall hand over to the Controller all documents, processing and usage results created, as well as data sets acquired in connection with the contractual relationship or shall destroy them in a data protection-compliant manner with prior consent. The same applies to test and reject material. The deletion protocol shall be provided upon request.

(3) Documentation serving as evidence of proper and orderly data processing shall be retained by the Processor in accordance with the respective retention periods beyond the end of the contract. He may hand them over to the Controller upon termination of the contract for his relief.

(4) Personal data of the data subjects shall only be stored for as long as necessary to fulfil the purpose of the respective data processing operation and to the extent that there are no legal retention periods opposing deletion.

11. Liability

The processor is liable for damages caused to the controller due to breaches of this agreement or relevant data protection laws by the processor or any subcontractors. The liability provisions of the contract for office services (AGB) apply to damages.

12. Miscellaneous

(1) Should the controller's or its customers' data be endangered by attachment or confiscation by the Processor or subcontractor, by insolvency or comparison proceedings, or by other events or measures of third parties, the Processor shall immediately inform the controller. The Processor shall promptly inform all parties involved in this context that the ownership of the data lies with the controller.

(2) Changes and additions to this contract and all its components - including any assurances from the Processor - require a written agreement and explicit indication that it is an amendment or addition to these conditions. This also applies to waiving this formal requirement.

(3) Should individual provisions of this agreement be or become wholly or partially invalid, this shall not affect the validity of the remaining provisions. The wholly or partially invalid provision shall be replaced by a provision that comes as close as possible to the purpose of the invalidity and which the parties would have agreed to had they had known of the invalidity. The same applies if a gap is revealed in this agreement.

(4) German law applies.

(5) The place of jurisdiction is Stuttgart.

The document also references several annexes containing additional agreements or information:

Annex 1: service agreement

Annex 2: technical and organizational measures (TOM)

Annex 3: data protection officer

Annex 4: subcontractors

Annex 1 - Service Agreement

1. Subject and Duration of the Contract

- Opening incoming mail, scanning its contents, and forwarding via email, fax, or similar.
- Forwarding incoming faxes via email, fax, or similar.
- Providing office support services such as typing and order processing.
- Capturing and storing data of personally appearing individuals and transmitting it via email or similar means or by handing out printouts.
- Telephone service in the form of answering calls on behalf of the Controller, transferring calls to agreed destinations, and capturing and storing caller data for transmission (via email, fax, SMS, by handing out printouts, or input/storage in the online platform managed and provided by the Controller).

2. Specification of the Contract Content

(1) Nature and Purpose of the Intended Data Processing

The type of processing of personal data is determined by the scope of services booked according to the main contract - also see under point 1: Subject and Duration of the Contract.

The purpose of processing personal data by the Processor for the Controller is to outsource office and telephone service tasks to support the Controller's business processes.

The provision of contractually agreed data processing takes place exclusively in a member state of the European Union or another contracting state of the Agreement on the European Economic Area. Any transfer to a third country requires the prior consent of the Controller and may only take place if the specific conditions of Articles 44 et seq. of the GDPR are met. The appropriate level of protection in Germany is determined by an adequacy decision of the Commission (Art. 45 para. 3 GDPR).

(2) Type of Data

- Personal master and contact data (including name, address, email address, telephone number, date of birth, etc.)
- Phone calls (conversation content, date, time)
- Incoming faxes
- Incoming mail of all kinds
- Contractual, billing, and booking data
- Other unforeseeable data

(3) Categories of Affected Persons

- Employees/retirees of the Controller
- Customers of the Controller
- Prospects of the Controller
- Callers of the Controller
- Other unforeseeable categories of affected persons

Annex 2 - Technical and Organizational Measures

1. Confidentiality (Art. 32 Para. 1 lit. b GDPR)

Access Control:

- ☐ Alarm system
- ☐ Automatic access control system
- ☐ Locking system with code lock
- ☐ Biometric access barriers
- ☐ Photoelectric sensors/motion detectors
- ☒ Key management (key issuance, etc.)
- ☐ Visitor logging
- ☐ Careful selection of security personnel
- ☒ The reception desk is always staffed during opening hours
- ☒ Securing building shafts
- ☐ Chip card/transponder locking system
- ☒ Manual locking system
- ☐ Video surveillance of entrances
- ☒ Security locks
- ☐ Personnel control at gatehouse/reception
- ☒ Careful selection of cleaning personnel
- ☐ Mandatory carrying of authorization badges

Access and Access Control

- ☒ Assignment of user rights
- ☒ Password assignment
- ☒ Authentication with username/password
- ☒ Enclosure locks
- ☐ Blocking external interfaces (USB)
- ☒ Encryption of data storage in laptops/notebooks
- ☒ Creation of user profiles
- ☐ Authentication with biometric methods
- ☒ Assignment of user profiles to IT systems
- ☒ Use of VPN technology
- ☒ Use of software firewall
- ☒ Use of hardware firewall

- ☒ Use of anti-virus software
- ☒ Use of intrusion detection systems
- ☐ Use of spyware & PUA software
- ☒ Development of authorization concepts
- ☒ Minimum number of administrators
- ☒ Logging of accesses to applications, especially for input, modification, and deletion of data
- ☒ Physical destruction of data carriers before reuse
- ☒ Use of paper shredders or service providers (preferably with data protection seal)
- ☒ Encryption of data carriers
- ☒ "Clean Desk" policy
- ☒ Manual desktop lock instruction
- ☒ Minimum password lengths and password managers
- ☐ Encryption of smartphone contents
- ☒ Encryption of mobile data storage devices
- ☐ Use of central smartphone administration software (e.g., for remote data deletion)
- ☒ Rights management by system administrator
- ☒ Password policy including password length, password change
- ☒ Secure storage of data carriers
- ☒ Proper destruction of data carriers (DIN 32757)
- ☐ Logging of destruction
- ☒ Appropriate data shredders (at least level P4)
- ☒ Always up-to-date software versions
- ☒ Automatic desktop lock

Purpose Limitation/Separation Control

- ☒ Physically separate storage on separate systems or data carriers
- ☒ Development of authorization concepts
- ☒ Logical Controller separation (software-based)
- ☐ Encryption of datasets processed for the same purpose

☐ Assigning purpose attributes/data fields to datasets

☐ For pseudonymized data: separation of the mapping file and storage on a separate, secured IT system

☒ Determination of database rights

☐ Separation of productive and test systems

Input Control

☒ Logging of data input, modification, and deletion

☐ Creation of an overview showing which applications can input, modify, and delete data

☐ Traceability of data input, modification, and deletion by individual usernames (not user groups)

☐ Retention of forms from which data has been transferred to automated processing

☒ Assignment of rights to input, modify, and delete data

☐ Other:

2. Integrity (Art. 32 Para. 1 lit. b GDPR)

Transmission Control

☒ Establishment of dedicated lines or VPN tunnels

☐ Creation of an overview of regular retrieval and transmission processes

☒ Documentation of data recipients and the timeframes for planned transfer or agreed deletion deadlines

☒ For physical transport: careful selection of transport personnel and vehicles

☒ Email encryption (S/MIME)

☐ For physical transport: secure transport containers/packaging

☐ Transfer of data in anonymized or pseudonymized form

☐ Encryption of external data carriers upon transfer (CDs, USB sticks, etc.)

☒ State-of-the-art encryption of data transmissions

☒ Work instructions for employees

3. Availability and Resilience (Art. 32 Para. 1 lit. b GDPR)

Availability Control

- ☒ Uninterruptible power supply (UPS)
- ☐ Air conditioning in server rooms
- ☒ Devices for monitoring temperature and humidity in server rooms
- ☒ Protected power strips in server rooms
- ☐ Fire and smoke detection systems
- ☒ Fire extinguishers in front of server rooms
- ☐ Alarm notification for unauthorized access to server rooms
- ☒ Creation and continuous monitoring of a backup & recovery concept
- ☒ Data recovery testing
- ☒ Creation of an emergency plan
- ☒ Storage of data backups at a secure, off-site location
- ☒ Server rooms not located below sanitary facilities
- ☐ In flood-prone areas: server rooms above the waterline
- ☒ Conducting penetration tests
- ☒ Additional backups stored at particularly secure locations
- ☒ Regular IT maintenance (updates, patches)
- ☒ Separate partitions for operating systems and data
- ☒ Use of hard disc mirroring
- ☒ Incident response management

4. Procedure for Regular Review, Assessment, and Evaluation (Art. 32 Para. 1 lit. d GDPR; Art. 25 Para. 1 GDPR)

Data Protection Management

- ☒ Central documentation of all procedures and regulations for data protection with access for employees as needed/authorized
- ☒ Internal/external data protection officer
- ☒ Use of software solutions for data protection management
- ☒ Employees trained and obligated to confidentiality/data secrecy
- ☒ Regular sensitization of employees, at least annually
- ☒ The organization complies with the information obligations under Art. 13, 14 GDPR

☒ Formalized process for handling inquiries from data subjects is available

☒ Data protection impact assessment (DPIA) is conducted as needed

Incident Response Management

☒ Documentation of security incidents and data breaches

☒ Use of antivirus software and regular updates

☒ Documented procedure for handling security incidents communicated to employees in writing

☒ Documented process for detecting and reporting security incidents/data breaches (including reporting obligations to supervisory authority)

☒ Involvement of the data protection officer in security incidents and data breaches

☒ Use of spam filters and regular updates

☒ Use of firewall and regular updates

Data Protection-friendly Defaults (Art. 25 Para. 2 GDPR)

☒ Privacy by default adhered to

☒ Privacy by design adhered to

☒ No more personal data collected than necessary for the respective purpose

Contractual Control (Art. 28 GDPR):

☒ Selection of Processor with due diligence (especially regarding data security)

☒ Prior examination and documentation of security measures taken by the Processor

☒ Written instructions to the Processor (e.g., through a data processing agreement) pursuant to Art. 28 et seq. EU-GDPR

☒ Obligation of the Processor's employees to maintain data secrecy

☒ Processor has appointed a data protection officer (if required)

☒ Ensuring data destruction after completion of the contract

☒ Effective control rights against the Processor agreed upon

☒ Ongoing review of the Processor and their activities

☒ Contractual penalties for violations

☒ Checking compliance with contractors

☒ Ensuring the destruction of data after completion of the order

☒ Regulation on the use of additional

☒ Obligation of the Contractor's employees to maintain confidentiality/data secrecy

☒ Conclusion of the necessary agreement on order processing (adequacy decision or EU standard contractual clauses)

Annex 3 - Data Protection Officer

Data Protection Officer/Contact Person of the Processor:

secom IT GmbH

Address: Nienburger Str. 9a, 27232 Sulingen

Tel.: 04271 9473 800

Email: datenschutz@secom-it.de

Annex 4 – Subcontractors

Company Name	Contact Information	Services Provided
ecos GmbH & Co. KG	Mergenthalerallee 10-12 65760 Eschborn	Newsletter distribution, handling of large inquiries across multiple ecos locations, management of telephone directory entries with Deutsche Telekom, management of email accounts
Partner Business Center (centers affiliated with the ecosGroup)	See Website www.ecos-office.com/de/standorte/	Depending on the services booked by the Controller.
GesMIT mbH	Bruchbrunnenstraße 19 66123 Saarbrücken	Provision, support, and maintenance for telephone management system as well as SMS or fax transmission
Locaboo GmbH	Balanstr. 73 | Haus 12 81541 München	Room planning
LIONWARE GmbH	Isestraße 123 20149 Hamburg	Identity verification
microPLAN IT-Systemhaus GmbH	Spatzenweg 2 48282 Emsdetten	Maintenance and support for telephone system
ZDS Bürosysteme Vertrieb & Service GmbH	Schlattgrabenstraße 24 72141 Walddorfhäslach	Maintenance and support for office printing and scanning solutions
Systempartner Stuttgart IT-Service GmbH	Schulze-Delitzsch-Straße 41 70565 Stuttgart	Maintenance and support for other IT systems
Tedesco Dienstleistungen	Taunusstraße 54 71032 Böblingen	Building and office cleaning with waste separation and waste disposal