Date: 04.09.2026

Data Processing Agreement

(remberg Software)

1. Subject Matter, Definitions and Order of Precedence

1.1 This Data Processing Agreement (hereinafter referred to as "**DPA**") governs the rights and obligations under data protection law pursuant to Art. 28 of the Regulation (EU) 2016/679 - General Data Protection Regulation (hereinafter referred to as "**GDPR**"), insofar as the Contractor (as processor within the meaning of Art. 4 No. 8 GDPR) processes personal data on behalf of the Client (as controller within the meaning of Art. 4 No. 7 GDPR) as part of the provision of services in accordance with the offer, order, order form, or service description and general terms and conditions (hereinafter jointly referred to as "**Main Agreement**"). As the controller, the Client bears sole responsibility for the lawfulness of the transfer of personal data to the Contractor and for the lawfulness of the data processing.

1.2 The definitions of the Main Agreement apply accordingly to the DPA (including annexes), with the following exception: the customer is also referred to as the "**Client**" and remberg is also referred to as the "**Contractor**". Insofar as the terms "data processing" or "processing" (of data) are used in the DPA, the definition of processing within the meaning of Art. 4 No. 2 GDPR shall apply.

1.3 In the event of contradictions or ambiguities between the provisions of the main part of the DPA and the provisions of the annexes to the DPA, the provisions of the main part of the DPA shall take precedence. In the event of inconsistencies or ambiguities between the provisions of the DPA and the provisions of the Main Agreement, the provisions of the DPA shall take precedence insofar as data protection issues are concerned.

2. Description of Data Processing and Term

2.1 The details of the data processing, in particular the purposes for which the personal data is processed on behalf of the Client and the categories of personal data, are set out in **Annex 1** to this DPA. The details of the provision of services are regulated in the Main Agreement.

2.2 The term of the DPA corresponds to the term of the Main Agreement. The DPA ends automatically upon termination of the Main Agreement.

3. Technical and Organizational Measures

3.1 The Contractor shall take all necessary technical and organizational measures in its area of responsibility in accordance with Art. 32 GDPR to protect personal data. The technical and organizational measures are specified in **Annex 2**. The Client has reviewed the technical and

organizational measures in **Annex 2** and considers them to be appropriate within the meaning of Art. 32 GDPR, taking into account the nature, scope, circumstances and purposes of the data processing.

3.2 If a review by the Client reveals a need to adapt the technical and organizational measures listed in **Annex 2**, the Parties shall mutually agree on an adaptation of the technical and organizational measures by suitable means.

3.3 The technical and organizational measures listed in Annex 2 are subject to technical progress and further development. The Contractor is entitled to implement other adequate measures, whereby the security level of the technical and organizational measures listed in **Annex 2** may not be undercut. The Client must be notified of any significant changes in writing (text form is sufficient).

4. Right of Instruction of the Client

4.1 The Contractor shall process personal data exclusively in accordance with the Client's instructions, unless the Contractor is legally obliged to process the data differently; in this case, the Contractor shall inform the Client of this legal obligation prior to processing, unless the law in question prohibits such information due to an important public interest.

4.2 The Client's instructions shall be governed by (a) the provisions of the Main Agreement, (b) the DPA and (c) other instructions of the Client for the provision of the contractual services in accordance with the provisions of the Main Agreement, each of which must be documented in writing (text form is sufficient). The Client shall immediately confirm verbal instructions in writing or in text form.

4.3 The Contractor shall inform the Client immediately if it is of the opinion that an instruction violates applicable data protection law. The Contractor shall be entitled to suspend the execution of the instruction until the Client has confirmed or amended the instruction.

5. Rights of Data Subjects

5.1 As the controller, the Client is responsible for safeguarding the rights of data subjects (Art. 15 et seq. GDPR). The Contractor shall inform the Client if data subjects assert their data subject rights against the Contractor in connection with the data processing.

5.2 The Contractor shall support the Client in its area of responsibility and as far as possible through suitable technical and organizational measures in the fulfilment and satisfaction of data subject rights. In doing so, the Contractor shall not fulfill data subject rights on its own authority, but only on the documented instructions of the Client. The Contractor may demand reasonable remuneration for supporting the Client in the fulfillment of data subject rights.

5.3 Insofar as this is possible within the scope of the functionalities of the systems made available in the context of the provision of services, the Client shall provide information on, correct, delete or restrict personal data itself.

6. Reports of Security Breaches

6.1 The Contractor shall design the data processing, its operating procedures and the associated processes, systems and facilities in such a way that the Contractor can detect, recognize and report possible breaches of the protection of personal data.

6.2 The Contractor shall notify the Client immediately if there is a breach of the protection of personal data within the meaning of Art. 4 No. 12 GDPR that has led to the destruction, loss, alteration or unauthorized disclosure of or access to personal data.

6.3 The Contractor shall notify the Client in a way that enables the Client to comply with its legal obligations, in particular pursuant to Art. 33 and 34 GDPR. The Contractor shall document the relevant information and make it available to the Client for further measures.

7. Obligations of the Contractor

7.1 In order to maintain confidentiality, the Contractor shall only use persons for the processing of personal data who have been obligated to maintain confidentiality or who are subject to an appropriate statutory duty of confidentiality and who have been familiarized with the data protection provisions relevant to them.

7.2 The Contractor shall support the Client to the extent necessary and appropriate according to the type of data processing in ensuring compliance with legal obligations, in particular in carrying out data protection impact assessments in accordance with Art. 35 GDPR and in necessary consultations with the competent supervisory authorities in accordance with Art. 36 GDPR.

7.3 The Contractor's data protection officer can be reached at the following contact details:

DataCo GmbH
Dachauer Strasse 65
80335 Munich
Germany

+49 89 7400 45840
www.dataguard.de

7.4 The Contractor shall inform the Client immediately of any measures and inspections by a supervisory authority or other official inquiries in connection with data processing. Insofar as the Client is itself subject to measures and inspections by a supervisory authority, the Contractor shall support the Client to the necessary and reasonable extent in responding and provide it with all relevant information in this context. The Contractor may demand reasonable remuneration for supporting the Client.

7.5 The Contractor shall regularly review its internal processes and the technical and organizational measures (see Annex 2) to ensure that data processing in its area of responsibility is carried out in accordance with the requirements of (a) the applicable data protection regulations and (b) the provisions of the DPA.

7.6 The Contractor processes personal data both (a) within the European Union (hereinafter referred to as the "**EU**") or the contracting states of the Agreement on the European Economic Area (hereinafter referred to as the "**EEA**") and (b) outside the EU or the EEA. Data processing outside the EU or the EEA is only carried out by the Contractor if the special protection provisions of Art. 44 et seq. GDPR are met in order to ensure an adequate level of data protection (e.g. adequate level of data protection on the basis of an adequacy decision by the European Commission pursuant to Art. 45 GDPR and/or by concluding EU standard contractual clauses pursuant to Art. 46 para. 2 lit. c and d in conjunction with Art. 47 GDPR).

8. Data Processing by Subcontractors

8.1 Data processing by a subcontractor within the meaning of this Section 8 exists if the Contractor commissions other contractors (hereinafter referred to as "**Sub-Processors**") in whole or in part with the processing of personal data as part of the provision of services in accordance with the Main Agreement. This does not include any ancillary services used by the Contractor (e.g. telecommunications, transportation, cleaning or security services). However, the Contractor shall also take appropriate contractual provisions and control measures when outsourcing ancillary services in order to ensure data protection and data security.

8.2 The Sub-Processors currently used by the Contractor are listed in **Annex 3**. The Client has taken note of the Sub-Processors listed in Annex 3 and agrees to the use of these Sub-Processors in the context of the provision of services.

8.3 The commissioning of new or the modification of existing Sub-Processors in accordance with **Annex 3** is permissible if the Contractor notifies the Client of the deployment of the Sub-Processor in advance in writing (text form is sufficient) and the Client does not object within a reasonable period, which may not exceed thirty (30) days, whereby an objection by the Client is always only possible for good cause. If no objection is raised, the commissioning of or change

to the Sub-Processor shall be deemed to have been approved by the Client. If the Client objects for good cause and the parties fail to reach an amicable solution with regard to the Sub-Processor concerned, the Contractor may, at its discretion, provide the service without the intended change or – if the provision of the service without the intended change is unreasonable for the Contractor – terminate the service to the Client without notice to the end of the quarter within two (2) weeks of receipt of the objection. In the event of termination, the service shall be provided until the end of the service without the intended change.

8.4 Access to personal data by the Sub-Processor may only take place if the Contractor has concluded an agreement with the Sub-Processor in accordance with Art. 28 GDPR, which contains data protection provisions that are fundamentally comparable with the provisions of this DPA. In particular, the Contractor shall ensure that sufficient guarantees exist for the implementation of the technical and organizational measures.

8.5 If the Sub-Processor provides the agreed service outside the EU or the EEA, Section 7.6 shall apply accordingly.

8.6 The Contractor shall remain responsible to the Client for the fulfillment of the obligations of the contracted Sub-Processor.

9. Control Rights of the Client

9.1 The Client shall be entitled to verify compliance with (a) the applicable data protection provisions and (b) the provisions of the DPA, in particular with regard to technical and organizational measures. In accordance with this Section 9, the Contractor shall provide the Client in its area of responsibility with all information necessary to prove compliance with the applicable data protection provisions and shall enable and support checks on data processing in the context of the subsequent data processing.

9.2 If, in individual cases, it is necessary to verify (a) compliance with the applicable data protection provisions or (b) the provisions of the DPA, the Client shall have the right, after consultation with the Contractor, to carry out or have carried out corresponding inspections at the Contractor's respective business premises where the data processing takes place, either itself or by suitable inspectors to be determined in individual cases who are obliged to maintain confidentiality. The review shall be limited to the processing of personal data and shall be carried out without avoidable disruption to the Contractor. The Contractor shall be entitled to object to the selection of the auditor for good cause (e.g. unreliability or competitive relationship with the Contractor). Unless there are urgent, objectively justified reasons, which must be documented accordingly by the Client, inspections shall be carried out on the Contractor's business premises after reasonable advance notice of at least one (1) month during the Contractor's normal business

hours and at most every twelve (12) months. The Contractor may demand reasonable remuneration for assistance in carrying out the inspection. The time and effort required for an inspection for the Client is generally limited to one (1) day per calendar year.

9.3 The parties agree that audits of the Client and the provision of information and evidence by the Contractor shall primarily take place in such a way that the Contractor provides the Client with current attestations, reports or report extracts from independent third parties (e.g. auditors, internal audit, data protection officer, IT security department, data protection or quality auditors) or corresponding certifications through IT security or data protection audits.

10. Deletion of Personal Data and Return of Data Carriers

10.1 No copies or duplicates of personal data are made without the Client's knowledge. Excluded from this are backup copies, insofar as they are required for proper data processing, as well as data required to fulfill statutory retention obligations.

10.2 Upon termination of the DPA (or prior to such termination if instructed to do so by the Client), the Contractor shall return to the Client all personal data in its possession or, at the Client's discretion, destroy such data in accordance with data protection regulations, unless the Contractor is required by law to continue storing the data. The deletion or destruction shall be confirmed to the Client in text form.

10.3 The parties agree that the data shall be automatically deleted in accordance with Section 10.2 upon termination of the Main Agreement, unless the Client requests the Contractor to surrender its data from receipt of the notice of termination until no later than 14 days prior to the termination of the Main Agreement. The confirmation period pursuant to Section 10.2 shall apply accordingly.

11. Final Provisions

11.1 Amendments and supplements to the DPA must be made in writing (text form with electronic signature is sufficient). This also applies to the waiver of the written form requirement. If amendments to the DPA are or become necessary in order to meet the requirements of applicable data protection law, the parties shall reach agreement on this in good time.

11.2 Should one or more provisions of the DPA be or become invalid or unenforceable in whole or in part, this shall not affect the validity of the remaining provisions. The parties undertake to jointly replace the invalid or unenforceable provision with a valid provision that comes as close as

possible to the economic intentions of the parties. The same shall apply to any loopholes in the DPA. The parties agree that this provision does not constitute a mere reversal of the burden of proof, but rather expressly waives Section 139 BGB.

11.3 The DPA is subject to the law of the Federal Republic of Germany to the exclusion of the UN Convention on Contracts for the International Sale of Goods.

Annex 1 - Description of the Data Processing

1. Type of Processing

The data processing is carried out for the following purposes:

- *Collection, recording, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data in connection with the provision, operation, support and maintenance of the remberg Anything Relationship Management (XRM) software for the Client and its users in accordance with the provisions of the Main Agreement*

2. Categories of Personal Data that are processed

The data processing includes the following data categories:

- *Personnel master data (in particular name, e-mail address, telephone number)*
- *Company data (in particular company name, website, address, country, IP address)*
- *Communication data (in particular logs of the use of the software and changes made to data)*
- *Contract billing and payment data*

3. Sensitive Data processed (if applicable)

The data processing includes the following sensitive data (Art. 9 GDPR)

- *N/A*

4. Categories of Data Subjects whose Personal Data are processed

The data processing concerns the following categories of data subjects:

- *Employees - freelance and salaried - of the client or, if applicable, of a company affiliated with the client*
- *Former employees - freelance and salaried - of the client or, if applicable, of a company affiliated with the client*
- *Employees - freelance and salaried - of the client's customers*
- *Employees - freelance and salaried - of the client's interested parties*

5. Duration of processing

The data processing has the following period:

- *Data processing is carried out for the duration of the Main Agreement*

Annex 2 – Technical and Organizational Measures of the Contractor

The Contractor shall take the following technical and organizational measures for data security within the meaning of Art. 32 GDPR.

1. Confidentiality

- **Entry Control**

  Measures that are suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data is processed or used.

  Processing takes place in the data centers of Amazon Web Services. AWS is responsible for physical security. The measures include, among others, 24/7 security personnel, biometric access controls, video surveillance and strict access logging. Compliance is evidenced by SOC and ISO certificates.

  The following applies to our own business premises:

  - Alarm system
  - Electric door openers
  - Key regulation
  - Careful selection of cleaning staff
  - Data protection arrangements with cleaning staff
  - Guests are always accompanied by employees
  - Logging of visitors
  - Instruction to close windows and doors outside working hours

- **Access Control**

  Measures that are suitable for preventing data processing systems from being used by unauthorized persons.

  - Assignment of user rights

- Password assignment & authentication with user name / password
- Use of multi-factor authentication
- Use of anti-virus software
- Automatic desktop lock
- BIOS protection (separate password)
- Use of a VPN for remote access
- Firewall
- Mobile Device Management
- Key regulation
- Encryption of data carriers in laptops / notebooks
- Encryption of mobile devices
- Encryption of mobile data carriers
- Assignment of user profiles to IT systems
- Data protection and / or security policy
- IT security policy
- "Secure password" policy
- "Manual desktop lock" instructions
- Management of user authorizations
- Assignment of role-based user authorizations ("need to know")

- Mobile Device Policy
- "Clean desk" policy
- "Deletion / destruction" policy
- Careful selection of cleaning staff

- **Data Access Control**

  Measures that ensure that persons authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified or removed without authorization during processing, use and after storage.

  - Use of authorization concepts
  - Management of rights by system administrators
  - Secure storage of data carriers
  - There is a strict password policy including password length
  - Number of administrators reduced to the "bare minimum"
  - Needs-based access rights
  - Logging of access to applications, in particular when entering, changing and deleting data
  - Data protection compliant document shredder (in accordance with ISO/IEC 21964; at least level 4, cross cut)
  - Secured interfaces (USB, Firewire, network, etc.)
  - Physical and data protection compliant deletion of data carriers

- **Separation**

  Measures to ensure that data collected for different purposes can be processed separately.

  - Separate folder structures (data processing on behalf of clients)

- Separation of production and test system
- Logical client separation (on the software side)
- Definition of database rights
- Control via authorization concept

2. Integrity

- **Input Control**

  Measures that ensure that it is possible to subsequently check and determine whether and by whom personal data has been entered, modified or removed from data processing systems.

  - Document management
  - Technical logging of the entry, modification and deletion of data
  - Manual or automated review of logs
  - Retention of forms from which data has been transferred into automated processing
  - Clear responsibilities for deletions
  - Traceability of entry, modification and deletion of data through individual user names
  - Assignment of rights to enter, change and delete data on the basis of an authorization concept
  - Create an overview showing which applications can be used to enter, change and delete which data.

- **Transfer Control**

  Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or during their transport or storage on data carriers, and that it is possible to verify and establish to which bodies personal data are intended to be transmitted by data transmission equipment.

- E-mail encryption
- Provision via encrypted connections, e.g. SSL encryption (SFTP, HTTPS)
- Setting up dedicated lines or VPN tunnels (Virtual Private Network)
- Use of signature procedures, such as electronic signatures
- Logging of access and retrievals
- Rules for the data protection compliant destruction of data
- Rules to avoid the creation of physical copies of data

3. Availability and Resilience

Measures to ensure that personal data is protected against accidental destruction or loss.

As our services are hosted on Amazon Web Services (AWS), the physical availability and resilience of the infrastructure is fully ensured by AWS. AWS uses state-of-the-art redundancy concepts, including uninterruptible power supply (UPS), emergency generators and redundant network connections across geographically separated availability zones, which are regularly audited in accordance with ISO 27001 and SOC 2. This is complemented by automated backup strategies, continuous monitoring of system performance and the use of scaling mechanisms (e.g. auto-scaling) to guarantee the stability and accessibility of the applications even during high load peaks or hardware failures.

- Air conditioning in server rooms
- Uninterruptible power supply (UPS)
- Fire and smoke detection systems
- Storage of data backups in a secure, off-site location
- Creation of a backup & recovery concept
- Testing data recovery

- Monitoring of the backup process

- Existence of an emergency plan

4. Procedures for Regular Review, Assessment and Evaluation

- **Data Protection Measures**

  Measures to ensure that the technical and organizational measures taken are still effective. This must take place regularly.

  - At least annual review of the effectiveness of the technical protection measures

  - Security certification in accordance with ISO 27001

  - Central documentation of all procedures and rules on data protection, accessible to employees as required / authorized (e.g. wiki, intranet, ...)

  - Employees trained and bound to confidentiality / data secrecy

  - The organization complies with the information obligations under Art. 13 and 14 GDPR

  - A formalized process for handling access requests from data subjects is in place

- **Incident Response Management**

  Measures that support the response to security breaches.

  - Use of firewall(s) and regular updates

  - Use of spam filter(s) and regular updates

  - Use of virus scanner(s) and regular updates

  - Intrusion Detection System (IDS)

  - Intrusion Prevention System (IPS)

  - Documented reporting process for data breaches and security incidents

- Documented process for handling security incidents
- Documentation of data breaches and security incidents
- Process and responsibilities for the follow-up of security incidents and data breaches

- **Privacy by Default**

  Measures for data avoidance and data minimization.

  - Restriction of processing to personal data required for the purpose
  - Simple exercise of the right of withdrawal by data subjects through technical measures
  - Training / awareness-raising of employees
  - Policy for the development of apps / tools etc.

- **Technical and Organizational Measures for Teleworking**

  Measures to ensure that the processing of personal data outside the processor's business premises (e.g. in the context of teleworking, home-based work, home office, mobile working) takes place in compliance with an appropriate level of data protection.

  - Login procedure with user name and password
  - Automatic desktop lock
  - "Manual desktop lock" instructions
  - Mobile Device Policy
  - Data protection policy for the home office, etc.
  - "Clean desk" requirement also for work in the home office / teleworking etc.
  - "Secure password" requirement specifically also for work in the home office / teleworking etc.
  - Requirement to avoid paper printouts

- Requirement to conduct telephone calls involving personal data without third parties listening in
- Requirement not to store data locally or on mobile storage media where possible

For further information on the technical and organizational measures taken by our Sub-Processors, please refer to the referenced data protection information in **Annex 3**.

Annex 3 - Sub-Processors

For the processing of data on behalf of the Client, the Contractor uses the services of third parties who process data on its behalf (sub-processors).

The current list of subcontracted processors can be found here: remberg.com/subcontractors