Data Processing Addendum

The following data processing addendum (hereinafter referred to as the "**Addendum**") supplements the General Terms and Conditions of Devano GmbH for its RebaseData Services (hereinafter referred to as "General Terms") and is entered into by You, as in the company which has accepted Devano's General Terms, hereinafter referred to also as "**Client**" or "Data Exporter", and **Devano GmbH**, Mitteisstr. 3, 80935 Munich, Germany, hereinafter referred to also as "**Provider**" or "Data Importer", both also referred to in the Addendum as "Party" individually and as "Parties" together.

The Addendum shall be effective, and replace any previously applicable contractual specifications relating to its subject matter, from the moment the Gereral Terms are effectively accepted.

1. Definitions

1.1. *GDPR*: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

1.2. *CCPA*: intended as the California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 or "CPRA").

1.3. *Applicable Data Protection Law*: all applicable worldwide legislation relating to data protection and privacy which applies to the respective Party in the role of Processing Personal Data in the context of the General Terms, including, but not limited to, GDPR, Directive 2002/58/EC (the 'e-Privacy Directive'), the CCPA and other applicable U.S. federal and state privacy laws, in each case as amended, repealed, consolidated or replaced from time to time.

1.4. *Personal Data*: intended as defined in Art. 4(1) GDPR;

1.5. *California Personal information*: intended as Personal Data that is subject to the CCPA;

1.6. *Data Subject*: intended as defined in Art. 4(1) GDPR;

1.7. *Processing*: intended as defined in Art. 4(2) GDPR;

1.8. *Controller*: intended as defined in Art. 4(7) GDPR;

1.9. *Processor*: intended as defined in Art. 4(8) GDPR;

1.10. *Third Party*: intended as defined in Art. 4(10) GDPR;

1.11. *Personal Data Breach*: intended as defined in Art. 4(12) GDPR.

1.12. *RebaseData Platform*: RebaseData's servers and online spaces used by the Provider to fulfil its obligations under the General Terms, in which the Client may log in, upload and download databases in accordance with the General Terms.

2. Scope and Subject Matter of the Addendum

This Addendum shall cover the roles, rights and responsibilities each Party shall bear in relation to the Processing carried out in the context of the General Terms.

3. Subject and Duration of Processing

Details of the subject matter and the duration of Processing are defined under the General Terms. An isolated orderly termination of this Agreement is excluded.

4. Processing Details

4.1. Processing Roles

Within the context of the services provided under the General Terms, the Client assumes the role of Controller, while the Provider assumes the role of Processor. Each role is defined in Sec. 1 of this Addendum.

4.2. Nature of Processing

In the context of this Addendum, Personal Data may be:

- Transferred between the Parties;
- Structured;
- Stored;
- Adapted;
- Aligned;
- Combined;

among other possible types of Processing.

4.3. Purpose of Processing

The purpose of the Processing is for the Provider to provide the services as specified under the General Terms, to the Client. The Provider may further process Personal Data in the context of this Addendum in pursuit of its own data platform or security purposes, or in case such Processing is required by law.

4.4. Location of Processing

For the purposes of this Addendum, Personal Data shall be processed within the European Economic Area.

4.5. Categories of processed Personal Data

In the context of this Addendum, the following categories of Personal Data shall be processed:

- Contact information of the Client, including full name of the contact person and email address;
- Login information, as well as data generated when logging in the RebaseData Platform;
- Survey information, collected at the moment of sign-up to the RebaseData Platform;
- Billing information for sending invoices, if the Client is an individual and not an enterprise;

- If any, the Personal Data included in the datasets uploaded in the RebaseData Platform for conversion.

4.6. Categories of affected Data Subjects

Apart from the Data Subjects associated with the Client, the categories of Data Subjects affected by the Processing carried out herein depend on the data included in the files uploaded in the RebaseData Platform for conversion.

5. Technical and organisational measures

5.1. The Provider must document the implementation of the technical and organisational measures prior to the commencement of the Processing carried out in the context of this Addendum.

5.2. The Provider must implement data security measures and to ensure a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems and services, in accordance with Art. 28(3)(c) and (e) and Art. 32 GDPR, in particular in conjunction with Art. 5(1) and (2) GDPR. Thereby, the state of the art, the implementation costs and the nature, scope and purpose of the processing as well as the varying probability and severity of the risk for the rights and freedoms of natural persons according to Art. 32(1) GDPR must be taken into account. The Provider lists out the implemented security measures in pursuit of compliance with the aforementioned GDPR dispositions in Annex I of this Addendum.

5.3. The technical and organisational measures are subject to technical progress and further development. In that regard, the Provider is permitted to implement alternative and appropriate measures, which either guarantee the same level of security as the substituted measure or further improve it. Substantial changes are to be documented and notified to the Client without undue delay.

6. Processor Obligations

6.1. Personal Data processed in the context of this Addendum shall be so only under written instruction of the Client. Any changes to the instructions must be communicated to the Provider in writing. The Provider shall notify the Client without undue delay, if it is of the opinion that fulfilling the Client’s instructions would violate Applicable Data Protection Law.

6.2. The Provider shall notify the Client in writing of any Personal Data Breach it becomes aware of without undue delay. The notification must contain all specifications regarding the mitigation measures implemented by the Provider until that moment in time, aimed at contrasting the effects of the Personal Data Breach. The Provider shall dedicate reasonable efforts for cooperating with the Client in the handling of the Personal Data Breach, including but not limited to during the investigation of the Personal Data Breach, the implementation of further mitigating measures and the reporting of the Personal Data Breach to a supervisory authority, intended as defined under art. 4(21) GDPR.

6.3. In accordance with art. 28(3) sentence 2 lit. b GDPR the Provider guarantees that the persons authorised to process the Personal Data in the context of this Addendum have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and have been previously familiarised with data protection obligations. The confidentiality obligation shall extend to beyond the termination of this Addendum.

6.4. The Parties and, where applicable, their representatives, shall cooperate and assist each other when required to carry out tasks in pursuit of compliance with art. 32-36 GDPR, in particular in case of inquiries forwarded by a supervisory authority. Any communication from a supervisory authority received by the Provider, which involves processing carried out on behalf of the Client, shall be communicated to the Client without undue delay: this also applies if a competent authority investigates in the course of administrative or criminal proceedings.

6.5. The Provider shall review its internal processes as well as its implemented technical and organisational measures with regularity, to ensure that the processing within its area of responsibility complies with the requirements of applicable data protection law and that the rights of Data Subjects are protected.

7. Sub-processors

7.1. The Provider is hereby generally authorised to engage the services of sub-processors for carrying out processing activities on behalf of the Client. Sub-processors are understood to be third parties offering services to the public, with whom the Provider has concluded an agreement for receiving their offered services. The Provider makes an up-to-date list of the engaged sub-processors available to the Client prior to the commencement of the Processing in the context of this Addendum.

7.2. The Provider is required to inform the Client in writing of any new sub-processor it is intending to engage for carrying out Processing in the context of this Addendum. The Client shall have 15 days from the receipt of said communication from the Provider to oppose the engagement of the new sub-processor. The objection must be communicated to the Provider in writing. In case no objection from the Client is received from the Provider within the specified period, then the engagement of the new sub-processor is intended as agreed upon by the Client.

7.3. The Provider shall engage sub-processors by means of a written agreement, in compliance with the requirements specified under art. 28(4) GDPR.

8. Rights of the Controller

8.1. The Client has the right to carry out inspections on the Provider’s Processing activities at its discretion, including on-site, in consultation with the Provider or to have them carried out by third-party auditors to be appointed in individual cases. The inspection plan must be submitted by the Client at least 1 calendar month prior to the designated commencement date of the inspection, and must describe the designated scope and areas subject to inspection. The inspections shall be carried out during the Provider’s business hours, or, in any case, within periods of the day as to not disrupt the Provider’s normal working proceedings. The Provider shall allocate all reasonable resources and efforts to cooperate with the Client and its designated auditors in the context of the inspection, including making available all requested material, including but not limited to written documentation and having employees which are reasonably relevant for the inspection’s scope available for interviewing, to the extent the requested material does not consist in highly confidential information for the Provider and is reasonably found to be within of the scope of the inspection. All parties involved in the inspection shall be bound to a written agreement of confidentiality.

8.2. Upon request, the Provider shall provide the Client with the necessary information and/or documentation, in particular to prove the implementation of the technical and organisational measures specified in this Addendum.

9. Data Handling

9.1. The Provider's production of copies and/or duplicates of the Personal Data processed in the context of this Addendum are forbidden, unless necessary for purposes of providing the services under the General Terms or for creating backups of the same, to the extent necessary for fulfilling the security requirements set under this Addendum or unless otherwise required under Applicable Data Protection Law.

9.2. Upon any of the following conditions:

a. termination of or withdrawal from the General Terms; or

b. complete fulfilment of the purposes of Processing under the General Terms,

the Provider shall, to the discretion of the Client, either permanently delete the personal data processed in the context of this Addendum or return them to the Client. Proof of deletion may be submitted by the Provider upon request.

9.3. If any Personal Data processed in the context of this Addendum is retained by the Processor on the basis of security requirements or statutory obligations, the Processor shall retain said personal data to the sole amount of time necessary to fulfil said obligations.

10. Additional Clauses for California Personal Data

10.1. The 'Additional Provisions for California Personal Data' section of this Addendum will apply only with respect to California Personal Data.

10.2. When processing California Personal Data in accordance with the Client's instructions, the Parties acknowledge and agree that the Client is a Business and the Provider is a Service Provider for the purposes of the CCPA.

10.3. The Provider certifies that California Personal Data shall be processed minding the role of a Service Provider, strictly for the purpose of performing the services specified under the General Terms or as otherwise permitted by the CCPA. Further, the Client certifies that it i) will not Sell or Share California Personal Data; (ii) will not Process California Personal Data outside the direct business relationship between the Parties, unless required by Applicable Data Protection Law; and (iii) will not combine the California Personal Data received from the Client with personal data collected or received from another source, be it from other clients or other Third Parties.

10.4. The Provider shall (i) comply with obligations applicable as a Service Provider under the CCPA and (ii) provide California Personal Data with the same level of privacy protection as is required under the CCPA. The Provider shall notify the Client without undue delay if it is determined that the Client can no longer meet its obligations as a Service Provider under the CCPA.

10.5. The Client shall have the right to take reasonable and appropriate steps to help ensure that the Provider uses California Personal Data in a manner consistent with Client's obligations under the CCPA. Upon notice, the Client shall have the right to take reasonable and appropriate steps in accordance with this Addendum to stop and remediate unauthorised use of California Personal Data.

10.6. The Parties acknowledge and agree that the disclosure of California Personal Data by the Client to the Provider does not form part of any monetary or other valuable consideration exchanged between the Parties.

11. Liability

11.1. Each Party shall be liable to the other Parties of this Addendum for any damages it causes the other Parties as a result of a breach of any of the clauses found herein or of Applicable Data Protection Law.

11.2. Where more than one Party is responsible for any damage caused to the Data Subject as a result of a breach of either this Addendum or Applicable Data Protection Law, all responsible Parties shall be jointly and severally liable and the Data Subject is entitled to bring an action in court against any of these Parties.

11.3. The Parties agree that if one Party is held liable under the previous subsection, it shall be entitled to claim back from the other Parties that part of the compensation corresponding to its / their responsibility for the damage.

11.4. The Provider may not invoke the conduct of a sub-processor to avoid its own liability.

12. Final Provisions

12.1. Each Party, when communicating with the counterparty, shall use the communication channels provided under the signatory parties' details, provided under the signatures below.

12.2. If any of the provisions of this Addendum clash in significance and/or effect with any of the provisions of the General Terms or any other agreement established between the Parties relating to the services provided by the Provider to the Client, the provisions of this Addendum shall prevail. Where applicable, if any of the provisions of this Addendum clash in significance and/or effect with any standard contractual clauses or similar clauses published by a public data protection body (hereinafter "SCCs") annexed to this Addendum, the provisions of the SCCs shall prevail.

12.3. Should individual provisions of this Addendum be wholly or partially invalid or unenforceable or become ineffective as a result of changes in the legislation after its conclusion, its remaining provisions and overall validity shall remain unaffected. The invalid or unenforceable provision shall be replaced by applicable statutory provisions or a replacement clause agreed upon by the Parties. Should the Addendum prove incomplete, such provisions shall be deemed to have been agreed which correspond to its purpose and would have been agreed upon by the Parties in the case of consideration.

12.4. Any changes applied to this Addendum shall be made in writing, under agreement of the Parties.

12.5. This Addendum is subject to the choice of law and jurisdiction made under the General Terms.

Annex I

Technical and Organisational Measures implemented by the Provider

Confidentiality

Access and authorisation controls: measures suitable for preventing unauthorised persons from gaining access to data processing systems.	
Measure	**Description**
Physical access management	● electronic physical entry control system with log ● high security perimeter fencing around the entire data centre park ● documented distribution of keys to employees and colocation customers for colocation racks (each Client only for his rack) ● policies for accompanying and designating guests in the building ● data centre staff present 24/7 ● video monitoring at entrances and exits; security door ● interlocking systems and server rooms ● For data centre visitors, entrance to the building is only permitted in the company of an employee ● electronic physical access control system with log
IAM policy	Processed data is accessible only from authorised persons, via individual log-in credentials, assigned and managed by the system administrator.
Password policy	Set passwords are logically set to be accepted only with minimum character requirements - character amount, special characters, alphanumeric characters.
Lock screen policy	An automated screen lock policy is installed in all hardware devices with allowed access to processed data.
Firewall	Traffic is monitored and filtered to impede unauthorised access attempts.
SSH encryption	Encryption of all SSH traffic.
Isolation controls: measures that ensure that data collected for diverse purposes is processed separately from other data.	
Separation of testing and production environments	Sandboxes are logically set up for testing purposes, keeping production data logically separated.
Physical separation	Testing and production environments are stored in different physical servers.
Segregation	Folders storing different types of data and information are logically stored in different environments, each one with their own assigned access policy.
Isolated database conversion	Each database conversion is run in an isolated environment.
Retention controls: measures that ensure the maintained confidentiality of data even after expiration of the agreement.	

<table>
<tr><td>Deletion policy</td><td>In accordance with the Addendum and the General Terms, the different types of data are deleted after defined periods.</td></tr>
<tr><td colspan="2"><b>Pseudonymisation controls</b>: measures aimed at rendering the identification of data subjects through the use of the processed data not possible without the use of additional information.</td></tr>
<tr><td>Privacy by design</td><td>Pseudonymisation techniques such as hashing, encryption and tokenization are used wherever possible in the used programmes’ logic.</td></tr>
</table>

Integrity

<table>
<tr><td colspan="2"><b>Transfer controls</b>: measures that ensure data is not accessed, read, copied, altered, removed or otherwise handled by unauthorised persons during electronic transmissions or storage, and that render the correct reception of data to the designated recipients possible.</td></tr>
<tr><td><b>Measure</b></td><td><b>Description</b></td></tr>
<tr><td>SSL encryption</td><td>Secure Socket Layer encryption is applied to all transport of data packets between the data repository servers and the operational hardware units.</td></tr>
<tr><td colspan="2"><b>Monitoring controls</b>: measures to ensure any unauthorised manipulation of data is detected and acted upon in a timely and effective manner.</td></tr>
<tr><td>Event logging</td><td>Any event of access and editing of data is logged for monitoring.</td></tr>
</table>

Availability and Resilience

<table>
<tr><td colspan="2"><b>Availability and resilience controls</b>: measures designed to ensure the continuous or reasonable availability of the processed data, even in case of system failure, natural events or disasters of other nature.</td></tr>
<tr><td><b>Measure</b></td><td><b>Description</b></td></tr>
<tr><td>Backup and recovery</td><td>Daily backups of login credentials and purchased subscriptions are carried out. Database input files or conversion result files are not included in the daily backups, however, which need to be stored by the users on their own device.</td></tr>
<tr><td>Disk mirroring</td><td>Logical disk volumes are replicated onto separate physical hard disks on a regular basis.</td></tr>
<tr><td>Monitoring</td><td>Servers are monitored on a continuous basis.</td></tr>
<tr><td>Energy backup</td><td>An emergency power supply system is in place.</td></tr>
<tr><td>DDoS protection</td><td>DDoS monitoring and protection programmes are permanently implemented.</td></tr>
<tr><td>Rapid recovery policy</td><td>For all internal systems, there is a defined escalation chain which specifies who is to be informed in the event of an error in order to restore the system as quickly as possible.</td></tr>
</table>

Other Organisational Measures

Measure	Description
Due diligence	Sub-Processors are engaged only after a due diligence assessment, aimed at ensuring that they comply with the business, legal and compliance requirements of Provider, including ensuring that adequate technical and organisational measures are implemented and communication channels for fast engagement in case of breaches or similar are established.
Conclusion of agreements with sub-processors	Provider concludes data processing agreements (DPAs) with all its engaged sub-processors, in accordance with Art. 28 (3) GDPR. Prior assessments of each DPA are carried out to ensure compliance with applicable data protection laws.

Annex II

Sub-Processors List

Sub-processor name & privacy notice link	HQ address	Country	Sub-processing activity	Certification
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen	Germany	Data hosting	ISO 27001
Wavecon GmbH	Thomas-Mann-Straße 16-20 90471 Nuremberg	Germany	Data hosting Server administration services	ISO 27001