Data Processing Agreement

1. Object of the data processing

1.1 Within the scope of the contract concluded between the parties, it is not excluded that the Contractor processes personal data of the Client or its contractual partners on behalf of the Client, the processing of which is decided by the Client as the controller (hereinafter referred to as "Data"). This agreement on the processing of personal data on behalf of the client (hereinafter referred to as the agreement) specifies the rights and obligations of the parties under data protection law.

2. Subject matter, type, purpose and duration of the order processing

2.1 The Contractor processes the data in accordance with Art. 28 Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter GDPR) on behalf of and in accordance with the instructions of the Client.

2.2 The processing of data within the scope of order processing shall be carried out in accordance with the provisions on the type, scope and purpose of data processing contained in Annex 1. It relates to the types of data specified in Annex 1 and the categories of data subjects named therein. In addition, the type and scope of processing also result from the main contract.

2.3 The processing of the data takes place in the territory of the Federal Republic of Germany, in another member state of the European Union (EU) or in a state of the European Economic Area (EEA). The Contractor may also process data outside the EEA in compliance with this Agreement and Art. 44 et seq. GDPR may also process data outside the EEA.

2.4 The duration of this agreement (hereinafter: term) is based on the main contract.

3. Authority of the client to issue instructions

3.1 The Contractor shall process the data exclusively in accordance with the Client's instructions as set out in this Agreement and the main contract. Individual instructions which deviate significantly from the provisions of this Agreement or the main contract or which impose additional requirements shall require the prior consent of the Contractor. Individual instructions shall be documented by the Contractor in text form.

3.2 If the Contractor is of the opinion that an individual instruction violates applicable data protection law, it shall inform the Client of this immediately; in the event of an obviously unlawful individual instruction, the Contractor shall not be bound by this individual instruction, otherwise it shall be entitled to suspend the execution of the instruction until the Client confirms the instruction.

4. Obligations of the client

4.1 The client is responsible for the lawfulness of the processing and for safeguarding the rights of the data subjects. The client has the sole authority to issue instructions to the contractor with regard to the processing of the data.

4.2 The Client must inform the Contractor immediately if it discovers errors or irregularities in relation to the Contractor's services with regard to data protection regulations or its instructions.

5 Obligations of the Contractor

5.1 The Contractor shall ensure and regularly monitor that the processing under the main contract in its area of responsibility, which includes the subcontractor, is carried out in accordance with the provisions of this Agreement.

5.2 The Contractor may not process any data for its own purposes within the scope of commissioned processing without the prior consent of the Client. This shall not apply, and the Client shall have no right to issue instructions in this respect, if the Contractor is obliged to process data by applicable law; in such a case, the Contractor shall notify the Client of this prior to processing, unless applicable law prohibits such notification due to an important public interest.

5.3 The Contractor shall support the Client in official supervisory procedures regarding the processing by the Contractor, insofar as this is necessary and reasonable for the Contractor.

5.4 The Contractor shall oblige the persons employed in the processing to maintain confidentiality, unless this has already been done or unless these persons are subject to comparable appropriate statutory confidentiality obligations.

5.5 The contractor is obliged to appoint a data protection officer if and as long as the legal requirements for an appointment obligation are met.

5.6 The Contractor shall support the Client so that the Client can fulfill its obligations under Art. 32 GDPR and, if requested, under Art. 35 GDPR (data protection impact assessment) and Art. 36 GDPR (consultation with the supervisory authority), insofar as this is reasonable for the Contractor.

5.7 Upon request, the Contractor shall provide the Client with all necessary information in text form to prove compliance with the obligations set out in Art. 28 GDPR.

6. Technical and organizational measures

6.1 The Contractor shall implement the technical and organizational measures listed in Annex 2 at the latest at the start of data processing and maintain them during the term. These measures relate to data security and to ensuring a level of protection appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. The state of the art, the

implementation costs and
the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons pursuant to Art. 32 para. 1 GDPR must be taken into account.

6.2 The Contractor shall be permitted to implement alternative technical and organizational measures, provided that this does not fall below the security level of the measures in Annex 2. Significant changes require the prior consent of the Client in text form.

7. Notification of breaches by the contractor

7.1 The Contractor shall inform the Client immediately in the event of a data breach if it discovers that it or one of its employees has violated data protection regulations or this Agreement during processing.

7.2 The Contractor shall support the Client so that the Client can fulfill its reporting obligations due to data breaches in accordance with Art. 33 f. GDPR. GDPR, insofar as this is reasonable for the Contractor. The Client shall reimburse the Contractor for any expenses and costs incurred as a result, which must be proven.

8. Control rights of the client

8.1 The Client shall be entitled to enter the Contractor's business premises in which data is processed, at its own expense, without disrupting business operations and while maintaining confidentiality of trade and business secrets and other confidentiality obligations of the Contractor, after giving due notice and during normal business hours, in order to satisfy itself that the measures pursuant to § 6 are being complied with. The Client shall be entitled to have this inspection carried out by a third party bound to confidentiality. This authorization is limited to the premises of the Contractor and does not extend to the premises of third parties (e.g. Hetzner or other cloud service providers), even if data of the Client is processed there.

8.2 The Contractor shall grant the Client or a third party commissioned by the Client the rights of access, information and inspection required to carry out the checks and shall cooperate in the checks to an appropriate extent.

8.3 The Contractor is entitled not to disclose information that is sensitive with regard to the Contractor's business or if the Contractor would be in breach of statutory or other contractual obligations by disclosing it.

8.4 The Client must inform the Contractor immediately of all circumstances related to the performance of the inspection. As a rule, the Client may carry out one inspection per year. The Client shall be entitled to carry out further inspections in the event of special occurrences.

8.5 The Contractor shall receive a lump-sum expense allowance of EUR 1,800 per day of the inspection from the Client for its expenses incurred in the course of these inspections. This shall not apply if the

Contractor is culpably responsible for the reason for the inspection. The Client shall be entitled to prove that the expenses were not incurred or were lower.
8.6 If the Client commissions a third party to carry out the inspection, the Client must oblige the third party in writing in the same way as the Client is obliged to the Contractor on the basis of § 8. The Client must demonstrably oblige the third party to maintain confidentiality, unless the third party is subject to a statutory confidentiality obligation.

8.7 At the Contractor's discretion, proof of compliance with the measures under § 6 may also be provided by submitting a suitable certificate, reports from independent bodies or certification by a data protection audit if the audit report enables the Client to satisfy itself of compliance with these measures. § Section 8 (1) remains unaffected.

9. Subcontractors

9.1 The Contractor may entrust suitable subcontractors with the processing of data if the Client consents to this in text form in individual cases. The Contractor also consents to the use of the subcontractors listed in Annex 3.

9.2 Subcontracting relationships within the meaning of this agreement are only those services that relate to the main contract and involve data processing. No consent is required for the commissioning of subcontractors where the subcontractor merely uses an ancillary service to support the fulfillment of the main contract (e.g. postal, transport, telecommunications services such as Asana or Slack).

9.3 The Contractor shall inform the Client of any intended change with regard to the involvement or replacement of subcontractors. The Client may object to the involvement or replacement of subcontractors in text form within 14 days of being informed by the Contractor for good cause.

9.4 The subcontractor shall be subject to essentially the same data protection obligations as set out in this Agreement. In particular, it must be ensured that the technical and organizational measures are implemented by the subcontractor in such a way that the processing is carried out in accordance with the requirements of data protection law. The Contractor shall be liable to the Client for its subcontractors in accordance with Section 278 BGB.

9.5 The provisions of the above paragraphs shall also apply if the subcontractor in turn engages a subcontractor.

10. Rights of the data subjects

10.1 The rights of the persons affected by the processing must be asserted against the client. If a data subject should contact the Contractor directly to assert their rights, the Contractor shall forward this request to the Client.

10.2 In the event that a data subject asserts justified data protection claims against the Client, the

Contractor shall support the Client in fulfilling these claims with suitable technical and organizational measures within the scope of what is legally and actually possible, provided this is not unreasonable for the Contractor. § Section 8 (5) shall apply accordingly.

11. Return and deletion of data and data carriers provided

11.1 At the end of the term, the Contractor shall delete data at the Client's discretion and/or, if it was transmitted on physical data carriers, return it, unless the Contractor is obliged to store it. The Contractor shall have no right of retention to the data unless its counterclaim has been legally established or is undisputed.

11.2 Documentation that serves as proof of proper processing or statutory retention periods may be retained by the Contractor beyond the end of the term within the scope of the law

12 Relationship to the main contract, choice of law

12.1 Insofar as no special provisions are contained in this agreement, the provisions of the main contract shall apply. In the event of contradictions between this agreement and other agreements between the parties, the provisions of this agreement shall take precedence.

12.2 The GDPR and supplementary German law apply.

Appendix 1

Details on the client data and processing

Topic	**Description**
Subject matter of the contract	Provision of web-based software & database access including maintenance and support, as well as ad hoc data intelligence services
Duration	For the duration of the main contract
Nature and purpose	The personal data is processed for the purpose of fulfilling the orders of and communicating with the controller.
Type of personal data	E-mail addresses, IP addresses, name
Categories of affected persons	Employees & customers of the person responsible

Appendix 2

Technical and organizational measures (Art 32 (1) GDPR)

1. pseudonymization and encryption of personal data

- Pseudonymization of personal data
- Encryption of personal data

Explanation:

Pseudonymization measures:

- Avoiding the storage of IP addresses, shortening IP addresses if necessary
- Avoidance of the storage of cookie IDs

Encryption of personal data:

- Access to the application is only possible via encrypted transmission channels and by logging in with a user name and password

2. Access control

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

☒ Assignment of user rights
☒Creating user profiles
☒ Password assignment
Authentication with biometric procedures
☒ Authentication with user name / password
☒ Assignment of user profiles to IT systems
☐ Use of a hardware firewall
☒ Use of VPN technology
Locking external interfaces (USB etc.)
☒ Use of a software firewall
Encryption of data carriers in laptops / notebooks
☒ No use of mobile data carriers for the storage of personal data
Encryption of smartphone content
☒ Use of central smartphone administration software (e.g. for external deletion of data) ☒ Use of anti-virus software

3. 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.

☒ Creation of an authorization concept
Management of rights by system administrator
☒ Number of administrators reduced to the "bare minimum"
☒ Password policy incl. password length, password change
☒ Logging of access to applications, in particular when entering, changing and deleting data ☐ Secure storage of data carriers
☐ Physical deletion of data carriers before reuse
Proper destruction of data carriers
☒ Use of document shredders or service providers (if possible with a data protection seal of approval)
☐ Logging of the destruction
☒ Encryption of data carriers

4. 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.

☒ Logging the entry, modification and deletion of data
☐ Create an overview showing which applications can be used to enter, change and delete which data.
Traceability of data entry, modification and deletion through individual user names (not user groups)
☐ Retention of forms from which data has been transferred to automated processing
☒ Assignment of rights to enter, change and delete data based on an authorization

concept **5. Order control**

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

☒ Selection of the contractor under due diligence aspects (in particular with regard to data security)
☐ Prior inspection and documentation of the safety measures taken by the

contractor ☒ Written instructions to the contractor (e.g. through an order processing contract) ☒ Obligation of the Contractor's employees to maintain data secrecy ☒ Contractor has appointed a data protection officer
☐ Ensuring the destruction of data after completion of the order
☐ Effective control rights agreed with the contractor
☐ Ongoing review of the contractor and its activities
☐ Contractual penalties for breaches

6. Availability control

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

☒ Data is only stored in data centers of providers that have ISO 27001 or equivalent certification

The measures taken there usually include

☒ Uninterruptible power supply (UPS)
☒ Air conditioning in server rooms
☒ Devices for monitoring temperature and humidity in server rooms
Protective socket strips in server rooms
☒ Fire and smoke detection systems
Fire extinguishers in server rooms
☒ Alarm message for unauthorized access to server rooms
☒ Creation of a backup & recovery concept
☒ Testing data recovery
☒ Creation of an emergency plan
☒ Redundant storage of data backups in the cloud
☒ Server rooms not under sanitary facilities
☒ In flood areas: Server rooms above the water line

7. Separation requirement

Measures to ensure that data collected for different purposes can be processed separately.
☐ Physically separate storage on separate systems or data carriers
☒ Logical client separation (on the software side)
☒ Creation of an authorization concept
☐ Encryption of data records that are processed for the same purpose ☐ Providing the data records with purpose attributes/data fields
For pseudonymized data: Separation of the allocation file and storage on a separate, secure IT system
☒ Definition of database rights
☒ Separation of production and test system

Appendix 3

Approved subprocessors/subcontractors

- Freshdesk GmbH
- Google Ireland Limited
- Hetzner Online GmbH
- Amazon Web Services EMEA SARL, NL Germany
- HubSpot Germany GmbH
- Userflow Inc.