2024

Data Processing Agreement (DPA)

According to Art. 28 GDPR

Between:

Peak Privacy ApS
ÅBOULEVARD 42
2201 Copenhagen N

(Responsible party - hereinafter referred to as principal)

and the company:

meetergo GmbH
Hauptstr. 44
40789 Monheim am Rhein

(Data Processor)

Preamble

The Data Processor shall process personal data from the Client's area of responsibility under data protection law within the meaning of Article 28 of the General Data Protection Regulation (GDPR) within the scope of contracts concluded or to be concluded. The personal data provided to the Contractor by the Client shall be subject to the provisions of the GDPR and the other provisions of data protection law (e.g. BDSG).

This agreement sets out the framework conditions to ensure compliance with data protection regulations.

1. Subject matter and duration of the contract

The object of the data handling contract is the provision of the *meetergo* software. This is a Software-as-a-Service service (Saas) with the following object:

- Use of *meetergo* for project coordination
- Use of *meetergo* as a scheduling tool
- Use of *meetergo* as a tool for communication (video as well as audio communication)

The duration of the order

- The duration of this contract agreement is based on the duration of use of the *meetergo* software.

2. Concretisation of the content of the order

Nature and purpose of the intended processing of data

Detailed description of the subject matter of the contract with regard to the scope, nature and purpose of the contractor's tasks:

Availability and appointment data can be entered in meetergo so that one's own appointment calendar can be shared with third parties (e.g. via the booking link). Appointments in available slots can be booked directly via the appointment calendar. Furthermore, notifications can be configured before and after the appointment, as well as forms for entering relevant data for the appointment. The team function also enables the management of team availability and assignment of appointments to specific staff members. Optionally, video/audio conferences can also be held directly on meetergo.

The provision of the contractually agreed data processing shall take place exclusively in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the client and may only take place if the special requirements of Art. 44 et seq. GDPR are fulfilled.

Type of data

The following types/categories of data are the subject of the processing of personal data (enumeration/description of the categories of data)

- Personal master data (also from third-party customers)
- Communication data (e.g. telephone, e-mail)
- Customer history or tracking of usage behaviour
- Contract billing and payment data

Categories of persons concerned

The categories of data subjects affected by the processing include:

- Customers
- Interested parties
- Employees
- Third-party customers

3. Technical and organisational measures

The contractor shall document the implementation of the technical and organisational measures set out and required in the run-up to the awarding of the contract before the start of the processing, in particular with regard to the specific execution of the contract, and shall hand them over to the client for inspection. If accepted by the Client, the documented measures shall become the basis of the contract. Insofar as the examination/audit of the Client reveals a need for adaptation, this shall be implemented by mutual agreement.

The contractor shall establish security pursuant to Art. 28 (3) lit. c, 32 GDPR, in particular in connection with Art. 5 (1), (2) GDPR. Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk with regard to confidentiality, integrity, availability and the resilience of the systems. In this context, 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 within the meaning of Article 32 (1) of the GDPR must be taken into account [details in Annex 1].

The technical and organisational measures are subject to technical progress and further development. In this respect, the contractor is permitted to implement alternative adequate measures. In doing so, the security level of the specified measures must not be undercut. Significant changes shall be documented.

4. Correction, restriction and deletion of data

The contractor may not correct, delete or restrict the processing of data processed under the contract on its own authority but only in accordance with documented instructions from the client. Insofar as a data subject contacts the Contractor directly in this regard, the Contractor shall forward this request to the Client without delay.

Insofar as included in the scope of services, the deletion concept, the right to be forgotten, correction, data portability and information shall be ensured directly by the Contractor in accordance with the Client's documented instructions.

5. Quality assurance and other obligations of the contractor

In addition to compliance with the provisions of this contract, the Contractor shall have legal obligations pursuant to Articles 28 to 33 of the GDPR; in this respect, the Contractor shall in particular ensure compliance with the following requirements:

a) Written appointment of a data protection officer who carries out his or her activities in accordance with Art. 38 and 39 of the GDPR.
   The contact details of the data protection officer shall be communicated to the client for the purpose of direct contact. The client shall be informed immediately of any change of data protection officer.

b) The Contractor is not obliged to appoint a data protection officer. Mr. Dominik Rapacki, +49 221 1612239, **privacy@meetergo.com** is appointed as contact person at the Contractor.

c) Maintaining confidentiality in accordance with Art. 28 (3) sentence 2 lit. b, 29, 32 (4) GDPR. When carrying out the work, the contractor shall only use employees who have been obligated to maintain confidentiality and who have previously been familiarised with the data protection provisions relevant to them. The Contractor and any person subordinate to the Contractor who has access to personal data may process this data exclusively in accordance with the Client's instructions, including the powers granted in this contract, unless they are legally obliged to process it.

d) The implementation of and compliance with all technical and organisational measures required for this order in accordance with Art. 28 (3) sentence 2 lit. c, 32 GDPR [details in Annex 1].

e) The contracting authority and the contractor shall cooperate with the supervisory authority in the performance of its duties upon request.

f) The immediate information of the client about control actions and measures of the supervisory authority, insofar as they relate to this order. This also applies insofar as a competent authority is investigating the Contractor in the context of administrative offence or criminal proceedings with regard to the processing of personal data during the commissioned processing.

g) Insofar as the Client, for its part, is exposed to an inspection by the supervisory authority, administrative offence or criminal proceedings, the liability claim of a data subject or a third party or any other claim in connection with the commissioned processing at the Contractor, the Contractor shall support it to the best of its ability.

h) The contractor shall regularly monitor the internal processes as well as the technical and organisational measures to ensure that the processing in its area of responsibility is carried out in accordance with the requirements of the applicable data protection law and that the protection of the rights of the data subject is guaranteed.

i) Verifiability of the technical and organisational measures taken vis-à-vis the Client within the scope of its control powers pursuant to clause 7 of this contract.

6. Subcontracting relationships

Subcontracting relationships within the meaning of this provision shall be understood to be those services which directly relate to the provision of the main service. This does not include ancillary services which the contractor uses, for example, as telecommunications services, postal/transport services, maintenance and user service 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 Contractor shall be obliged to implement appropriate and legally compliant contractual agreements as well as control measures to ensure data protection and data security of the Client's data also in the case of outsourced ancillary services.

The Contractor may only engage subcontractors (further processors) with the prior express written or documented consent of the Client.

The Client agrees to the commissioning of the following subcontractors - subject to the condition of a contractual agreement in accordance with Article 28 (2-4) of the GDPR:

Company Subcontractor	Country	Power
Hotjar Ltd	Malta	Cloud-based Usability Services
Amazon Europe Core S.à r.l.	Germany (AWS Frankfurt)	Cloud service provider
Stripe, Inc.	United States	Cloud-based Billing Services
Crisp IM SaS	France	Cloud-based Customer Support

The transfer of personal data of the Principal to the subcontractor and its first activity shall only be permitted once all requirements for subcontracting have been met.
If the subcontractor provides the agreed service outside the EU / EEA, the contractor shall ensure that it is permissible under data protection law by taking appropriate measures. The same shall apply if service providers within the meaning of para. 1 sentence 2 are to be used.
Any further outsourcing by the subcontractor requires the express consent of the principal (at least in text form); all contractual provisions in the contractual chain must also be imposed on the further subcontractor.

For further subcontractors responsible for the implementation of optional tools, please refer to our website: https://meetergo.crisp.help/en/article/list-of-subprocessors-1nak22t/?bust=1718097315792

7. Control rights of the principal

The Client has the right to carry out inspections in consultation with the Contractor or to have them carried out by inspectors to be named in individual cases. It shall have the right to satisfy itself of the Contractor's compliance with this Agreement in its business operations by means of spot checks, which must generally be notified in good time.

The Contractor shall ensure that the Client can satisfy itself of the Contractor's compliance with its obligations pursuant to Art. 28 of the GDPR. The Contractor undertakes to provide the Client with the necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organisational measures.

Evidence of such measures, which do not only concern the specific order, can be provided through

- compliance with approved rules of conduct in accordance with Art. 40 GDPR;
- certification in accordance with an approved certification procedure pursuant to Art. 42 GDPR;
- current attestations, reports or report extracts from independent bodies (e.g. auditors, auditing, data protection officers, IT security department, data protection auditors, quality auditors);
- suitable certification by IT security or data protection audit (e.g. according to BSI-Grundschutz).

The contractor may claim remuneration for enabling inspections by the client.

8. Notification of infringements by the contractor

The Contractor shall assist the Client in complying with the personal data security obligations, data breach notification obligations, data protection impact assessments and prior consultations referred to in Articles 32 to 36 of the GDPR. This includes, among others

a) ensuring an adequate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing as well as the predicted likelihood and severity of a potential security breach and allow for the immediate detection of relevant breach events;
b) the obligation to report personal data breaches to the principal without delay;
c) the obligation to assist the principal within the scope of his duty to inform the data subject and, in this context, to provide him with all relevant information without delay;
d) the support of the client for its data protection impact assessment; and
e) the support of the principal in the context of prior consultations with the supervisory authority.

The Contractor may claim remuneration for support services which are not included in the specifications or which are not due to the Contractor's misconduct.

9. Authority of the principal to issue instructions

The client shall confirm verbal instructions without delay (at least in text form).

The Contractor shall inform the Client without delay if it is of the opinion that an instruction violates data protection regulations. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Client.

10. Deletion of data and return of data carriers

Copies or duplicates of the data shall not be made without the knowledge of the client. Excluded from this are security copies, insofar as they are necessary to ensure proper data processing, as well as data required with regard to compliance with statutory retention obligations.

After completion of the contractually agreed work or earlier upon request by the Client - at the latest upon termination of the service agreement - the Contractor shall hand over to the Client or, after prior consent, destroy in accordance with data protection law all documents, processing and utilisation results produced and data files which have come into its possession and which are connected with the contractual relationship. The same applies to test and reject material. The protocol of the deletion shall be submitted upon request.

Documentation which serves as proof of the orderly and proper data processing shall be kept by the contractor beyond the end of the contract in accordance with the respective retention periods. He may hand them over to the Client at the end of the contract to relieve him of the burden.

11 Term and termination

This Agreement shall enter into force upon signature by both Parties and shall remain in force for as long as the relevant service relationship continues.

Monheim am Rhein, the

2025-04-26

Signature / Stamp

Dominik Rapacki

Signature / Stamp Processor

Attachment(s):

1. Technical-organisational measures of the contractor

Annex - Technical-organisational measures of the Contractor

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

- Physical Access control
  No unauthorised access to data processing systems
  - Magnetic or chip cards
  - Key
  - Plant security or gatekeeper
  - Alarm systems
  - Video systems

- Logical Access control
  No unauthorised system use
  - (Secure) passwords
  - automatic locking mechanisms
  - Two-factor authentication
  - No unauthorised reading, copying, modification or removal within the system
  - Authorisation concepts and needs-based access rights
  - Logging of accesses

- Separation control
  Separate processing of data collected for different purposes

- Pseudonymisation (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)
  The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is kept separately and is subject to appropriate technical and organisational measures.

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

- Transfer control
  No unauthorised reading, copying, modification or removal during electronic transmission or transport
  - Encryption
  - electronic signature

- Input control
  Determining whether and by whom personal data have been entered into, modified or removed from data processing systems.
  - Logging
  - Document management

3. Availability and resilience (Art. 32(1)(b) GDPR)

_ Availability control
Protection against accidental or deliberate destruction or loss
- Backup strategy (online/offline; on-site/off-site)
- Uninterruptible power supply (UPS)
- Virus protection
- Firewall
- Reporting channels and emergency plans

_ Rapid recoverability (Art. 32(1)(c) GDPR);

4. Procedures for regular review, assessment and evaluation (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

_ Data protection management

_ Data protection-friendly default settings (Art. 25 (2) GDPR)

_ Order control
No commissioned data processing within the meaning of Art. 28 GDPR without corresponding instructions from the client
- Clear contract design
- formalised order management
- Strict selection of the service provider
- Duty of prior conviction
- Follow-up checks