Data Processing Agreement

pursuant to Article 28 GDPR

As at: July 2026 · Version 2.2

Between

the customer who enters into the Main Agreement with meetergo GmbH for use of the meetergo platform, to the extent that the customer acts as a controller within the meaning of Article 4(7) GDPR (the “Controller”),

and

meetergo GmbH, Hauptstraße 44, 40789 Monheim am Rhein, Germany, represented by its managing directors Dominik Rapacki and Richard Gödel, email: privacy@meetergo.com, telephone: +49 221 16 12 239

(processor within the meaning of Article 4(8) GDPR, the “Processor”),

together referred to as the “Parties”.

Preamble

Under the “meetergo” brand, the Processor operates a software-as-a-service platform for scheduling, forms, integrated video and audio conferencing, CRM functionality and workflows. In providing this platform, the Processor processes personal data for which the Controller is responsible within the meaning of Article 28 GDPR.

This Agreement specifies the Parties' data protection rights and obligations in connection with the Processor's processing of personal data on behalf of the Controller. It applies to all activities connected with the main agreement between the Parties concerning use of the meetergo platform (the “Main Agreement”) in which the Processor's personnel or persons engaged by the Processor may come into contact with the Controller's personal data.

1. Subject matter, nature, purpose and duration of processing

1.1 Subject matter

The subject matter of the processing is the provision of the meetergo software as a software-as-a-service offering under the Main Agreement, in particular:

- use of meetergo for scheduling and availability management;
- use of forms, workflows and CRM functionality to collect and manage contact details and communications;
- use of integrated video and audio conferencing through meetergo Connect;
- use of optional AI-supported features and other platform modules under the Main Agreement.

1.2 Nature and purpose

The nature and purpose of processing are set out in the Main Agreement and the Processor's then-current Privacy Notice, available at https://meetergo.com/privacy. Processing principally consists of collecting, recording, organising, retrieving, transmitting, making available, deleting and backing up personal data provided by the Controller or generated through its use of the platform, in each case for the purpose of providing the contractually agreed services.

1.3 Duration

This Agreement is concluded in electronic form pursuant to Article 28(9) GDPR. It takes effect when incorporated into and electronically concluded with the Main Agreement, or when accepted separately by

electronic means. A handwritten or electronic signature is not required. This Agreement remains in force for the term of the Main Agreement. Retention and assistance obligations which, by their nature, continue after termination remain unaffected.

2. Details of the processing

2.1 Place of processing

Personal data is processed exclusively in Member States of the European Union or in another state party to the Agreement on the European Economic Area, unless an approved engagement of a sub-processor under section 6 involves a transfer to a third country. Any such transfer is made in compliance with Articles 44 et seq. GDPR.

2.2 Categories of personal data

Processing is limited to personal data for which the Controller is responsible. Depending on the Controller's use of the platform, this may include in particular:

- basic personal data (name, form of address, title, role, address and company affiliation);
- communication data (email address, telephone number and, where applicable, messaging identifiers);
- appointment and availability data, including booking and cancellation history;
- form content and responses;
- content of video and audio conferences (transmitted only for the duration of the call; stored only where the Controller actively starts the optional recording function, and then until deleted by the Controller);
- usage and log data relating to the above activities (such as booking timestamps, the booker's IP address and user agent).

Where the Controller enters data into the platform or collects data through booking, form or CRM fields that constitutes special categories of personal data within the meaning of Article 9(1) GDPR, in particular health data, such data is also covered by this Agreement. The Controller alone decides whether and to what extent such data is collected and is responsible for ensuring that an exception under Article 9(2) GDPR applies. The Processor processes such data solely on the Controller's instructions. The technical and organisational measures in Annex 1 apply without limitation. Where the Controller is subject to a special duty of professional secrecy under section 203 of the German Criminal Code (StGB), the Parties shall additionally enter into the separate confidentiality agreement available in the Controller's customer account.

Data processed by the Processor in its own capacity as controller under section 2.4, including the Controller's account, billing and payment data, is not covered by this Agreement.

2.3 Categories of data subjects

Processing may concern only data subjects for whom the Controller is responsible. Depending on the Controller's use of the platform, these may include in particular:

- the Controller's customers, prospects and other business contacts;
- bookers, form respondents and participants in meetergo Connect calls whom the Controller invites to the platform;
- the Controller's personnel, where they participate as hosts or team members in booking, form or conferencing activities;
- job applicants, where the Controller uses meetergo to coordinate applications.

The Processor processes the account and access data of users and administrators designated by the Controller in its own capacity as controller under section 2.4.

2.4 Processing by the Processor as controller

Where the Processor processes personal data in its own capacity as controller in connection with operating the platform, including account and access data of users and administrators designated by the Controller, billing and payment data, security and abuse logs, and technical telemetry used to operate the platform, the Processor rather than the customer is the controller. Such processing is not covered by this Agreement and is governed by the Processor's then-current Privacy Notice.

3. Technical and organisational measures

The Processor shall implement the technical and organisational measures required by Article 32 GDPR to ensure a level of security appropriate to the risk with regard to the confidentiality, integrity, availability and resilience of the systems. These measures are documented in Annex 1 to this Agreement.

The Processor may develop these measures in line with the state of the art, provided that the level of security specified in Annex 1 is not reduced. Material changes shall be documented and disclosed to the Controller on request.

A summary of the security measures is also available at
https://help.meetergo.com/en/legal/security-best-practices.

4. Rectification, restriction and erasure of data

The Processor shall process personal data entrusted to it only on the documented instructions of the Controller. It shall rectify, restrict or erase such data only where instructed by the Controller or where the meetergo application provides the Controller with corresponding self-service functions.

If a data subject contacts the Processor directly to exercise their rights, the Processor shall promptly forward the request to the Controller and inform the data subject accordingly. The Processor shall not independently respond to the substance of the request unless expressly agreed otherwise.

Within the scope of the services covered by the Main Agreement, the Processor shall assist the Controller through appropriate technical and organisational measures in responding to data subject requests for access, rectification, erasure, restriction, data portability and objection under Articles 12 to 22 GDPR.

5. Quality assurance and other Processor obligations

In addition to complying with this Agreement, the Processor shall comply with its statutory obligations under Articles 28 to 33 GDPR and shall in particular ensure the following:

a) The Processor is not required to designate a data protection officer under Article 37(1) GDPR. Mr Dominik Rapacki, Managing Director, is the contact for data protection matters. Enquiries should be sent to privacy@meetergo.com and will be handled together with the internal privacy team.

b) Confidentiality shall be maintained in accordance with Articles 28(3)(b), 29 and 32(4) GDPR. The Processor shall use only personnel who are bound by confidentiality obligations and have been made aware of the data protection provisions relevant to their work. Such persons may process entrusted data only on the Controller's instructions or where required by law.

c) The technical and organisational measures required by Article 32 GDPR and set out in Annex 1 shall be implemented and maintained.

d) The Processor shall cooperate with the supervisory authority on request in the performance of the Parties' respective obligations under Article 31 GDPR.

e) The Processor shall promptly inform the Controller of inspections and measures by a supervisory authority insofar as they concern the processing under this Agreement.

f) The Processor shall assist the Controller to the best of its ability if the Controller is subject to an inspection by a supervisory authority, administrative or criminal proceedings, a liability claim by a data subject or third party, or another claim connected with the processing under this Agreement.

g) The Processor shall regularly review its internal processes and technical and organisational measures to ensure that processing within its area of responsibility complies with applicable data protection law and protects the rights of data subjects.

h) The Processor shall be able to demonstrate the technical and organisational measures implemented to the Controller within the scope of the Controller's audit rights under section 10.

i) Where necessary, the Processor shall assist the Controller with data protection impact assessments under Article 35 GDPR and prior consultations with the supervisory authority under Article 36 GDPR.

6. Sub-processing

6.1 General authorisation

The Controller grants the Processor general written authorisation under the second sentence of Article 28(2) GDPR to engage the other processors listed at the link in section 6.3 (the “Sub-processors”) and to engage additional Sub-processors in accordance with section 6.2.

Each Sub-processor is bound by a contract that imposes in substance the same data protection obligations as those imposed on the Processor in relation to the Controller under this Agreement, in accordance with Article 28(4) GDPR. The Processor remains responsible to the Controller for the Sub-processor's compliance with its data protection obligations.

Ancillary services used by the Processor as a third party to support its business operations, such as telecommunications, postal and transport services, cleaning, maintenance and user support without access to data, do not constitute sub-processing under this Agreement. The Processor shall nevertheless put in place appropriate contractual and practical safeguards for data protection and data security in relation to such services.

6.2 Changes to Sub-processors

In accordance with the second sentence of Article 28(2) GDPR, the Processor shall inform the Controller of any intended addition or replacement of a Sub-processor at least thirty (30) calendar days before the change takes effect. Notice shall be sent to the registered account holder's email address and the list linked in section 6.3 shall be updated.

The Controller may object to the intended change within that period on reasonable data protection grounds. If the Controller objects, the Parties shall seek an agreed solution. If no agreement can be reached, the Controller may terminate the Main Agreement for cause in respect of the affected service by giving reasonable notice. Any further rights and remedies remain unaffected.

6.3 Authoritative list of Sub-processors

The Processor publishes and maintains the current, complete and authoritative list of Sub-processors, including the legal entity, place and purpose of processing, and the transfer mechanism under Chapter V GDPR, at https://help.meetergo.com/en/legal/list-of-subprocessors. That list forms part of this Agreement. The version in effect at the time of processing applies. Changes shall be announced in accordance with section 6.2.

For information, the following table summarises the position when this Agreement was concluded (July 2026). If this table differs from the published online list, the online list controls.

Category	Sub-processor (legal entity)	Seat / place of processing
Web application hosting and authentication	Hetzner Online GmbH	Germany (Nuremberg, Falkenstein)
Website hosting (meetergo.com)	OVH SAS (OVHcloud)	France
Content delivery	BunnyWay d.o.o. (bunny.net)	Slovenia (primarily EU edge nodes)
Transactional email	AhaSend B.V.	Netherlands
Customer support	Crisp IM SAS	France
SMS and WhatsApp	Twilio Ireland Limited	Ireland; onward transfer to Twilio, Inc. (United States) based on the Standard Contractual Clauses 2021/914 and the EU-US Data Privacy Framework
Billing and payments	Stripe Payments Europe Ltd	Ireland; onward transfer to Stripe, Inc. (United States) based on the Standard Contractual Clauses 2021/914 and the EU-US Data Privacy Framework
AI features (optional, opt-in)	Mistral AI SAS	France
AI features (optional, opt-in)	melious GmbH	Germany
Spam protection	Friendly Captcha GmbH	Germany
Applicant management	HeyJobs GmbH (Join)	Germany

The Processor uses Hetzner Online GmbH (Germany) to host the meetergo web application. User authentication is provided through an instance operated by the Processor within that infrastructure. OVH SAS (OVHcloud, France) is used to host the meetergo.com marketing website. Changes shall be announced in accordance with section 6.2.

6.4 Integration partners are not Sub-processors

Third-party services that the Controller connects to its meetergo account through the integration settings, such as the Controller's calendar provider, CRM, conferencing tools, payment tools or marketing tools, are not Sub-processors of the Processor. In this context, the Processor acts on the Controller's instructions. The Controller engages the integration partner directly under that partner's terms and is the controller responsible for the associated processing. Where such an integration results in a transfer to a third country, the Controller is responsible for compliance with Articles 44 et seq. GDPR.

7. International data transfers

Any transfer of personal data under this Agreement to a third country shall be made only in compliance with Articles 44 et seq. GDPR. The applicable transfer mechanisms are:

- adequacy decisions adopted by the European Commission under Article 45 GDPR;
- the EU-US Data Privacy Framework (adequacy decision of 10 July 2023), where the US recipient is self-certified;
- the Standard Contractual Clauses 2021/914 under Article 46(2)(c) GDPR, using the applicable module, as either a fallback or the primary transfer mechanism.

The applicable mechanism for each Sub-processor is stated in the list linked in section 6.3. Where required, the

Processor shall implement supplementary technical, organisational and contractual measures, including a transfer impact assessment, and shall provide corresponding evidence at the Controller's request.

8. Notification of personal data breaches

The Processor shall assist the Controller in ensuring compliance with the obligations under Articles 32 to 36 GDPR relating to the security of personal data, notification of personal data breaches, data protection impact assessments and prior consultations. This includes in particular:

a) ensuring an appropriate level of protection through suitable technical and organisational measures that enable relevant breach events to be detected immediately;

b) notifying the Controller of personal data breaches **without undue delay after becoming aware of them, generally within twenty-four (24) hours,** so that the Controller can comply with its own notification and communication obligations under Articles 33 and 34 GDPR within the applicable time limits;

c) providing all relevant information required by the Controller to comply with its notification and communication obligations towards supervisory authorities and data subjects;

d) assisting the Controller with data protection impact assessments;

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

The Processor shall provide the assistance described in this section without additional charge to the extent required by Article 28(3)(f) GDPR. The Processor may charge reasonable fees at its then-current hourly rates only for assistance that exceeds the scope required by Article 28(3)(f) GDPR and is not attributable to any fault of the Processor.

9. Controller instructions

The Processor shall process personal data only on documented instructions from the Controller. The requirements set out in this Agreement, the Main Agreement and the configurations made by the Controller in the application constitute such instructions.

The Controller shall promptly confirm oral instructions at least in text form. The Processor shall promptly inform the Controller if, in its opinion, an instruction infringes data protection law. The Processor may suspend the instruction until the Controller confirms or modifies it.

10. Controller audit rights

The Controller has the right to satisfy itself that the Processor complies with its obligations under Article 28 GDPR. On request, the Processor shall provide the Controller with the information necessary for this purpose and, in particular, demonstrate implementation of the technical and organisational measures.

Evidence may be provided in particular through:

- adherence to approved codes of conduct under Article 40 GDPR;
- certification under an approved certification mechanism pursuant to Article 42 GDPR;
- current attestations, reports or extracts from reports issued by independent bodies, such as auditors or data protection auditors;
- self-assessments by the Processor based on an industry-standard security questionnaire.

Any further statutory audit and inspection rights of the Controller under Article 28(3)(h) GDPR remain unaffected.

11. Return and erasure after termination

Copies or duplicates of the data shall not be made without the Controller's knowledge, except for backup copies necessary to ensure proper processing and data required to comply with statutory retention obligations.

After termination of the Main Agreement, or earlier at the Controller's request, the Processor shall, at the Controller's choice, return or securely erase all personal data processed on the Controller's behalf in its possession, together with any copies, unless Union or Member State law requires storage of the personal data.

For return of the data, the Processor shall provide the application's standard export functions. Data may be exported during a return period of thirty (30) days after termination, after which it shall be erased. On separate request, the Processor shall document the erasure.

12. Liability

Liability is governed by the Main Agreement and applicable law, in particular Article 82 GDPR. Each Party shall indemnify the other upon first demand against third-party claims to the extent that they result from a culpable breach by the indemnifying Party of its obligations under this Agreement or applicable data protection law.

13. Final provisions

Amendments and additions to this Agreement must be made in text form. This also applies to any amendment of this clause.

If any provision of this Agreement is or becomes invalid or unenforceable, the validity of the remaining provisions shall not be affected. The Parties shall replace the invalid or unenforceable provision with a valid and enforceable provision that most closely reflects the economic purpose of the original provision.

This Agreement is governed by the laws of the Federal Republic of Germany, excluding its conflict-of-laws rules. To the extent permitted by law, the courts at the Processor's registered office shall have exclusive jurisdiction over all disputes arising out of or in connection with this Agreement.

In the event of a conflict, this Agreement prevails over the Main Agreement with respect to data protection matters.

14. Conclusion and evidence of this Agreement

The Processor shall document the electronic conclusion of this Agreement and make it permanently available to the Controller in a reproducible format. The Controller may view and download the version applicable to it from the administration area.

If the Parties enter into a separately negotiated data processing agreement in an individual case, that agreement shall prevail over this standard Agreement.

Annex 1: Technical and organisational measures

This Annex describes the technical and organisational measures implemented by the Processor within the meaning of Article 32 GDPR. The measures are continuously adapted to the state of the art, provided that the level of security specified in this Annex is not reduced.

1. Confidentiality (Article 32(1)(b) GDPR)

Physical access control	The web application is hosted by Hetzner Online GmbH in ISO/IEC 27001-certified data centres in Germany (Nuremberg and Falkenstein), and the website is hosted by OVH SAS in France. The data centres use multi-layered physical access controls, including mantraps, smart-card and biometric access, 24/7 security personnel and video surveillance. Access to the Processor's offices is limited to authorised personnel; visitors are accompanied and logged.
System access control	Mandatory password policies covering minimum length, complexity and lockout after failed attempts. Mandatory two-factor authentication for all personnel with production access. Automatic screen locking and role-based permissions applying the least-privilege principle. Centralised secrets management using self-hosted Infisical, with no plain-text secrets in source code or tickets.
Personnel reliability	Before personnel begin work, the Processor verifies their reliability using identity documents, employment references and, where legally permitted and necessary for the role, further evidence such as a certificate of conduct for privileged roles. All personnel with access to data are bound by data secrecy and confidentiality obligations under Article 28(3)(b) GDPR when they begin work and annually thereafter, and receive corresponding training.
Data access control	Differentiated authorisation schemes, with production data accessible only to expressly approved roles. Complete logging of administrative access and security-relevant events. Structured logs in a Grafana/Loki stack, retained in accordance with the security and retention policy.
Separation control	Tenant separation at application level, with a workspace ID on all relevant records. Logical separation of production, staging and development, with separate databases and credentials. Test and development environments do not use genuine production personal data unless, exceptionally, it has been pseudonymised.
Pseudonymisation and encryption	Encryption of data at rest in object storage using AES-256. Stored access tokens for third-party systems connected by the Controller are additionally encrypted at field level using AES-256-GCM. Migration of primary database volumes to volume encryption using LUKS with AES-256 is in progress. Until that migration is complete, the other measures in this Annex apply to those systems, in particular system access, data access and separation controls. TLS 1.2 or later is used for all data in transit, together with HSTS and secure cipher suites. Passwords are stored only as one-way hashes. Pseudonymisation is used for purposes including Free/Busy matching for connected calendars and audit logs, where IP addresses are stored as salted one-way hashes.

2. Integrity (Article 32(1)(b) GDPR)

Transfer control	Encrypted transmission of all data between client and server and between internal services. Authenticated API access, rate limiting and anti-abuse controls.
Input control	Creation, modification and erasure of relevant records are logged at application level. Critical configurations are versioned and administrator actions are recorded in audit trails.

Secure software development (SSDLC)	A mandatory secure software development lifecycle, including dual control through pull-request-based code review for every production code change; automated static application security testing (SAST) and secret scanning in the CI/CD pipeline; automated dependency and vulnerability scanning (SCA) for open-source components, with defined response times for critical vulnerabilities; separate build and deployment pipelines with signed artefacts; and mandatory developer training in secure software development based on the OWASP Top 10.

3. Availability and resilience (Article 32(1)(b) and (c) GDPR)

Availability control	Redundant infrastructure in German data centres and daily backups stored separately. Web application firewall, DDoS protection and upstream CDN filtering through BunnyWay d.o.o. Active monitoring using Grafana/Loki, with alerting and escalation chains. Endpoint protection and patch management on personnel devices.
Rapid recoverability	Documented recovery plans and regular restore testing, at least annually and quarterly for critical components. Recovery targets are defined by data class: **Core services** (web application, API and booking system): RTO no more than 4 hours and RPO no more than 1 hour. **Non-critical services** (such as internal tools and reporting): RTO no more than 24 hours and RPO no more than 24 hours. **Long-term backups:** retained for 30 days with geo-redundancy in an EU region.
Security testing and vulnerability management	Continuous automated vulnerability scanning of production infrastructure and container images, at least weekly. External penetration tests by independent third parties at least annually and additionally following material architectural or functional changes. A defined vulnerability response process under which critical findings are remediated within 7 days and high-severity findings within 30 days. Bug bounty programme or public security disclosure channel at security@meetergo.com. Report summaries are provided to customers on justified request and subject to an NDA.

4. Process for regularly testing, assessing and evaluating effectiveness (Article 32(1)(d) GDPR)

Data protection management	Internal data protection and security policies and mandatory training for all personnel with access to data. Central maintenance of records of processing activities and annual review of the technical and organisational measures. A structured incident response process and notification chain to the Controller under section 8 of this Agreement, without undue delay after becoming aware of a breach and generally within 24 hours.
Data protection by default (Article 25 GDPR)	Data minimisation by default in forms and booking flows. Optional features with particular data protection implications, such as AI features and CRM email sync, are opt-in and disabled in the default configuration.
Processing control	Careful selection of Sub-processors and contractual imposition of equivalent data protection standards under Article 28(4) GDPR. Regular review of engaged Sub-processors and updates to the list published at https://help.meetergo.com/en/legal/list-of-subprocessors.

End of Annex 1