Auftragsverarbeitungsvertrag

gemäß Art. 28 DSGVO

Stand: Juli 2026 · Version 2.2

Zwischen

dem Kunden, der mit der meetergo GmbH den Hauptvertrag über die Nutzung der meetergo-Plattform schließt und soweit dieser als Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO handelt (im Folgenden „Auftraggeber“),

und

der **meetergo GmbH**, Hauptstraße 44, 40789 Monheim am Rhein, Deutschland, vertreten durch die Geschäftsführer Dominik Rapacki und Richard Gödel, E-Mail: privacy@meetergo.com, Telefon: +49 221 16 12 239

(Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO, im Folgenden „Auftragnehmer“),

beide Parteien im Folgenden zusammen „die Parteien“.

Präambel

Der Auftragnehmer betreibt unter der Marke „meetergo“ eine Software-as-a-Service-Plattform für Terminplanung, Formulare, integrierte Video- und Audio-Konferenzen, CRM-Funktionalität und Workflows. Im Rahmen der Bereitstellung dieser Plattform verarbeitet der Auftragnehmer personenbezogene Daten aus dem datenschutzrechtlichen Verantwortungsbereich des Auftraggebers im Sinne von Art. 28 DSGVO.

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber. Sie gilt für alle Tätigkeiten, die mit dem zwischen den Parteien geschlossenen Hauptvertrag über die Nutzung der meetergo-Plattform (im Folgenden „Hauptvertrag“) im Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen.

1. Gegenstand, Art, Zweck und Dauer der Verarbeitung

1.1 Gegenstand

Gegenstand des Auftrags ist die Zurverfügungstellung der meetergo-Software als Software-as-a-Service-Leistung gemäß dem Hauptvertrag, insbesondere:

- die Nutzung von meetergo zur Terminplanung und Verfügbarkeitsverwaltung,
- die Nutzung von Formularen, Workflows und CRM-Funktionalität zur Erfassung und Verwaltung von Kontaktdaten und Kommunikation,
- die Nutzung integrierter Video- und Audio-Konferenzen über meetergo Connect,
- die Nutzung optionaler KI-gestützter Funktionen und weiterer Plattform-Module gemäß Hauptvertrag.

1.2 Art und Zweck

Art und Zweck der Verarbeitung ergeben sich aus dem Hauptvertrag und der jeweils gültigen Datenschutzerklärung des Auftragnehmers, abrufbar unter https://meetergo.com/datenschutz. Im Wesentlichen handelt es sich um die Erfassung, Speicherung, Strukturierung, Abfrage, Übermittlung, Bereitstellung, Löschung und Sicherung der vom Auftraggeber bzw. durch dessen Nutzung der Plattform anfallenden personenbezogenen Daten zur Erbringung der vertraglich geschuldeten Leistung.

1.3 Dauer

Diese Vereinbarung wird gemäß Art. 28 Abs. 9 DSGVO in elektronischer Form geschlossen. Sie wird durch Einbeziehung in den Hauptvertrag und dessen elektronischen Abschluss oder durch gesonderte elektronische Annahme wirksam. Eine eigenhändige oder elektronische Unterschrift ist nicht erforderlich. Die Vereinbarung gilt für die Laufzeit des Hauptvertrages. Aufbewahrungspflichten und Beistandspflichten, die ihrem Wesen nach über das Vertragsende hinauswirken, bleiben unberührt.

2. Konkretisierung des Auftragsinhalts

2.1 Verarbeitungsort

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich in Mitgliedstaaten der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum, soweit nicht im Rahmen genehmigter Unterauftragsverarbeitungen gemäß Abschnitt 6 eine Übermittlung in ein Drittland erfolgt. Jede solche Übermittlung erfolgt unter den Voraussetzungen der Art. 44 ff. DSGVO.

2.2 Kategorien personenbezogener Daten

Gegenstand der Verarbeitung sind ausschließlich personenbezogene Daten aus dem Verantwortungsbereich des Auftraggebers, je nach dessen Nutzung der Plattform insbesondere die folgenden Kategorien:

- Personenstammdaten (Name, Anrede, Titel, Funktion, Anschrift, Unternehmenszugehörigkeit),
- Kommunikationsdaten (E-Mail-Adresse, Telefonnummer, ggf. Messenger-Kennungen),
- Termin- und Verfügbarkeitsdaten, Buchungs- und Stornierungsverläufe,
- Formularinhalte und Antworten,
- Inhalte aus Video- und Audio-Konferenzen (nur während der Anrufdauer; keine Aufzeichnung durch meetergo Connect),
- Nutzungs- und Protokolldaten der vorgenannten Vorgänge (z. B. Buchungszeitpunkte, IP-Adresse, User-Agent der Buchenden).

Nicht Gegenstand dieser Vereinbarung sind die vom Auftragnehmer in eigener Verantwortlichkeit verarbeiteten Daten nach Abschnitt 2.4, insbesondere Konto-, Abrechnungs- und Zahlungsdaten des Auftraggebers.

2.3 Kategorien betroffener Personen

Von der Verarbeitung können ausschließlich Personen aus dem Verantwortungsbereich des Auftraggebers betroffen sein, je nach dessen Nutzung der Plattform insbesondere:

- Kunden, Interessenten und sonstige Geschäftspartner des Auftraggebers,
- Buchende, Formularteilnehmer und Teilnehmer von meetergo-Connect-Anrufen, die der Auftraggeber zur Plattform einlädt,
- Beschäftigte des Auftraggebers, soweit sie als Hosts oder Team-Mitglieder in Buchungs-, Formular- oder Konferenzvorgänge einbezogen sind,
- Bewerber, soweit der Auftraggeber meetergo zur Bewerberkoordination nutzt.

Die Konto- und Zugangsdaten der vom Auftraggeber benannten Nutzer und Administratoren verarbeitet der Auftragnehmer nach Abschnitt 2.4 in eigener Verantwortlichkeit.

2.4 Eigene Verantwortlichkeit des Auftragnehmers

Soweit der Auftragnehmer im Zusammenhang mit dem Betrieb der Plattform personenbezogene Daten in eigener Verantwortlichkeit verarbeitet, insbesondere Konto- und Zugangsdaten der vom Auftraggeber benannten Nutzer und Administratoren, Abrechnungs- und Zahlungsdaten, Sicherheits- und Missbrauchsprotokolle sowie technische Telemetrie zum Betrieb der Plattform, ist nicht der Auftraggeber,

sondern der Auftragnehmer Verantwortlicher. Diese Verarbeitungen sind nicht Gegenstand dieser Vereinbarung. Maßgeblich ist insoweit die jeweils gültige Datenschutzerklärung des Auftragnehmers.

3. Technisch-organisatorische Maßnahmen

Der Auftragnehmer trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau hinsichtlich der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme zu gewährleisten. Diese Maßnahmen sind in Anlage 1 zu dieser Vereinbarung dokumentiert.

Der Auftragnehmer ist berechtigt, die Maßnahmen entsprechend dem Stand der Technik fortzuentwickeln; das durch Anlage 1 festgelegte Sicherheitsniveau darf dabei nicht unterschritten werden. Wesentliche Änderungen werden dokumentiert und sind dem Auftraggeber auf Anfrage offenzulegen.

Eine Zusammenfassung der eingesetzten Sicherheitsmaßnahmen ist außerdem unter https://help.meetergo.com/de/legal/security-best-practices abrufbar.

4. Berichtigung, Einschränkung und Löschung von Daten

Der Auftragnehmer verarbeitet die ihm überlassenen personenbezogenen Daten ausschließlich nach dokumentierter Weisung des Auftraggebers. Er berichtigt, schränkt ein oder löscht diese Daten nur, soweit der Auftraggeber dies anweist oder soweit die meetergo-Anwendung dem Auftraggeber entsprechende Funktionen bereitstellt, die der Auftraggeber selbständig ausführen kann.

Wendet sich eine betroffene Person mit einem Anliegen zur Wahrnehmung ihrer Rechte unmittelbar an den Auftragnehmer, leitet dieser die Anfrage unverzüglich an den Auftraggeber weiter und informiert die betroffene Person darüber. Eine eigenständige inhaltliche Bearbeitung erfolgt durch den Auftragnehmer nicht, soweit nicht ausdrücklich anders vereinbart.

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen der vom Hauptvertrag gedeckten Leistungen bei der Erfüllung von Auskunfts-, Berichtigungs-, Lösch-, Einschränkungs-, Datenübertragbarkeits- und Widerspruchsersuchen betroffener Personen (Art. 12 bis 22 DSGVO) durch geeignete technische und organisatorische Maßnahmen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zur Einhaltung der Regelungen dieser Vereinbarung die gesetzlichen Pflichten gemäß Art. 28 bis 33 DSGVO; insbesondere gewährleistet er die Einhaltung der folgenden Vorgaben:

a) Der Auftragnehmer ist nach Art. 37 Abs. 1 DSGVO nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner für datenschutzrechtliche Fragen wird Herr Dominik Rapacki, Geschäftsführer, benannt. Anfragen sind an privacy@meetergo.com zu richten und werden gemeinsam mit dem internen Datenschutzteam bearbeitet.

b) Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 lit. b und Art. 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt nur Beschäftigte ein, die zur Vertraulichkeit verpflichtet und mit den für sie relevanten datenschutzrechtlichen Bestimmungen vertraut gemacht worden sind. Diese Personen dürfen die ihnen anvertrauten Daten ausschließlich nach Weisung des Auftraggebers oder aufgrund gesetzlicher Verpflichtung verarbeiten.

c) Umsetzung und laufende Einhaltung der nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen gemäß Anlage 1.

d) Zusammenarbeit mit der Aufsichtsbehörde auf deren Anforderung im Rahmen der Aufgabenerfüllung beider Parteien (Art. 31 DSGVO).

e) Unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen.

f) Unterstützung des Auftraggebers nach besten Kräften, sofern dieser einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung ausgesetzt ist.

g) Regelmäßige Kontrolle der internen Prozesse sowie der technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Abschnitt 10.

i) Unterstützung des Auftraggebers, soweit erforderlich, bei der Erstellung von Datenschutz-Folgenabschätzungen (Art. 35 DSGVO) sowie bei vorherigen Konsultationen mit der Aufsichtsbehörde (Art. 36 DSGVO).

6. Unterauftragsverarbeitung

6.1 Allgemeine Genehmigung

Der Auftraggeber erteilt dem Auftragnehmer hiermit eine allgemeine schriftliche Genehmigung gemäß Art. 28 Abs. 2 Satz 2 DSGVO zur Beauftragung der in der gemäß Abschnitt 6.3 verlinkten Liste aufgeführten weiteren Auftragsverarbeiter (im Folgenden „Unterauftragsverarbeiter“) sowie zur Hinzuziehung weiterer Unterauftragsverarbeiter nach Maßgabe von Abschnitt 6.2.

Mit jedem Unterauftragsverarbeiter besteht ein Vertrag, der diesem im Wesentlichen die gleichen Datenschutzpflichten auferlegt, die der Auftragnehmer gegenüber dem Auftraggeber hat (Art. 28 Abs. 4 DSGVO). Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die Einhaltung der Datenschutzpflichten durch den Unterauftragsverarbeiter verantwortlich.

Nicht als Unterauftragsverarbeitung im Sinne dieser Vereinbarung gelten Nebenleistungen, die der Auftragnehmer als Dritter zur Unterstützung des Geschäftsbetriebs in Anspruch nimmt (z. B. Telekommunikationsleistungen, Post- und Transportdienstleistungen, Reinigung, Wartung und Benutzerservice ohne Datenzugriff). Der Auftragnehmer ist auch insoweit zu angemessenen vertraglichen und tatsächlichen Vorkehrungen für Datenschutz und Datensicherheit verpflichtet.

6.2 Änderung der Unterauftragsverarbeiter

Der Auftragnehmer informiert den Auftraggeber gemäß Art. 28 Abs. 2 Satz 2 DSGVO über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters mit einer Frist von mindestens dreißig (30) Kalendertagen vor Wirksamwerden der Änderung. Die Information erfolgt durch eine Benachrichtigung an die E-Mail-Adresse des registrierten Kontoinhabers sowie durch Aktualisierung der unter Abschnitt 6.3 verlinkten Liste.

Der Auftraggeber kann der beabsichtigten Änderung innerhalb dieser Frist aus berechtigten datenschutzrechtlichen Gründen widersprechen. Im Falle eines Widerspruchs werden die Parteien einvernehmlich eine Lösung anstreben. Lässt sich keine Einigung erzielen, ist der Auftraggeber berechtigt, den Hauptvertrag im Hinblick auf die betroffene Leistung außerordentlich mit angemessener Frist zu kündigen. Weitergehende Ansprüche bleiben unberührt.

6.3 Maßgebliche Liste der Unterauftragsverarbeiter

Die jeweils aktuelle, vollständige und maßgebliche Liste der Unterauftragsverarbeiter, einschließlich Angabe der Rechtsentität, des Verarbeitungsortes, des Zwecks und des Übermittlungsmechanismus nach Kapitel V DSGVO, wird vom Auftragnehmer unter https://help.meetergo.com/de/legal/list-of-subprocessors veröffentlicht und gepflegt. Diese Liste ist Bestandteil dieser Vereinbarung. Maßgeblich ist die jeweils zum Zeitpunkt der Verarbeitung gültige Fassung; Änderungen werden gemäß Abschnitt 6.2 angekündigt.

Zur Information ist nachfolgend eine zusammenfassende Übersicht des Standes zum Zeitpunkt des Vertragsschlusses (Juli 2026) wiedergegeben. Bei Abweichungen zwischen dieser Übersicht und der online veröffentlichten Liste ist die online veröffentlichte Liste maßgeblich.

Kategorie	Unterauftragsverarbeiter (Rechtsentität)	Sitz / Verarbeitungsort
Hosting Web-Anwendung, Authentifizierung	Hetzner Online GmbH	Deutschland (Nürnberg, Falkenstein)
Hosting Website (meetergo.com)	OVH SAS (OVHcloud)	Frankreich
Objektspeicher und Medien-Transcoding	Amazon Web Services EMEA SARL	Deutschland (AWS Frankfurt)
Content Delivery	BunnyWay d.o.o. (bunny.net)	Slowenien (überwiegend EU-Edge-Knoten)
Transaktionale E-Mail	AhaSend B.V.	Niederlande
Kundenbetreuung	Crisp IM SAS	Frankreich
SMS und WhatsApp	Twilio Ireland Limited	Irland; Weiterübermittlung an Twilio, Inc. (USA) auf Grundlage der Standardvertragsklauseln 2021/914 und des EU-US Data Privacy Framework
Abrechnung und Zahlungen	Stripe Payments Europe Ltd	Irland; Weiterübermittlung an Stripe, Inc. (USA) auf Grundlage der Standardvertragsklauseln 2021/914 und des EU-US Data Privacy Framework
Produktanalyse	PostHog Inc.	EU (EU-Cloud-Region, ausschließlich EU-Hosting); Übermittlung an US-Konzerngesellschaft auf Grundlage der Standardvertragsklauseln 2021/914 und des EU-US Data Privacy Framework
KI-Funktionen (optional, Opt-in)	Mistral AI SAS	Frankreich
KI-Funktionen (optional, Opt-in)	melious GmbH	Deutschland
Spam-Schutz	Friendly Captcha GmbH	Deutschland
Bewerbermanagement	HeyJobs GmbH (Join)	Deutschland

Der Auftragnehmer setzt für die Bereitstellung der meetergo-Web-Anwendung Hetzner Online GmbH (Deutschland) als Hosting-Anbieter ein; die Nutzer-Authentifizierung erfolgt über eine vom Auftragnehmer selbst betriebene Instanz innerhalb dieser Infrastruktur. OVH SAS (OVHcloud, Frankreich) wird für das Hosting der Marketing-Website meetergo.com verwendet. Amazon Web Services EMEA SARL wird ausschließlich für Objektspeicher und Medien-Transcoding im Rechenzentrum Frankfurt eingesetzt. Änderungen werden gemäß Abschnitt 6.2 angekündigt.

6.4 Integrationspartner sind keine Unterauftragsverarbeiter

Drittdienste, die der Auftraggeber selbst über die Integrationseinstellungen mit seinem meetergo-Account verbindet (z. B. der vom Auftraggeber verwendete Kalender-Anbieter, sein CRM, Konferenz-Tools, Zahlungs- und Marketing-Tools), sind keine Unterauftragsverarbeiter des Auftragnehmers. Der Auftragnehmer handelt insoweit auf Weisung des Auftraggebers. Der Auftraggeber bindet den Integrationspartner unmittelbar auf Grundlage von dessen Bedingungen ein und ist für die damit verbundene Verarbeitung Verantwortlicher. Soweit eine solche Integration eine Übermittlung in ein Drittland zur Folge hat, ist der Auftraggeber für die Einhaltung der Art. 44 ff. DSGVO verantwortlich.

7. Internationale Datenübermittlungen

Soweit personenbezogene Daten im Rahmen dieser Vereinbarung in ein Drittland übermittelt werden, erfolgt dies ausschließlich unter den Voraussetzungen der Art. 44 ff. DSGVO. Maßgebliche Übermittlungsmechanismen sind:

- Angemessenheitsbeschlüsse der Europäischen Kommission gemäß Art. 45 DSGVO,
- das EU-US Data Privacy Framework (Angemessenheitsbeschluss vom 10. Juli 2023), soweit der US-Empfänger selbstzertifiziert ist,
- Standardvertragsklauseln 2021/914 gemäß Art. 46 Abs. 2 lit. c DSGVO, in der jeweils einschlägigen Modulvariante, als Fallback oder primärer Mechanismus.

Der jeweils anwendbare Mechanismus pro Unterauftragsverarbeiter ist in der unter Abschnitt 6.3 verlinkten Liste angegeben. Der Auftragnehmer ergreift, soweit erforderlich, ergänzende technische, organisatorische und vertragliche Maßnahmen (Transfer Impact Assessment) und stellt entsprechende Nachweise auf Anforderung des Auftraggebers bereit.

8. Mitteilung bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, zur Meldung von Datenschutzverletzungen, zu Datenschutz-Folgenabschätzungen und vorherigen Konsultationen. Hierzu gehören insbesondere:

a) die Sicherstellung eines angemessenen Schutzniveaus durch geeignete technische und organisatorische Maßnahmen, die eine sofortige Feststellung relevanter Verletzungsereignisse ermöglichen,

b) die Verpflichtung, dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten **unverzüglich nach Kenntniserlangung, in der Regel innerhalb von vierundzwanzig (24) Stunden,** zu melden, damit der Auftraggeber seine eigenen Melde- und Informationspflichten gemäß Art. 33 und 34 DSGVO innerhalb der dort vorgesehenen Fristen erfüllen kann,

c) die Bereitstellung sämtlicher relevanter Informationen, die der Auftraggeber zur Erfüllung seiner Melde- und Informationspflichten gegenüber den Aufsichtsbehörden und den betroffenen Personen benötigt,

d) die Unterstützung des Auftraggebers bei der Durchführung von Datenschutz-Folgenabschätzungen,

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

Die in diesem Abschnitt geregelten Unterstützungsleistungen erbringt der Auftragnehmer im Rahmen der nach Art. 28 Abs. 3 lit. f DSGVO geschuldeten Pflichten unentgeltlich. Lediglich für solche Unterstützungsleistungen, die über das nach Art. 28 Abs. 3 lit. f DSGVO geschuldete Maß hinausgehen und nicht auf ein Verschulden des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine angemessene Vergütung nach seinen jeweils gültigen Stundensätzen beanspruchen.

9. Weisungsbefugnis des Auftraggebers

Der Auftragnehmer verarbeitet die personenbezogenen Daten ausschließlich auf dokumentierte Weisung des Auftraggebers. Die in dieser Vereinbarung, im Hauptvertrag und in den vom Auftraggeber in der Anwendung vorgenommenen Konfigurationen niedergelegten Vorgaben gelten als solche Weisungen.

Mündliche Weisungen bestätigt der Auftraggeber unverzüglich, mindestens in Textform. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt. Er ist berechtigt, die Durchführung der Weisung auszusetzen, bis sie vom Auftraggeber bestätigt oder geändert wird.

10. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, sich von der Einhaltung der Pflichten des Auftragnehmers aus Art. 28 DSGVO zu überzeugen. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die hierfür erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

Der Nachweis kann insbesondere erbracht werden durch:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO,
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO,
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Stellen (z. B. Wirtschaftsprüfer, Datenschutzauditoren),
- Selbstauskünfte des Auftragnehmers auf Basis eines branchenüblichen Sicherheitsfragebogens.

Weitergehende gesetzliche Kontroll- und Inspektionsrechte des Auftraggebers nach Art. 28 Abs. 3 lit. h DSGVO bleiben unberührt.

11. Löschung und Rückgabe nach Vertragsende

Kopien oder Duplikate der Daten werden ohne Kenntnis des Auftraggebers nicht erstellt. Ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die zur Erfüllung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Nach Beendigung des Hauptvertrages, oder früher auf Anforderung des Auftraggebers, hat der Auftragnehmer sämtliche in seinem Besitz befindlichen, im Auftrag verarbeiteten personenbezogenen Daten und etwaige Kopien nach Wahl des Auftraggebers zurückzugeben oder datenschutzgerecht zu löschen, sofern nicht nach Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

Für die Rückgabe stellt der Auftragnehmer Standard-Exportfunktionen der Anwendung bereit. Der Export ist innerhalb einer Rückgabefrist von dreißig (30) Tagen nach Vertragsende möglich; danach werden die Daten gelöscht. Auf gesonderte Anforderung dokumentiert der Auftragnehmer die Löschung.

12. Haftung

Für die Haftung gelten die Regelungen des Hauptvertrages sowie die gesetzlichen Bestimmungen, insbesondere Art. 82 DSGVO. Die Parteien stellen einander auf erstes Anfordern von Ansprüchen Dritter frei, soweit diese auf einer schuldhaften Verletzung der Pflichten der jeweils anderen Partei aus dieser Vereinbarung oder aus den datenschutzrechtlichen Vorschriften beruhen.

13. Schlussbestimmungen

Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Dies gilt auch für die Änderung dieser Klausel.

Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder werden, so wird hierdurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Die Parteien werden die unwirksame oder undurchführbare Bestimmung durch eine wirksame und durchführbare Bestimmung ersetzen, die dem wirtschaftlichen Zweck der ursprünglichen Bestimmung am nächsten kommt.

Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss der kollisionsrechtlichen Vorschriften. Ausschließlicher Gerichtsstand für sämtliche Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung ist, soweit gesetzlich zulässig, der Sitz des Auftragnehmers.

Im Widerspruchsfall gehen die Regelungen dieser Vereinbarung den Regelungen des Hauptvertrages vor, soweit es um datenschutzrechtliche Fragen geht.

14. Vertragsschluss und Nachweis

Der Auftragnehmer dokumentiert den elektronischen Vertragsschluss und stellt dem Auftraggeber diese Vereinbarung dauerhaft in einem wiedergabefähigen Format zur Verfügung. Der Auftraggeber kann die jeweils für ihn geltende Fassung im Administrationsbereich einsehen und herunterladen.

Schließen die Parteien im Einzelfall einen gesondert ausgehandelten Auftragsverarbeitungsvertrag, geht dieser der vorliegenden Standardvereinbarung vor.

Anlage 1: Technisch-organisatorische Maßnahmen

Diese Anlage beschreibt die vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO. Die Maßnahmen werden laufend an den Stand der Technik angepasst; das in dieser Anlage festgelegte Sicherheitsniveau wird dabei nicht unterschritten.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle	Hosting der Web-Anwendung bei Hetzner Online GmbH in ISO/IEC 27001-zertifizierten Rechenzentren in Deutschland (Nürnberg, Falkenstein); Hosting der Website bei OVH SAS in Frankreich. Mehrstufige physische Zugangskontrollen (Mantraps, Chipkarten- und Biometrie-Zutritt, 24/7 Wachpersonal, Videoüberwachung) auf Seiten der Rechenzentren. Büroräume des Auftragnehmers: Zutritt nur für berechtigte Beschäftigte; Besucher werden begleitet und protokolliert.
Zugangskontrolle	Verbindliche Passwort-Richtlinien (Mindestlänge, Komplexität, Sperre nach Fehlversuchen). Verpflichtende Zwei-Faktor-Authentifizierung für alle Mitarbeitenden mit Produktivzugang. Automatische Bildschirmsperren; rollenbasierte Zugriffsrechte nach Least-Privilege-Prinzip. Zentrale Verwaltung von Geheimnissen über self-hosted Infisical; keine Klartext-Geheimnisse in Quellcode oder Tickets.
Zuverlässigkeit der Beschäftigten	Vor Aufnahme der Tätigkeit prüft der Auftragnehmer die Zuverlässigkeit der Beschäftigten anhand vorgelegter Identitätsnachweise, Arbeitszeugnisse und – soweit gesetzlich zulässig und für die Tätigkeit erforderlich – weiterer Nachweise (z. B. Führungszeugnis bei privilegierten Rollen). Alle Beschäftigten mit Datenzugang werden zu Beginn der Tätigkeit und danach jährlich auf das Datengeheimnis sowie auf Vertraulichkeit verpflichtet (Art. 28 Abs. 3 lit. b DSGVO) und entsprechend geschult.
Zugriffskontrolle	Differenzierte Berechtigungskonzepte; Zugriff auf Produktivdaten nur für ausdrücklich freigeschaltete Rollen. Vollständige Protokollierung administrativer Zugriffe und sicherheitsrelevanter Ereignisse. Strukturierte Logs in einem Grafana/Loki-Stack mit Aufbewahrung gemäß Sicherheits- und Aufbewahrungskonzept.
Trennungskontrolle	Mandantentrennung auf Anwendungsebene (Workspace-ID auf allen relevanten Datensätzen). Logische Trennung von Produktion, Staging und Entwicklung; getrennte Datenbanken und Zugangsdaten. Test- und Entwicklungsumgebungen verwenden keine echten personenbezogenen Produktivdaten, soweit nicht ausnahmsweise pseudonymisiert.
Pseudonymisierung und Verschlüsselung	Verschlüsselung ruhender Daten (AES-256) in den primären Datenbanken und im Objekt-Speicher. TLS 1.2+ für sämtliche Übertragungen; HSTS und sichere Cipher-Suites. Passwörter ausschließlich als Einweg-Hashes gespeichert. Pseudonymisierung u. a. bei Free/Busy-Abgleich verbundener Kalender sowie bei Audit-Protokollen (gesalzene Einweg-Hashes von IP-Adressen).

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle	Verschlüsselte Übertragung sämtlicher Daten zwischen Client und Server sowie zwischen internen Diensten. Authentifizierte API-Zugänge; Rate-Limiting und Anti-Missbrauchs-Mechanismen.
Eingabekontrolle	Protokollierung von Erstellung, Änderung und Löschung relevanter Datensätze auf Anwendungsebene. Versionierung kritischer Konfigurationen und Audit-Trails für Administrator-Aktionen.

Sichere Softwareentwicklung (SSDLC)	Verbindlicher Secure-Software-Development-Lifecycle: Vier-Augen-Prinzip durch Pull-Request-basiertes Code-Review für jede produktive Codeänderung; automatisiertes statisches Code-Scanning (SAST) und Secret-Scanning in der CI/CD-Pipeline; automatisierte Abhängigkeits- und Schwachstellenprüfungen (SCA) auf Open-Source-Komponenten mit definierter Reaktionsfrist für kritische Schwachstellen; getrennte Build- und Deployment-Pipelines mit signierten Artefakten; verbindliche Schulung der Entwickler zu sicherer Softwareentwicklung (OWASP Top 10).

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

Verfügbarkeitskontrolle	Redundante Infrastruktur in deutschen Rechenzentren; tägliche Backups mit getrennter Aufbewahrung. Web Application Firewall, DDoS-Schutz und CDN-vorgelagerte Filterung (BunnyWay d.o.o.). Aktives Monitoring (Grafana/Loki) mit Alarmierungs- und Eskalationsketten. Endpoint-Schutz und Patch-Management auf Beschäftigten-Geräten.
Rasche Wiederherstellbarkeit	Dokumentierte Wiederanlaufpläne; regelmäßige Tests von Restore-Prozessen (mindestens jährlich, bei kritischen Komponenten quartalsweise). Definierte Recovery-Ziele je nach Datenklasse: **Kerndienste** (Web-Anwendung, API, Buchungssystem): RTO höchstens 4 Stunden, RPO höchstens 1 Stunde. **Nicht-kritische Dienste** (z. B. interne Werkzeuge, Reporting): RTO höchstens 24 Stunden, RPO höchstens 24 Stunden. **Langzeit-Backups:** Aufbewahrung 30 Tage, georedundant in EU-Region.
Sicherheitsprüfungen und Schwachstellenmanagement	Kontinuierliches automatisiertes Schwachstellen-Scanning der Produktivinfrastruktur und Container-Images (mindestens wöchentlich). Externe Penetrationstests durch unabhängige Drittanbieter mindestens jährlich sowie zusätzlich anlassbezogen bei wesentlichen Architektur- oder Funktionsänderungen. Definierter Schwachstellen-Reaktionsprozess: kritische Befunde werden innerhalb von 7 Tagen, hohe Befunde innerhalb von 30 Tagen behoben. Bug-Bounty-Programm bzw. öffentlicher Security-Disclosure-Kanal unter security@meetergo.com. Berichtszusammenfassungen werden Kunden auf begründete Anfrage und unter NDA bereitgestellt.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

Datenschutz-Management	Interne Datenschutz- und Sicherheitsleitlinien; verbindliche Schulungen für alle Beschäftigten mit Datenzugang. Zentrale Pflege des Verarbeitungsverzeichnisses; jährliche Überprüfung der TOMs. Strukturierter Incident-Response-Prozess; Meldekette an Auftraggeber gemäß Abschnitt 8 dieser Vereinbarung (unverzüglich nach Kenntniserlangung, in der Regel innerhalb von 24 Stunden).
Datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO)	Standardmäßige Datenminimierung in Formularen und Buchungsabläufen. Optionale Funktionen mit besonderen Datenschutzimplikationen (z. B. KI-Funktionen, CRM Email Sync) sind opt-in und in der Standardkonfiguration deaktiviert.
Auftragskontrolle	Sorgfältige Auswahl der Unterauftragsverarbeiter; vertragliche Verpflichtung auf gleichwertige Datenschutzstandards (Art. 28 Abs. 4 DSGVO). Regelmäßige Überprüfung der eingesetzten Unterauftragsverarbeiter und Aktualisierung der unter https://help.meetergo.com/de/legal/list-of-subprocessors veröffentlichten Liste.

Ende der Anlage 1