# Auftragsverarbeitung nach Art. 28 DSGVO

Zwischen dem Commitly Kunden (Verantwortlicher oder Auftraggeber) und der Commitly GmbH (Auftragsverarbeiter oder Auftragnehmer) wird nachfolgender Vertrag geschlossen.

## PRÄAMBEL

Zwischen dem Verantwortlichen und dem Auftragsverarbeiter besteht ein Vertrag über die Nutzung der in Ziffer 1 näher bezeichneten Software Commitly (im Weiteren Lizenzvereinbarung) das Auftragsverarbeiters durch den Verantwortlichen. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Umsetzung eigener Geschäftszwecke im Zusammenhang mit dem Dienstleistungsvertrag - eine Übertragung von „Funktionen“ ist ausdrücklich nicht beabsichtigt.

## 1. GEGENSTAND DER VEREINBARUNG

1. Der Nutzer hat die Möglichkeit, bestehende Bankkonten bei deutschen und österreichischen Finanzinstituten mit Commitly zu verbinden und seine Finanzen gemäß den unternehmerischen Erfordernissen aufzubereiten und auf dieser Basis Planungen für zukünftige Zahlungsflüsse zu erstellen. Die Verbindung erfolgt durch Bereitstellung einer Schnittstelle zwischen der kontoführenden Bank und Commitly durch einen externen Dienstleister.
2. Im Rahmen der Verbindung wird im reinen Lesezugriff die Umsatzliste des verbundenen Kontos über eine automatisierte Schnittstelle ausgelesen. Dabei werden primär folgende Informationen übernommen: Datum des Umsatzes (Valuta), Geschäftspartner der Transaktion (Sender oder Empfänger), Beschreibung der Transaktion (Verwendungszweck oder Referenz), Währung, Betrag. Technisch können zusätzliche Daten durch die Bank übermittelt werden.
3. Neben der Erhebung, Verarbeitung und Nutzung von Daten im Auftrag als Hauptzweck werden u.a. personenbezogene Daten im Rahmen der Kunden, Lieferanten und Personalverwaltung sowie für sonstige Zwecke (z. B. Geschäftspartner und Interessentenbetreuung, Hilfe und Support, Analyse und Verbesserung des Dienstleistungsangebots von Commitly, Marktanalysen und Marketingmaßnahmen) erhoben, verarbeitet oder genutzt.
4. Der Gegenstand dieses Auftrags ergibt sich im übrigen aus der bestehenden Lizenzvereinbarung, auf die hier verwiesen wird (im Weiteren „Lizenzvereinbarung“). Dabei handelt es sich um die Verarbeitung personenbezogener Daten (im Weiteren „Daten“) durch den Auftragsverarbeiter für den Verantwortlichen im Zusammenhang mit der Nutzung der Software von Commitly.

# 2. DAUER DER VEREINBARUNG

Die Laufzeit dieses Vertrages entspricht der Laufzeit der Lizenzvereinbarung.

# 3. PFLICHTEN DES AUFTRAGNEHMERS

1. Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen dokumentierten Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.
2. Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.
3. Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind **Anlage 1** zu entnehmen).
4. Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenverarbeitung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.
5. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).
6. Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

7. Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch von ihm beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.
8. Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, in dessen Auftrag zu vernichten. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.
9. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

# 4. TECHNISCH-ORGANISATORISCHE MAßNAHMEN

1. Der Auftragnehmer verpflichtet externe Rechenzentren sowie sonstige Unterauftragsverarbeiter, die innerbetriebliche Organisation so zu gestalten, dass es den besonderen Anforderungen des Datenschutzes gerecht wird. Insbesondere findet die Datenverarbeitung auf Datenverarbeitungsanlagen statt, für die das Rechenzentrum oder der sonstige Unterauftragsverarbeiter alle technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen hat.
2. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen (Einzelheiten in Anlage 1).
3. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

# 5. UNTERAUFTRAGSVERHÄLTNISSE

1. Als Unterauftragsverhältnisse im Sinne dieses Vertrags sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragsverarbeiter z.B. als Telekommunikationsleistungen, Post/ Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Verantwortlichen auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
2. Die Auslagerung auf Unterauftragsverarbeiter oder der Wechsel der bestehenden genehmigten Unterauftragsverarbeiter sind zulässig, soweit der Auftragsverarbeiter die geplante Beauftragung eines Unterauftragsverarbeiters dem Verantwortlichen in angemessener Frist, mindestens jedoch zwei Wochenvorab, schriftlich oder in Textform anzeigt und der Verantwortliche nicht bis zum Zeitpunkt der Ubergabe der Daten gegenüber dem Auftragsverarbeiter schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 4 DSGVO zugrunde gelegt wird. Im Falle des Einspruchs des Verantwortlichen steht dem Auftragsverarbeiter ein außerordentliches Kündigungsrecht sowohl hinsichtlich dieser Vereinbarung als auch bezüglich der Leistungsvereinbarung zu.
3. Der Verantwortliche stimmt der Beauftragung der in der **Anlage 2** vor Beginn der Verarbeitung mitgeteilten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 4 DSGVO zu.
4. Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR und liegt kein Beschluss gemäß Art 45 Abs 3 DSGVO vor, stellt der Auftragsverarbeiter die datenschutzrechtliche Zulässigkeit durch das Ergreifen hinreichender hinreichende Garantien iSd Art 46 DSGVO.Die Weitergabe von personenbezogenen Daten des Verantwortlichen an den Unterauftragsverarbeiter und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

# ANLAGE 1 – TECHNISCH-ORGANISATORISCHE MASSNAHMEN

# 1. VERTRAULICHKEIT (ART. 32 ABS. 1 LIT. B DSGVO)

A. Zutrittskontrolle - Rechenzentrumsräume:

Commitly Kundendaten werden in Rechenzentren von AWS Frankfurt verarbeitet und gespeichert. Es wurden alle erforderlichen Maßnahmen gemäß Art. 32 DSGVO ergriffen.

B. Zugangskontrolle:

- Der Benutzer und Administratorzugriff auf das Commitly System beruht auf einem rollenbasierten Zugriffsberechtigungsmodell. Jeder Nutzer erhält eine eindeutige ID, um sicherzustellen, dass alle Systemkomponenten nur von berechtigten Benutzern und Administratoren genutzt werden können.
- Es existieren technische Policies zur Passwortkomplexität und PasswortRotation.
- Bei Commitly gilt das Prinzip der Minimalberechtigung. Jeder Benutzer erhält nur die Zugriffsrechte, die erforderlich sind, um seine vertraglichen Tätigkeiten durchzuführen. Benutzerkonten werden immer zunächst mit den wenigsten Zugriffsrechten ausgestattet. Für die Einräumung von Zugriffsrechten über die Minimalberechtigung hinaus, muss eine entsprechende Berechtigung vorliegen.
- Einsatz von Firewallsystemen, Virenscanner und Intrusion Detection Systemen auf Commitly Serversystemen
- Auf Commitly IT Equipment (z.B. Notebooks) sind Virenscanner installiert, die eine Malware Erkennung und einen EMail Filter enthalten
- Der Zugriff auf Commitly Serversysteme erfolgt SSH verschlüsselt („Public key“) durch einen BastionHost, der den Zugriff auf Netzwerkgeräte und andere Cloud-Komponenten beschränkt.
- Alle Commitly Serversysteme speichern Daten ausschließlich auf verschlüsselten Datenträgern ab.

C. Zugriffskontrolle:

- Zugriffsberechtigung auf Commitly Produktivsysteme ist auf einen kleinen Kreis von Mitarbeitern (“Commitly Systemadministratoren”) beschränkt

- Alle Zugriffe auf Commitly Produktivsysteme durch Commitly Systemadministratoren werden mit UserID, Zeitstempel und Anlass protokolliert und GoBDkonform für 10 Jahre aufbewahrt.
- Commitly Systemadministratoren haben keinen Zugriff auf die Zugriffsprotokolle
- Es existiert ein internes Kontrollsystem, das sicherstellt, dass die Rechtmäßigkeit für Zugriffe auf Commitly Produktivsysteme regelmäßig stichprobenartig überprüft und diese Stichprobenkontrollen ebenfalls protokolliert werden

D. Trennungskontrolle:

- Datensätze unterschiedlicher Commitly Kunden werden in einer einheitlichen Datenbank speziell markiert (TenantID, softwareseitige Mandantenfähigkeit).
- Test und Produktivdaten sind strikt getrennt in unabhängigen Systemen, Entwicklungssysteme sind ebenfalls unabhängig von Test und Produktivsystemen
- Unterschiedliche Domains Zertifikate für Test und Produktivsysteme

# 2. INTEGRITÄT (ART. 32 ABS. 1 LIT. B DSGVO)

A. Weitergabekontrolle:

- Datenübertragung zwischen Commitly Serversystemen erfolgt ausschließlich innerhalb abgegrenzter und durch BastionHosts abgeschirmter Subsysteme
- Soweit Daten zu beauftragten Partnern übertragen werden, sind diese Datenübertragungskanäle immer TLS verschlüsselt
- Wo dies technisch möglich ist, kommen VPNVerbindungen zum Einsatz
- Soweit dies möglich ist, werden Daten zudem nur in anonymisierter oder pseudonymisierter Form
- weitergeben (z.B. Google anonymizeIP)
- Datenabrufe und Übermittlungsaktivitäten werden protokolliert

B. Eingabekontrolle:

Relevante Einträge und Vorgänge in Commitly werden als Funktion für den Kunden protokolliert.

# 3. VERFÜGBARKEIT UND BELASTBARKEIT (ART. 32 ABS. 1 LIT. B DSGVO)

A. Verfügbarkeitskontrolle:

- Es werden regelmäßig automatische Sicherungskopien und Backups aller Commitly Kundendaten erstellt
- Es gibt ein Konzept zur Rekonstruktion der Datenbestände und zudem eine regelmäßige Überprüfung, dass die Datensicherungen auch tatsächlich wieder eingespielt werden können (Datenintegrität der Backups)
- Commitly Produktivsysteme sind mehrfach redundant ausgelegt

B. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO):

- Mehrfachredundante Auslegung von Serversystemen und Datenbanken • Backups werden regelmäßig auf Wiedereinspielbarkeit geprüft

# 4. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG (ART. 32 ABS. 1 LIT. D DSGVO; ART. 25 ABS. 1 DSGVO)

1. Datenschutzmanagement ist ein integraler Bestandteil der Prozesse und Aktivitäten der Commitly GmbH, mit entsprechender Planung zu Maßnahmen zum Umgang mit Chancen/Risiken und die Ausstattung mit angemessenen Ressourcen, Kompetenzen, Awareness und Kommunikation.
2. Dediziertes IncidentResponseManagement wurde nicht eingerichtet, ist aber fixer Bestandteil des Datenschutzmanagements.
3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)
4. Auftragskontrolle:
   - Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Verantwortlichen
   - Klare, eindeutige Weisungen
   - Verhinderung von Zugriffen unbefugter Dritter auf die Daten
   - Verbot, Daten in unzulässiger Weise zu kopieren
   - Vereinbarungen über Art des Datentransfers und deren Dokumentation
   - Kontrollrechte durch den Auftraggeber
   - Strenge Auswahl der Dienstleister
   - Nachkontrollen

Commitly GmbH (Stand: 26.08.2022)

# ANLAGE 2 – UNTERAUFTRAGSVERARBEITER

Der Verantwortliche stimmt der Beauftragung der nachfolgenden Unterauftragsverarbeiter zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 24 DSGVO:

| Nr | Firma | Anschrift | Leistung | Drittlandsübermittlungen |
|---|---|---|---|---|
| 1 | finAPI GmbH (Schnittstellenanbieter) | Ainmillerstraße 11, 80801 München | Einheitliche Schnittstelle zum Abruf von Online Banking Informationen | |
| 2 | Chargebee Inc. (Abo-Verwaltung) | 340 S Lemon Avenue, #1537, Walnut, California 91789, USA | Abo Management Software | |
| 3 | PayPal (Europe) S.à r.l. et Cie, S.C.A. (Zahlungsabwicklung) | 22-24 Boulevard Royal L-2449, Luxembourg | Abwicklung der Zahlungen zwischen Commitly und seinen Nutzern | Standardvertragsklauseln https://www.chargebee.com/docs/2.0/eu-gdpr.html |
| 4 | Intercom Inc. (Customer Experience) | 55 2nd Street, 4th Floor, San Francisco, California, 94105, USA | Medium für Kommunikation und Hilfebereich innerhalb unseres Produktes/ unserer Produkte | Standardvertragsklauseln https://www.intercom.com/de/legal/data-processing-agreement |
| 5 | Amazon Web Services Inc. (“AWS Frankfurt”) | 410 Terry Avenue North, Seattle WA 98109, USA | Hosting und Betriebsaufgaben | Standardvertragsklauseln https://d1.awsstatic.com/whitepapers/Security/navigating-compliance-with-eu-data-transfer-requirements.pdf |
| 6 | Mailchimp (Newsletter Management) | Rocket Science Group, Leon Ave NE, Suite 500, Atlanta, GA 30308, USA | Versendung unseres Newsletters an registrierte Interessenten sowie Versand von transaktionalen Emails | Standardvertragsklauseln https://mailchimp.com/de/legal/data-processing-addendum/ |
| 7 | Zendesk (Support Management) | Zendesk, Inc., 989 Market Street #300, San Francisco, CA 94102, USA | Kundensupport-System | Standardvertragsklauseln https://www.zendesk.de/blog/eu-us-data-transfers-after-schrems-ii/ https://support.zendesk.com/hc/en-us/articles/4408883599130 |

| | | | | |
|---|---|---|---|---|
| 8 | Pipedrive (CRM Management) | PIPEDRIVE IRELAND LIMITED, 4th Floor, 7/8 Wilton Terrace, Dublin 2 | Kundenkommunikation | Standardvertragsklauseln<br>https://www.pipedrive.com/en/terms-of-service<br>https://www.pipedrive.com/en/privacy |
| 9 | Google Inc. | Amphitheatre Parkway, Mountain View, CA 94043, USA | Interne und externe Kommunikation über Google Workspace | Standardvertragsklauseln<br>https://workspace.google.com/terms/dpa_terms.html |