AUFTRAGSVERARBEITUNGS-Vertrag (AVV) gemäß Art. 28 DSGVO

(Version 27.02.2025)

ZWISCHEN

Auftraggeber
Näher bezeichnet siehe Abschnitt Vertragsparteien

UND

Auftragnehmer
Domonda GmbH
Wattgasse 48
1170 Wien

Präambel

Der Auftragnehmer ist ein Software- und Servicedienstleistungsunternehmen, welches Buchhaltungs- und Buchhaltungsvorerfassungssoftware (Software) zur Nutzung über das Internet (Service) bereitstellt (sgn. Software as a Service - SaaS). Der Service richtet sich ausschließlich an gewerbliche Auftraggeber.

Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Der Gegenstand des Auftrags ergibt sich aus dem dazugehörigen mit dem Auftraggeber geschlossenen Vertrag über entsprechende Nutzungsrechte an der Software domonda (im Folgenden Leistungsvereinbarung). Sofern der Auftraggeber zu einem späteren Zeitpunkt weitere Nutzungsrechte oder sonstige zusätzliche Leistungen beauftragt, so gilt diese Vereinbarung entsprechend auch für diese Leistungen.
Aus dem Servicedienstleistungsvertrag ergeben sich Gegenstand und Dauer des Auftrages sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

Art der Daten

Gegenstand der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten sind die in der Tabellen angeführten Datenarten und -kategorien, die allesamt in einer normalen Schutzklasse von personenbezogenen Daten liegen (nach Art. 9 – EU-DSGVO – Verarbeitung besonderer Kategorien personenbezogener Daten). Der Auftraggeber trägt dafür Sorge, in das Datenverarbeitungssystem domonda keine “personenbezogenen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen”, weiteres keine “genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person” hochzuladen.

Art der Daten	**Art und Zweck der Datenverarbeitung**	**Betroffene Personen**
Firmendaten samt Namen von Mitarbeitern auf Rechnungen und Sonstigen Dokumenten (Firmenname, Firmenanschrift, Vorname und Nachname des Ansprechpartners bzw Sachbearbeiters lt Rechnung, weiter Firmendaten wie UID, Telefonnummer, E-Mail-Adressen). **Normaler Schutzbedarf**	Verarbeitung zum Zweck der Vertragserfüllung und Gewährleistung von domonda Funktionen. Der Auftraggeber lädt im Zuge der Nutzung des domonda Systems Daten mit personenbezogenen Informationen in das System, welche dann vom System gespeichert und tlw. für strukturierte Datenaufbereitung ausgelesen werden.	Sachbearbeiter auf Seiten von B2B Kunden des Auftraggebers, Mitarbeiter des Auftraggebers
Personenbezogene Daten auf Rechnungen und Sonstigen Dokumenten (Name, Anschrift, Kundennummer, Email),	Verarbeitung zum Zweck der Vertragserfüllung und gewährleistung von domonda Funktionen. Der Auftraggeber lädt im Zuge der Nutzung des	B2C Kunden des Auftraggebers

Rechnungsdaten mit Kaufpositionen **Normaler Schutzbedarf (Der Auftraggeber trägt dafür Sorge, keine personenbezogenen Daten mit höherem Schutzbedarf seiner Kunden ins System zu laden)**	domonda Systems Daten mit personenbezogenen Informationen in das System, welche dann vom System gespeichert und tlw. für strukturierte Datenaufbereitung ausgelesen werden.	
Bank-Verbindungsdaten von Firmenvertretern , (Kontoverbindungen, Kreditkartennummern, Paypal) **Normaler Schutzbedarf**	Verarbeitung zum Zweck der Vertragserfüllung und gewährleistung von domonda Funktionen. Der Auftraggeber und seine Mitarbeiter verbinden Ihre Bankkonten, Kreditkarten und Paypalkonten mit domonda. Domonda speichert diese Verbindungsdaten zur sofortigen und späteren Synchronsisierung von TRansaktionsdaten.	Mitarbeiter des Auftraggebers
Zahlungstransaktions-daten - Gegebenenfalls Daten von Dritten aus Kontoübersicht: Name, IBAN, Verwendungszweck, Betrag) **Normaler Schutzbedarf (Der Auftraggeber trägt dafür Sorge, keine personenbezogenen Daten mit höherem Schutzbedarf seiner Kunden ins System zu laden)**	Verarbeitung zum Zweck der Vertragserfüllung und gewährleistung von domonda Funktionen. Der Auftraggeber und seine Mitarbeiter verbinden Ihre Bankkonten, Kreditkarten und Paypalkonten mit domonda. Domonda lädt Zahlungstransaktionedaten ins System und verarbeitet diese für die Darstellung und zur Verbindung mit Belegdaten.	B2B-Geschäftspartner des Auftraggebers. B2C Kunden des Auftraggebers

Applikationsnutzerdaten (Zugangsdaten Username und Passwort, Vorname und Nachname, Log-Informationen) **Normaler Schutzbedarf**	Verarbeitung zum Zweck der Vertragserfüllung und gewährleistung von domonda Funktionen. Die Mitarbeiter des Auftraggebers benötigen Zugangsdaten für das System, weiters benötigt das System Identifikationsdaten der Person zur Darstellung von Loginfos für gesetzte Aktionen (Nachvollziehbarkeit von Tätigkeiten in domonda). Zur Verbesserung von domonda werden darüber hinaus Aktivitäten der Benutzer gespeichert (Logging)	Mitarbeiter des Auftraggebers

Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen 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.

(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 der 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, Daten Übertragbarkeit, 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-Folgenabschätzung, vorherige Konsultation).
(6) Der Auftraggeber 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 Verarbeitungs Ergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber in dessen Auftrag zu vernichten.
(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.

Ort der Durchführung der Datenverarbeitung

Datenverarbeitungstätigkeiten werden je nach Nutzungsumfang in domonda zumindest zum Teil auch außerhalb der EU bzw. des EWR durchgeführt, und zwar in den USA und in Bosnien Herzegowina. Das angemessene Datenschutzniveau ergibt sich aus den Standarddatenschutz- klauseln nach Art 46 Abs 2 lit c und d DSGVO.

Sub-Auftragsverarbeiter

Der Auftragnehmer ist befugt, Unternehmen als Sub-Auftragsverarbeiter hinzuziehen:

- Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab.
- Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen.
- Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.
- Der Auftragnehmer kann Sub-Auftragsverarbeiter zur manuellen Belegverifizierung und Führung der Buchhaltung, zur IT-gestützten Verarbeitung von Belegdaten, zum Betrieb des SW-Systems und von Subsystemen hinzuziehen.

Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmen durchgeführt.

Name und Anschrift des Subunternehmens	**Beschreibung der Teilleistung**

Amazon Web Services EMEA SARL, Niederlassung Deutschland, Marcel-Breuer-Str. 12, D-80807 München	Server-Cloud-Hosting in der Datenzone Frankfurt am Main.
Blumatix Consulting GmbH Schwarzstraße 48 5020 Salzburg – Austria	Automatisierte Beleg-Datenextraktion
Tink Germany GmbH Gottfried-Keller-Strasse 33 81245 München	Anbindung und Synchronisierung von Zahlungskonten, Paypal Konten und Kreditkonten. Verarbeitung von Konto und Transaktionsdaten. Ausführung von Kundenzahlungen in domonda. Die Nutzung dieses Unternehmens ist optional. Der Auftraggeber kann gegen diese Nutzung entscheiden, in dem er keine Bankanbindung per API / AISP bzw. keine Zahlung per API / PISP durchführt.
Google Ireland Limited Gordon House, Barrow Street Dublin 4 Ireland	Verschicken von Benachrichtigungs E-Mails, Routing von an domonda weitergeleitete E-Mails.
The Rocket Science Group, LLC 675 Ponce de Leon Ave NE Suite 5000 Atlanta, GA 30308 USA	Verschicken von Benachrichtigungs E-Mails. Funktionale Einschränkung: Nur relevant, wenn Sie einen Demo-Account bei domonda anlegen. Dann werden automatisierte Emails zu Werbezwecke über Mailchimp versendet.
LogRocket 87 Summer St. Boston, MA 02110	Software zur Datenanalyse, Tracking von Userverhalten zur Fehlerbehebung in domonda.
Functional Software, Inc. dba Sentry, 132 Hawthorne Street, San Francisco, CA 94107.	Analyseplattform für Fehlertracking.

Alfa Consulting d.o.o. Rustempašina 23 (Mellain centar), 71000 Sarajevo - Bosnien Herzegowina	Manuelle Beleg-Verifizierung und Buchhaltungsdienstleistungen innerhalb von domonda SaaS. Die Nutzung dieses Unternehmens ist optional. Der Auftraggeber kann gegen diese Nutzung entscheiden, in dem er keinen Zusatz-SLA (SLA Vollständigkeit, SLA Korrektheit, SLA Buchhaltung) zur Nachbearbeitung seiner Belege durch Domonda abschließt.
Slack Technologies, 500 Howard St, San Francisco, CA 94105, USA	In-App Chat zur Hilfestellung und Problemlösung in domonda. Die Nutzung dieses Unternehmens ist optional. Der Auftraggeber kann gegen diese Nutzung entscheiden, in dem er beim Onboarding auf die Möglichkeit des Supportkanals über den InApp-Chat verzichtet.
Zendesk Neue Schönhauser Str. 3-5 10178 Berlin Germany	Support Ticketing-System zur Hilfestellung und Problemlösung in domonda.

Vertragsparteien

Für Auftraggeber

Firmenname: _____

Name des Unterzeichners, Funktion: _____

Ort, Datum: _____

Unterschrift

Für Auftragnehmer

Firmenname: Domonda GmbH

Name des Unterzeichners, Funktion: Mathias Kimpl, CEO

Ort, Datum: Wien, am 27. Februar 2025

Unterschrift (siehe digitale Signatur)

Signiert von:	Mathias Kimpl
Datum:	27.02.2025 17:28:53

A-TRUST

Dieses Dokument ist digital signiert!

Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr 910/2014 vom 23. Juli 2014 ("eIDAS-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.

Prüfinformation: Informationen zur Prüfung der elektronischen Signatur finden Sie unter: www.a-trust.at/pdf

Anlage 1 - Technisch-Organisatorische Maßnahmen

A. Vertraulichkeit

Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch:

☒ Schlüssel	☒ Magnet- oder Chipkarten
☒ Elektrische Türöffner	☐ Portier
☒ Sicherheitspersonal	☒ Alarmanlagen
☐ Videoanlage	☒ Einbruchshemmende Fenster und/oder Sicherheitstüren
☐ Anmeldung beim Empfang mit Personenkontrolle	☒ Begleitung von Besuchern im Unternehmensgebäude
☐ Tragen von Firmen-/Besucherausweisen	☐ Sonstiges:

Externe Mitarbeiterinnen und Mitarbeiter, die über einen längeren Zeitraum beim Auftragnehmer tätig sind und Zugang zu vertraulichen Unterlagen und Daten erhalten könnten, werden schriftlich (im Rahmen von Geheimhaltungsverpflichtungen) auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen verpflichtet.
Für Fremdpersonal, das nur kurzfristig oder einmalig zum Einsatz kommt, gelten die gleichen Regeln wie für Besucherinnen und Besucher, d.h. dass etwa der Aufenthalt in sicherheitsrelevanten Bereichen nur in Begleitung von unternehmenseigenem Personal erlaubt ist.

Die Serverinfrastruktur wird bei Amazon AWS (Amazon Web Services EMEA) betrieben, die physische Zutrittsberechtigungsstruktur wird auf das Notwendigste beschränkt. (https://aws.amazon.com/de/compliance/data-center/controls/) MITARBEITERZUGANG ZU RECHENZENTREN: Nur autorisiertes AWS-Personal erhält Zugang zu den physischen Rechenzentren. Alle Mitarbeiter, die Zugang zu einem Rechenzentrum benötigen, müssen zunächst einen Antrag auf Zugang stellen und eine gültige geschäftliche Begründung vorlegen. Dieser Antrag wird basierend auf dem Prinzip geringstmöglicher Berechtigungen gewährt, d. h. Mitarbeiter müssen in der Anfrage angeben, auf welche Ebene des Rechenzentrums und für welchen Zeitraum sie Zugang benötigen. Die Anfrage wird geprüft und von autorisiertem Personal genehmigt. Der Zugang wird nach Ablauf des beantragten Zeitraums wieder entzogen. Mitarbeiter mit Zugang zu einem Rechenzentrum sind durch ihre Berechtigungen auf bestimmte Bereiche beschränkt. ZUGANG VON DRITTEN ZU RECHENZENTREN: Der Zugang von Dritten muss von autorisierten AWS-Mitarbeitern beantragt werden, die auch eine gültige geschäftliche Begründung für diesen Zugang vorlegen müssen. Dieser Antrag wird basierend auf dem Prinzip geringstmöglicher Berechtigungen gewährt, d. h. Mitarbeiter müssen in der Anfrage angeben, auf welche Ebene des Rechenzentrums und für welchen Zeitraum sie Zugang benötigen. Diese Anfragen werden von autorisiertem Personal genehmigt. Der Zugang wird nach Ablauf des beantragten Zeitraums wieder entzogen. Mitarbeiter mit

Zugang zu einem Rechenzentrum sind durch ihre Berechtigungen auf bestimmte Bereiche beschränkt. Personen mit einem Besucherausweis müssen diesen bei Ankunft am Standort vorlegen und werden von autorisiertem Personal angemeldet und begleitet.

Zugangskontrolle: Schutz vor unbefugter Systembenutzung durch:

☒ Kennwörter (einschließlich entsprechender Policy, z.B. Mindestlängen von mind. 8 Zeichen und drei der vier Kriterien von Großbuchstaben, Kleinbuchstaben, Sonderzeichen, Zahl)	☒ Verschlüsselung von Datenträgern
☒ Automatische Sperrmechanismen	☐ Sonstiges:
☐ Zwei-Faktor-Authentifizierung	

Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:

☐ Standard-Berechtigungsprofile auf „need to know-Basis“	☒ Standardprozess für Berechtigungsvergabe
☒ Protokollierung von Zugriffen	☒ Sichere Aufbewahrung von Speichermedien
☒ Periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten	☒ Datenschutzgerechte Wiederverwendung von Datenträgern
☒ Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger	☒ Clear-Desk/Clear-Screen Policy
☐ Sonstiges:	

Datenzugriffe auf das System sind über Row-Level-Security in der Datenbank am direkten Datenpunkt geschützt und sind so logisch von der Applikationsschicht getrennt. Eine Mandantenfähigkeit ist so auf technisch unterster Ebene geschützt und gewährleistet.

Admin Accounts in der Applikation sind getrennt von Standard-Accounts, Mitarbeiter erhalten nur zur Erledigung ihrer Aufgaben Zugriff auf personenbezogene Daten. Das Berechtigungskonzept differenziert nach Leseberechtigung, Schreibberechtigung und Löschrechten.
Usersessions verfallen nach 30 Minuten Inaktivität.

Bring-Your-Own-Device-Policy: Der Zugriff mit eigenen Geräten ist nur in definierten Ausnahmefällen gestattet. Der Zugriff auf die relevanten personenbezogenen Daten ist dabei nur in flüchtiger Form über den Webbrowser möglich, eine lokale Speicherung über die Policy geregelt.

Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert aufbewahrt.

☐ Ja	☒ Nein

Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

☐ Ja	☒ Nein

B. DatenIntegrität

Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:

☒ Verschlüsselung von Datenträgern	☒ Verschlüsselung von Dateien
☐ Virtual Private Networks (VPN)	☐ Elektronische Signatur
☒ Sonstiges: Das System verschlüsselt sämtliche Kommunikation zwischen dem Browser des Kunden und dem domonda-System mittels TLS (https im Browser).	

Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch:

☒ Protokollierung	☒ Dokumentenmanagement
☐ Sonstiges:	

C. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:

☒ Backup-Strategie (online/offline; on-site/off-site)	☒ Unterbrechungsfreie Stromversorgung (USV, Dieselaggregat)
☒ Virenschutz	☒ Firewall
☒ Meldewege und Notfallpläne	☒ Security Checks auf Infrastruktur- und Applikationsebene und Patch- und Schwachstellenmanagement
☒ Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum	☒ Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern

☒ Sonstiges: Branderkennung und -Bekämpfung.	

Branderkennung und -Bekämpfung: Die Serverinfrastruktur wird bei Amazon AWS (Amazon Web Services EMEA) betrieben. Die AWS-Rechenzentren sind mit automatischen Geräten zur Branderkennung und -bekämpfung ausgestattet. Die Branderkennungssysteme setzen Rauchsensoren in vernetzten, mechanischen und Infrastrukturbereichen ein. Diese Bereiche sind darüber hinaus durch Brandbekämpfungssysteme geschützt.

Rasche **Wiederherstellbarkeit:**

☒ Ja	☐ Nein

D. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen und Verpflichtung der Beschäftigten zur Vertraulichkeit und Verschwiegenheitspflicht:

☒ Ja	☐ Nein

Incident-Response-Management:

☒ Ja	☐ Nein

Datenschutzfreundliche Voreinstellungen:

☐ Ja	☒ Nein

Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers durch:

☒ Eindeutige Vertragsgestaltung	☐ Formalisiertes Auftragsmanagement
☒ Strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS)	☐ Vorabüberzeugungspflicht
☐ Nachkontrollen	☐ Sonstiges: