Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO

Vereinbarung
zwischen dem/der

ADRESSBLOCK

- Verantwortlicher – nachstehend Auftraggeber genannt -

und der

untermStrich Software GmbH
Kernhofer Straße 9
10317 Berlin

- Auftragsverarbeiter – nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

Fernzugriffe im Rahmen von Prüfungs- und/oder Wartungsarbeiten an Arbeitsplatzsystemen.
Dies wird erst nach Freigabe durch den jeweiligen Berechtigten/zuständigen Mitarbeiter des Auftraggebers durchgeführt.

(2) Dauer

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung des Wartungsvertrags.

2. Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: *Support und Schulung der untermStrich Software Lösung bzw. beauftragte Dienstleistungen.*

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

- Personenstammdaten
- Kommunikationsdaten (z.B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Daten die der Kunde im Rahmen der Dienstleistung bzw. des Supports von sich aus zur Verfügung stellt.

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Kunden
- Beschäftigte
- Ansprechpartner

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß den Anforderungen der DSGVO erfolgt und den Schutz für die Rechte und Freiheiten der betroffenen Person gewährleistet. Der Auftraggeber ergreift in seinem Verantwortungsbereich gemäß Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen, um die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.

(2) Die aktuellen technischen und organisatorischen Maßnahmen des Auftragnehmers sind unter diesem https://kunden.untermstrich.com/downloads.html einsehbar. Der Auftragnehmer stellt klar, dass es sich bei den unter dem Link aufgeführten technischen und organisatorischen Maßnahmen lediglich um Beschreibungen technischer Art handelt, welche nicht als Bestandteil dieser Vereinbarung anzusehen sind.

(3) Der Auftragnehmer betreibt ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 lit. d) DSGVO.

(4) Der Auftragnehmer passt die getroffenen Maßnahmen im Laufe der Zeit an die Entwicklungen beim Stand der Technik und die Risikolage an. Eine Änderung der getroffenen technischen und organisatorischen Maßnahmen bleibt dem Auftragnehmer vorbehalten, sofern das Schutzniveau nach Art 32 DSGVO nicht unterschritten wird.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter.

(2) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

5. Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Artt. 28 bis 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Frau Kerstin Gruber untermStrich software GmbH, +43 3862 58106; dsgvo@untermstrich.com benannt.
b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.
c) Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
d) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DSGVO - Einzelheiten in Anlage 1.
e) Die Verpflichtung, angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III DSGVO genannten Rechte der betroffenen Person nachzukommen.
f) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
g) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
h) Soweit der Auftraggeber seinerseits 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 beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.
i) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die 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 Person gewährleistet wird.
j) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Unterauftragsverhältnisse

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter im Sinne des Art. 28 DSGVO zur Vertragserfüllung einzusetzen.

(2) Die aktuell eingesetzten weiteren Auftragsverarbeiter sind in Anlage 2 aufgeführt. Der Auftraggeber erklärt sich mit deren Einsatz einverstanden.

(3) Der Auftragnehmer informiert den Auftraggeber, wenn er eine Änderung in Bezug auf die Hinzuziehung oder die Ersetzung weiterer Auftragsverarbeiter beabsichtigt. Der Auftraggeber kann gegen derartige Änderungen Widerspruch erheben.

(4) Der Widerspruch gegen die beabsichtigte Änderung kann nur aus einem sachlichen Grund innerhalb von 2 Wochen nach Zugang der Information über die Änderung gegenüber dem Auftragnehmer erhoben werden. Im Fall des Widerspruchs kann der Auftragnehmer nach eigener Wahl die Leistung ohne die beabsichtigte Änderung erbringen oder - sofern die Erbringung der Leistung ohne die beabsichtigte Änderung für den Auftragnehmer nicht zumutbar ist - die von der Änderung betroffene Leistung gegenüber dem Auftraggeber innerhalb einer angemessenen Frist (mindestens 2 Wochen) nach Zugang des Widerspruchs einstellen.

(5) Erteilt der Auftragnehmer Aufträge an weitere Auftragsverarbeiter, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag auf den weiteren Auftragsverarbeiter zu übertragen. Der Auftragnehmer stellt insbesondere durch regelmäßige Überprüfungen sicher, dass die weiteren Auftragsverarbeiter die technischen und organisatorischen Maßnahmen einhalten.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO.

(4) Der Auftragnehmer hat für die aus einer Wahrnehmung der Kontrollrechte des Auftraggebers einen angemessenen Vergütungsanspruch, der auf den marktüblichen Stundensätzen und dem für das Personal des Auftragnehmers erforderlichen Zeitaufwand für die Mitwirkung an der Maßnahme beruht.

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

9. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(Auftragnehmer)	(Auftraggeber)
……	……
(Ort, Datum)	(Ort, Datum)
untermStrich® software GmbH Kernerstraße 3 | D | 10317 Berlin www.untermStrich.com	
_____	_____
untermStrich software GmbH Helmut Geilersdorfer	(Unterschrift & Stempel)
	……
	(Name in Druckschrift)

Anlage 1 – Technisch-organisatorische Maßnahmen

TOM untermStrich Deutschland

untermStrich Deutschland

Datenschutzmanagement

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

- Regelmäßige Mitarbeiterschulungen
- Regelmäßige Überprüfung der Sicherheitsmaßnahmen
- Risikoanalyse (Folgenabschätzung)
- DSMS Intervalid

Eingabekontrolle

Gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingabe, Änderung und Löschung der Daten
- Protokollierung der Änderungen an Daten, Anwendungen und Systemen
- Protokollierung der Administrator-Aktivitäten
- Regelmäßige Löschung der Protokolldaten
- Erfassung gescheiterter Zugriffsversuche

Verfügbarkeitskontrolle

Gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Firewall
- Virenschutz (Auf allen Clients und direkt im Mailserver)
- Feuer-und Rauchmeldeanlagen
- Keine eignenen Server. Server siehe untermStrich Österreich.

Weitergabekontrolle

Gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Verschlüsselung der Datenträger, vor allem alle mobilen Geräte/Laptops
- Keine USB Sticks o.ä. im Einsatz
- Nutzung von Echtdaten nur in anonymisierter Form
- Passwortschutz einzelner Dokumente mit getrennter Kennwortübermittlung
- Firewall mit IDP und Applikation Firewall (Mod-Security), VPN

- Nachweis über Versand, Inventarisierung und Zerstörung von Datenträgern
- Dokumentation der Empfänger von Daten und der Zeitspanne der geplanten Überlassung bzw. vereinbarten Löschfristen
- Externe Dienstleister:
- Beauftragung externe Dienstleister nur mit Informationssicherheitsmanagementsystem entsprechend ISO 27001.
- Zugriff externe Dienstleister nur mit Auftragsverarbeitungsvertrag nach Art 28 DGSVO.

Zugangskontrolle

Verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Festlegung der Berechtigung zum Betrieb der Datenverarbeitungsgeräte und Absicherung der Geräte durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme.

- Authentifizierung mit Benutzerkennung und Passwort für den Client und für alle Dienste, zusätzlich VPN.
- Sicherstellung von Passwortanforderungen durch die Erstellung einer Passwortrichtlinie.
- Berechtigungskonzept auf System- und Netzwerkebene inkl. Benutzerberechtigungen und Profile.
- Einrichtung einer automatischen Bildschirmsperrung.
- Einrichtung von Vertretungsregelungen.

Zugriffskontrolle

Gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Berechtigungskonzept; differenzierte Rechte für Lesen, Verändern oder Löschen von Daten entsprechend der Aufgaben der Mitarbeiter
- Systemseitige Umsetzung der definierten Berechtigungen.
- Keine eigenen Testsysteme. Testsysteme siehe untermStrich Österreich.
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten.
- Prozess zur Rechtevergabe; Verantwortlich, Entscheidung über Vergabe/Entzug von Rechten, Kommunikation bei Änderungen, Dokumentation.
- Berechtigungen werden bei Abteilungs-/Funktionswechsel und Austritt eines Mitarbeiters
- aktualisiert oder entzogen, Änderungen protokolliert.
- Datenschutzkonforme Vernichtung / Löschung von Daten, die eine Kenntnisnahme durch Unbefugte ausschließt.
- Protokollierung der Vernichtung von Daten und Datenträgern.
- Einsatz von Aktenvernichtern und Dienstleistern zur Datenvernichtung.
- Anzahl der Administratoren auf das Notwendigste reduziert.
- Sichere Aufbewahrung von Datenträgern; für Unberechtigte nicht zugänglich.
- Verschlüsselungsmöglichkeit von E-Mails mit sensiblen, personenbezogenen Daten.

Zutritt

Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Gebäudesicherung :
- Personenkontrolle beim Empfang.
- Sicherheitsschlösser und Chip für den Eingang.
- Versperrung des Eingangs, wenn der Empfang nicht besetzt ist.
- Sicherung der Räume:
- Schlüsselverwaltung (Dokumentation von Ausgabe, Rücknahme bzw. Verlust, sichere Aufbewahrung)
- Sicherheitsverglasung
- Versperrung von Daten aus der Personalabteilung oder anderen personenbezogenen Daten
- Sicherung der Datenträger:
- Keine Server. Server siehe untermStrich Österreich.
- Nicht verbaute Datenträger werden versperrt aufbewahrt.

Onboarding/Offboarding

Mitarbeiteraufnahme/Mitarbieteroffboarding

- Onboarding:
- Erstellung eigener Username/Passwort mit passender Berechtigungsstruktur.
- Zuweisung Office 365 Account, Telefon, TeamViewer.
- VPN Zugriff, wenn VPN notwendig.
- Schlüsselübergabe, wenn Schlüssel notwendig.
- Offboarding
- Deaktivierung des Users zum Austrittsdatum.
- Deaktivierung von Office 365 Account, Telefon, TeamViewer.
- Deaktivierung des VPN Zugriffs
- Schlüsselübergabe

Anlage 2 – Unterauftragnehmer

Firma Unterauftragnehmer	Anschrift Land	Leistung
Koell Consulting Gmbh, Markus Köll	Spitzäckerweg 3 A-6460 Imst	Beratung Datenschutz
Michael Fußer	Duttenhoferstraße 1 D-78628 Rottweil	Support und Dienstleistungen