Auftraggeber (Verantwortlicher)
Name / Firma: _____
Anschrift: _____
_____
Vertreten durch: _____

(nachfolgend: "Auftraggeber")

Auftragnehmer (Auftragsverarbeiter)
Dirk Hildebrand (als selbständiger Einzelunternehmer)
Forstfeldstr. 2
34123 Kassel

(nachfolgend: "Auftragnehmer")

– zusammen auch "Parteien" –

§ 1 Gegenstand und Dauer der Auftragsverarbeitung

1.1 Gegenstand

Dieser Vertrag regelt die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers gemäß Art. 28 DSGVO. Zweck der Verarbeitung ist die Entwicklung, Bereitstellung, Wartung, Betreuung und der Support von Softwareanwendungen sowie die Erbringung von IT-Dienstleistungen für den Auftraggeber. Die Verarbeitung erfolgt insbesondere, soweit dies zur Entwicklung, Anpassung, Fehleranalyse, Administration, Pflege, Sicherung und Unterstützung von Anwendungen, Systemen und Diensten des Auftraggebers erforderlich ist. Dies kann auch personenbezogene Daten von Mitarbeitern, Kunden, Geschäftspartnern und sonstigen betroffenen Personen des Auftraggebers umfassen, die in den vom Auftragnehmer betreuten Anwendungen, Microsoft-365-Diensten oder sonstigen IT-Systemen des Auftraggebers verarbeitet werden. Der Auftragnehmer erbringt dabei insbesondere folgende Leistungen:

- Entwicklung und Betreuung individueller Softwareanwendungen (Apps)
- Administration und Support für Microsoft 365-Dienste (Exchange Online, Teams, SharePoint, Entra ID u. a.)
- Verwaltung von Microsoft 365-Mandanten und Nutzerkonten
- Konfiguration von Sicherheits- und Compliance-Einstellungen
- Sonstige IT-Dienstleistungen gemäß der zugrunde liegenden Beauftragung oder Vereinbarung

1.2 Dauer

Die Dauer richtet sich nach der Laufzeit der zugrunde liegenden Beauftragung oder Vereinbarung. Die Regelungen zur Löschung und Rückgabe von Daten (§ 8) gelten darüber hinaus fort.

§ 2 Art der Daten und Kreis der Betroffenen

2.1 Kategorien personenbezogener Daten

- Stammdaten und Kontaktdaten (z. B. Name, Anschrift, E-Mail-Adresse, Telefonnummer, Funktion, Organisationseinheit)
- Kommunikationsdaten und Kommunikationsinhalte, soweit sie im Rahmen der betreuten Systeme verarbeitet werden
- Benutzer-, Zugangs- und Berechtigungsdaten (z. B. Benutzerkonten, Benutzernamen, Rollen, Gruppen, Lizenzzuweisungen, technische Kennungen)
- Organisations-, Vertrags- und Beschäftigtendaten, soweit sie für Entwicklung, Support, Administration oder Fehleranalyse relevant sind
- Protokoll-, Nutzungs-, Diagnose- und Metadaten aus Anwendungen, Microsoft-365-Diensten und sonstigen betreuten IT-Systemen
- Inhaltsdaten aus den vom Auftraggeber bereitgestellten oder betreuten Anwendungen und Diensten, soweit deren Verarbeitung zur Leistungserbringung erforderlich ist

Besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO sowie personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten im Sinne von Art. 10 DSGVO werden durch den Auftragnehmer nur verarbeitet, soweit dies im Einzelfall vom Auftrag umfasst, rechtlich zulässig und zur Leistungserbringung erforderlich ist. In diesen Fällen sind durch den Auftraggeber geeignete Weisungen zu erteilen; der Auftragnehmer trifft insoweit angemessene zusätzliche Schutzmaßnahmen entsprechend dem jeweiligen Risiko.

2.2 Kreis der betroffenen Personen

- Mitarbeiter, Beschäftigte, Organmitglieder und sonstige interne Nutzer des Auftraggebers
- Kunden, Interessenten, Mitglieder, Lieferanten, Dienstleister und sonstige externe Kontakte des Auftraggebers
- Sonstige natürliche Personen, deren personenbezogene Daten im Rahmen der vereinbarten Leistungen, betreuten Anwendungen, Dienste oder IT-Systeme des Auftraggebers verarbeitet werden

§ 3 Weisungsgebundenheit

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers (Art. 28 Abs. 3 lit. a DSGVO), es sei denn, er ist hierzu durch das Recht der Europäischen Union oder der Mitgliedstaaten verpflichtet. Weisungen erfolgen in der Regel schriftlich oder per E-Mail; mündliche Weisungen sind unverzüglich schriftlich zu bestätigen. Hält der Auftragnehmer eine Weisung für einen Verstoß gegen datenschutzrechtliche Bestimmungen, ist er berechtigt und verpflichtet, den Auftraggeber darauf hinzuweisen.

§ 4 Technisch-organisatorische Maßnahmen (TOMs)

Der Auftragnehmer trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO. Dabei ist zu berücksichtigen, dass der Auftragnehmer als Einzelunternehmer tätig ist, ein Büro anmietet und Leistungen teilweise auch im Home-Office erbringt. Die Maßnahmen umfassen insbesondere:

- Zugang zu Endgeräten, Benutzerkonten und betreuten Kundensystemen nur mit individuellen, starken Passwörtern; soweit verfügbar und zumutbar wird zusätzlich Mehrfaktor-Authentifizierung eingesetzt
- Verarbeitung personenbezogener Daten nur auf Geräten und in Arbeitsumgebungen, die gegen unbefugten Zugriff geschützt sind; hierzu gehören insbesondere Gerätesperren, passwortgeschützte Benutzerkonten und ein sorgfältiger Umgang mit Arbeitsmitteln im Büro und im Home-Office
- Zugriffe auf personenbezogene Daten und Kundensysteme erfolgen nur im zur Vertragserfüllung erforderlichen Umfang und nach dem Prinzip der minimalen Rechtevergabe
- Zugangsdaten werden nicht offen abgelegt, sondern in einem geeigneten, geschützten Passwort-Manager oder in vergleichbar gesicherter Form verwahrt
- Die vom Auftragnehmer eingesetzten Endgeräte, Betriebssysteme und wesentlichen Softwarekomponenten werden regelmäßig aktualisiert; sicherheitsrelevante Updates werden zeitnah eingespielt, soweit dies technisch möglich und zumutbar ist
- Die Übertragung personenbezogener Daten erfolgt, soweit technisch vorgesehen oder zumutbar, über verschlüsselte Verbindungen, insbesondere mittels HTTPS, TLS, VPN oder vergleichbarer Schutzmechanismen
- Lokale Kopien personenbezogener Daten werden nur angelegt, soweit dies für Entwicklung, Support, Fehleranalyse oder Datensicherung vorübergehend erforderlich ist; sie werden nach Wegfall des Zwecks gelöscht oder dem Auftraggeber zurückgegeben
- Papierunterlagen und mobile Datenträger mit personenbezogenen Daten werden nur verwendet, soweit dies erforderlich ist, und vor unbefugtem Zugriff geschützt aufbewahrt; nicht mehr benötigte Unterlagen oder Datenträger werden datenschutzgerecht vernichtet oder gelöscht
- Soweit der Auftragnehmer eigene Datenbestände oder projektbezogene Arbeitsstände mit personenbezogenem Bezug speichert, werden angemessene Maßnahmen zur Sicherung der Verfügbarkeit und Wiederherstellbarkeit getroffen, etwa durch regelmäßige Sicherungen, geschützte Speicherorte oder vergleichbare Vorsorgemaßnahmen
- Daten verschiedener Auftraggeber werden organisatorisch und, soweit technisch möglich, auch logisch getrennt verarbeitet, insbesondere durch getrennte Mandanten, Konten, Projekte, Verzeichnisse oder vergleichbare Strukturen
- Der Auftragnehmer überprüft die eingesetzten technischen und organisatorischen Maßnahmen in angemessenen Abständen sowie anlassbezogen, insbesondere bei wesentlichen Änderungen der eingesetzten Systeme, Arbeitsabläufe oder Risiken

Die technischen und organisatorischen Maßnahmen werden dem Umfang und Risiko der jeweiligen Verarbeitung angemessen dokumentiert und auf berechtigte Anfrage des Auftraggebers in geeigneter Form nachgewiesen.

§ 5 Vertraulichkeit

Der Auftragnehmer behandelt alle im Rahmen dieses Vertrags zur Kenntnis gelangten personenbezogenen Daten sowie sonstige vertrauliche Informationen streng vertraulich. Als Einzelunternehmer wahrt er die Vertraulichkeit selbst; soweit er ausnahmsweise weitere Personen im Zusammenhang mit der Leistungserbringung einsetzt, stellt er sicher, dass diese vor ihrem Einsatz zur Vertraulichkeit verpflichtet sind (Art. 28 Abs. 3 lit. b DSGVO). Die Vertraulichkeitspflicht besteht auch nach Beendigung des Vertrags fort.

§ 6 Unterauftragsverarbeitung

Der Einsatz von Unterauftragnehmern durch den Auftragnehmer bedarf der vorherigen Genehmigung des Auftraggebers gemäß Art. 28 Abs. 2 DSGVO. Die bei Vertragsschluss bereits genehmigten Unterauftragnehmer und Unterauftragsverhältnisse sind nachfolgend aufgeführt:

- Microsoft Corporation bzw. mit Microsoft verbundene Unternehmen, soweit deren Dienste im Rahmen von Microsoft 365, Entra ID, SharePoint, Teams, Exchange Online, Power Platform, Azure oder hiermit technisch verbundenen Microsoft-Diensten für die Leistungserbringung genutzt werden
- Weitere Unterauftragnehmer oder externe Dienste nur, soweit deren Einsatz zur Vertragserfüllung erforderlich ist und der Auftraggeber diese vorab schriftlich oder in Textform genehmigt hat

Der Auftragnehmer verpflichtet Unterauftragnehmer vertraglich zu Datenschutzpflichten, die den in diesem Vertrag festgelegten Pflichten im Wesentlichen entsprechen. Beabsichtigte Änderungen in Bezug auf den Einsatz oder den Austausch von Unterauftragnehmern teilt der Auftragnehmer dem Auftraggeber rechtzeitig in Textform mit. Der Auftraggeber kann einer solchen Änderung aus wichtigem datenschutzrechtlichem Grund innerhalb einer angemessenen Frist widersprechen.

§ 7 Rechte der betroffenen Personen

Ersuchen betroffener Personen (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch) leitet der Auftragnehmer unverzüglich an den Auftraggeber weiter und unterstützt diesen auf Anfrage bei der Erfüllung seiner Pflichten. Eine eigenständige Beantwortung solcher Ersuchen durch den Auftragnehmer erfolgt grundsätzlich nicht, es sei denn, der Auftraggeber weist ihn hierzu an oder eine gesetzliche Verpflichtung besteht.

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen in angemessenem Umfang bei der Erfüllung der Pflichten des Auftraggebers nach Art. 32 bis 36 DSGVO, insbesondere bei der Umsetzung geeigneter Sicherheitsmaßnahmen, der Bewertung und Meldung von Datenschutzverletzungen, der Erstellung von Datenschutz-Folgenabschätzungen sowie einer etwa erforderlichen Konsultation der zuständigen Aufsichtsbehörde.

§ 8 Löschung und Rückgabe von Daten

Nach Abschluss der vereinbarten Leistungen, nach Beendigung der zugrunde liegenden Beauftragung oder Vereinbarung oder jederzeit auf dokumentierte Weisung des Auftraggebers gibt der Auftragnehmer personenbezogene Daten und vom Auftraggeber überlassene Unterlagen nach Wahl des Auftraggebers zurück oder löscht sie, sofern keine gesetzliche Aufbewahrungspflicht oder sonstige gesetzliche Berechtigung zur weiteren Speicherung besteht. Nicht sofort löschbare Sicherungskopien oder technisch bedingte Restbestände dürfen nur so lange aufbewahrt werden, wie dies aus technischen oder gesetzlichen Gründen erforderlich ist; sie sind währenddessen angemessen zu schützen und nach Wegfall des Grundes zu löschen. Dies umfasst insbesondere:

- Rückgabe, Löschung oder Sperrung von Zugangsdaten, Konten, technischen Kennungen und sonstigen Zugriffsmöglichkeiten, soweit diese dem Auftragnehmer für Zwecke der Leistungserbringung zur Verfügung gestellt wurden und keine weitere Berechtigung zur Nutzung besteht
- Löschung oder Rückgabe lokal gespeicherter Datenkopien, Exportdateien, Arbeitsstände, Testdaten, Protokolle und sonstiger beim Auftragnehmer vorhandener Datenbestände mit personenbezogenem Bezug, soweit ihre weitere Aufbewahrung nicht gesetzlich erforderlich ist
- Bestätigung der Rückgabe oder Löschung in Textform auf berechtigte Anfrage des Auftraggebers

§ 9 Meldepflichten bei Datenpannen

Der Auftragnehmer informiert den Auftraggeber unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO bekannt geworden ist. Die Information erfolgt ohne unangemessene Verzögerung und enthält, soweit zu diesem Zeitpunkt möglich, mindestens die nachfolgenden Angaben. Der Auftragnehmer unterstützt den Auftraggeber bei der Aufklärung des Vorfalls sowie bei der Erfüllung etwaiger Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO.

- Beschreibung des Vorfalls und betroffener Datenkategorien
- Wahrscheinliche Konsequenzen
- Ergriffene oder vorgeschlagene Abhilfemaßnahmen

§ 10 Kontrollrechte des Auftraggebers

Der Auftraggeber ist berechtigt, die Einhaltung dieses Vertrags sowie der gesetzlichen Datenschutzanforderungen in angemessenem Umfang zu kontrollieren. Der Nachweis kann insbesondere durch Auskünfte, Selbstauskünfte, Dokumentationen, Beschreibungen der technischen und organisatorischen Maßnahmen oder sonstige geeignete Unterlagen erbracht werden. Darüber hinaus sind Prüfungen durch den Auftraggeber oder einen zur Vertraulichkeit verpflichteten Prüfer zulässig, soweit hierfür ein berechtigter Anlass besteht, die Prüfung rechtzeitig angekündigt wird und sie den Geschäftsbetrieb des Auftragnehmers nicht unverhältnismäßig beeinträchtigt. Bei der Durchführung von Kontrollen sind Betriebs- und Geschäftsgeheimnisse des Auftragnehmers sowie die Vertraulichkeit gegenüber anderen Auftraggebern zu wahren. Die Kosten von anlasslosen Prüfungen trägt der Auftraggeber; gesetzlich zwingende weitergehende Kontrollrechte bleiben unberührt. Der Auftragnehmer stellt dem Auftraggeber die für den Nachweis der Einhaltung dieses Vertrags erforderlichen Informationen zur Verfügung (Art. 28 Abs. 3 lit. h DSGVO).

§ 11 Verantwortung für Kundenumgebungen

Der Auftragnehmer entwickelt und liefert Softwareanwendungen, die auf Systemen, Servern und Plattformen des Auftraggebers installiert und ausgeführt werden. Die Verantwortung für diese Umgebungen liegt ausschließlich beim Auftraggeber. Dies umfasst insbesondere:

- Bereitstellung und Betrieb der erforderlichen Server- und Plattforminfrastruktur
- Sicherstellung der Systemsicherheit, Verfügbarkeit und Aktualisierung der Betriebsumgebung
- Datensicherung und Backup der auf den Kundensystemen gespeicherten Daten
- Einhaltung geltender Sicherheits- und Compliance-Anforderungen der eigenen IT-Infrastruktur

Der Auftragnehmer haftet nicht für Schäden, Datenverluste oder Betriebsausfälle, die auf Unzulänglichkeiten, Fehlkonfigurationen oder Ausfälle der vom Auftraggeber betriebenen Umgebung zurückzuführen sind. Voraussetzung für eine ordnungsgemäße Leistungserbringung ist eine funktionsfähige und den vereinbarten Anforderungen entsprechende Betriebsumgebung des Auftraggebers.

§ 12 Haftung

Für die Haftung der Parteien gelten die gesetzlichen Vorschriften sowie die in der zugrunde liegenden Beauftragung oder Vereinbarung getroffenen Haftungsregelungen, soweit dem keine zwingenden gesetzlichen Vorschriften, insbesondere der DSGVO, entgegenstehen.

§ 13 Schlussbestimmungen

Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform. Sollten einzelne Bestimmungen unwirksam sein oder werden, berührt dies die Wirksamkeit des übrigen Vertrags nicht. Es gilt das Recht der Bundesrepublik Deutschland; Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftragnehmers.

Unterschriften

Dieser Vertrag wird in zwei Ausfertigungen unterzeichnet. Jede Partei erhält ein Exemplar.

Ort, Datum: _____	Ort, Datum: _____
_____	_____
Auftraggeber – Name, Funktion	Dirk Hildebrand – selbständiger Einzelunternehmer