Vertrag zur Auftragsverarbeitung

gemäß Art. 28 DSGVO

zwischen

_____

(Name / Firma des Auftraggebers)

_____

(Straße, Hausnummer)

_____

(PLZ, Ort)

vertreten durch: _____

– nachfolgend „Auftraggeber“ bzw. „Verantwortlicher“ genannt –

und

1x1 IT-Solutions

Inhaber: Stefan Bauerfeindt

Lieperstr. 8

14715 Märkisch Luch

E-Mail: info@1x1it.de

– nachfolgend „Auftragnehmer“ bzw. „Auftragsverarbeiter“ genannt –

– gemeinsam auch die „Parteien“ –

Präambel

Der Auftragnehmer erbringt für den Auftraggeber Dienstleistungen, im Rahmen derer personenbezogene Daten im Auftrag des Auftraggebers verarbeitet werden. Die Parteien schließen diese Vereinbarung zur Konkretisierung ihrer datenschutzrechtlichen Pflichten gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO).

Diese Vereinbarung gilt für alle Tätigkeiten, die mit dem zugrunde liegenden Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeitende des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen.

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Gegenstand

Gegenstand der Auftragsverarbeitung ist die Bereitstellung und der Betrieb der vom Auftragnehmer angebotenen Software-Dienste, insbesondere:

- 1x1-WorkOrderAgent (Auftragsverwaltung mit Rechnungswesen, Kundenportal, Terminplanung, Zeiterfassung)
- CalDAV / CardDAV Hosting (Kalender- und Kontaktverwaltung)
- Hierzu erforderliche Hosting-, Wartungs- und Supportleistungen

(2) Dauer

Die Vereinbarung beginnt mit dem Vertragsschluss des Hauptvertrages und endet automatisch mit dessen Beendigung. Sie gilt ungeachtet ihrer Laufzeit fort, solange der Auftragnehmer noch personenbezogene Daten des Auftraggebers verarbeitet.

§ 2 Art, Umfang und Zweck der Verarbeitung

(1) Art der Verarbeitung

Erhebung, Speicherung, Veränderung, Auslesen, Abfrage, Verwendung, Übermittlung an den Auftraggeber, Einschränkung, Löschung und Vernichtung von personenbezogenen Daten im Rahmen der vertraglich vereinbarten Leistungen.

(2) Zweck der Verarbeitung

Erbringung der vertraglich geschuldeten Leistungen gemäß Hauptvertrag, insbesondere die Bereitstellung der Software-Dienste sowie deren technische Wartung.

(3) Art der personenbezogenen Daten

Im Rahmen der Auftragsverarbeitung können folgende Datenkategorien verarbeitet werden:

- Stammdaten (Name, Anschrift, Geburtsdatum)
- Kommunikationsdaten (E-Mail, Telefonnummer, Faxnummer)
- Vertragsdaten (Kunden- und Auftragsnummern, Vertragsbeziehungen)
- Abrechnungs- und Zahlungsdaten (Rechnungsbeträge, Zahlungsziele)
- Termin- und Kalenderdaten
- Login- und Authentifizierungsdaten
- Protokolldaten der Anwendung (Logs)
- Optional: vom Auftraggeber im System hinterlegte sensible Daten (z. B. im Passwort-Tresor)

(4) Kategorien betroffener Personen

- Kunden des Auftraggebers
- Lieferanten und Geschäftspartner des Auftraggebers
- Mitarbeitende des Auftraggebers
- Sonstige Geschäftskontakte des Auftraggebers

§ 3 Pflichten des Auftraggebers

(1) Der Auftraggeber ist im datenschutzrechtlichen Sinne der Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO. Er ist allein verantwortlich für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der betroffenen Personen.

(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen schriftlich oder in elektronischer Form (z. B. per E-Mail). Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen.

(3) Der Auftraggeber benennt dem Auftragnehmer einen verantwortlichen Ansprechpartner für Fragen des Datenschutzes, die im Rahmen dieser Vereinbarung anfallen.

(4) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er bei den Auftragsergebnissen Fehler oder Unregelmäßigkeiten in Bezug auf datenschutzrechtliche Bestimmungen feststellt.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach den Weisungen des Auftraggebers, es sei denn, er ist gesetzlich zu einer anderen Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust gemäß Art. 32 DSGVO. Diese Maßnahmen sind in Anlage 1 dokumentiert.

(3) Der Auftragnehmer setzt zur Verarbeitung personenbezogener Daten nur Personen ein, die zuvor schriftlich auf das Datengeheimnis (vormals § 5 BDSG) bzw. zur Vertraulichkeit gemäß Art. 28 Abs. 3 lit. b DSGVO verpflichtet wurden.

(4) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorschriften verstößt.

(5) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

(6) Der Auftragnehmer hat einen Datenschutzbeauftragten benannt, sofern hierzu eine gesetzliche Verpflichtung besteht. Bei kleineren Unternehmen ohne Bestellpflicht erfolgt die Wahrnehmung der Datenschutzaufgaben durch die Geschäftsleitung.

(7) Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens jedoch innerhalb von 48 Stunden nach Bekanntwerden, schriftlich oder in elektronischer Form. Die Meldung enthält mindestens die in Art. 33 Abs. 3 DSGVO geforderten Angaben, soweit dem Auftragnehmer bekannt.

(8) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen gemäß § 7 dieses Vertrages.

§ 5 Unterauftragsverhältnisse

(1) Der Auftraggeber stimmt der Beauftragung der in Anlage 2 aufgeführten Unterauftragsverarbeiter zu allgemein zu.

(2) Der Auftragnehmer wird den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung weiterer Auftragsverarbeiter mindestens 30 Tage vor der Änderung in Kenntnis setzen, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(3) Bei Einspruch des Auftraggebers innerhalb von 14 Tagen nach Mitteilung steht dem Auftragnehmer das Recht zu, das Vertragsverhältnis aus wichtigem Grund mit angemessener Frist zu kündigen.

(4) Der Auftragnehmer schließt mit jedem Unterauftragsverarbeiter einen Vertrag, der die in dieser Vereinbarung getroffenen datenschutzrechtlichen Pflichten in vergleichbarer Weise auferlegt.

(5) Nicht als Unterauftragsverhältnisse im Sinne dieser Vorschrift gelten Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern in Anspruch nimmt.

§ 6 Rechte betroffener Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber soweit möglich bei der Bearbeitung von Anfragen und Ansprüchen Betroffener gemäß Kapitel III der DSGVO.

(2) Sofern eine betroffene Person sich unmittelbar an den Auftragnehmer wendet, leitet dieser die Anfrage unverzüglich an den Auftraggeber weiter.

(3) Der Auftraggeber trägt die ausschließliche Verantwortung für die Wahrung der Rechte der betroffenen Personen.

§ 7 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber überzeugt sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen. Hierfür kann er z. B. Auskünfte einholen, vorhandene Testate und Zertifikate prüfen oder nach rechtzeitiger Abstimmung Vor-Ort-Kontrollen während der üblichen Geschäftszeiten durchführen lassen.

(2) Vor-Ort-Kontrollen werden mit angemessenem Vorlauf (in der Regel mindestens 14 Tage) angekündigt. Die Häufigkeit ist auf einmal pro Kalenderjahr beschränkt, sofern kein konkreter Anlass für eine zusätzliche Prüfung vorliegt.

(3) Der Auftragnehmer kann die Mitwirkung an Vor-Ort-Kontrollen, die einen Zeitaufwand von mehr als einem Personentag jährlich erfordern, gegen marktübliche Vergütung anbieten.

§ 8 Löschung und Rückgabe der 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 – spätestens mit Beendigung des Hauptvertrages – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Daten und erstellten Verarbeitungs- und Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten.

(3) Die Aushändigung der Daten erfolgt in einem gängigen, maschinenlesbaren Format (z. B. CSV, XML, ICS, VCF).

(4) Die Vernichtung erfolgt spätestens 30 Tage nach Vertragsende, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht. Die Vernichtung wird auf Anfrage in Textform bestätigt.

(5) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

§ 9 Schlussbestimmungen

(1) Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden oder eine Lücke enthalten, bleiben die übrigen Bestimmungen davon unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Bestimmung eine solche Regelung zu vereinbaren, die dem Zweck der unwirksamen Bestimmung am nächsten kommt.

(2) Bei etwaigen Widersprüchen gehen Regelungen dieses Vertrages denen des Hauptvertrages vor. Sollten einzelne Regelungen dieses Vertrages unwirksam sein oder werden, so wird dadurch die Wirksamkeit des Vertrages im Übrigen nicht berührt.

(3) Änderungen und Ergänzungen dieses Vertrages und aller seiner Bestandteile bedürfen der Schriftform und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(4) Es gilt deutsches Recht. Erfüllungsort und ausschließlicher Gerichtsstand für alle Streitigkeiten aus diesem Vertrag ist – soweit gesetzlich zulässig – der Sitz des Auftragnehmers.

Unterschriften

Ort, Datum	*Ort, Datum*
Unterschrift / Stempel Auftraggeber	*Unterschrift / Stempel Auftragnehmer (1x1 IT-Solutions)*

Anlage 1

Technische und organisatorische Maßnahmen (TOM)

gemäß Art. 32 DSGVO

Der Auftragnehmer hat folgende technische und organisatorische Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und -dienste getroffen:

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

1.1 Zutrittskontrolle

Maßnahmen zur Verhinderung des unbefugten Zutritts zu Datenverarbeitungsanlagen:

- Server werden in zertifizierten deutschen Rechenzentren der Anbieter IONOS und dogado betrieben
- Die Rechenzentren verfügen über mehrstufige Zutrittskontrollen (Vereinzelungsanlagen, Videoüberwachung, Sicherheitspersonal)
- Der Auftragnehmer selbst hat keinen physischen Zugriff auf die Server-Hardware

1.2 Zugangskontrolle

Maßnahmen zur Verhinderung der unbefugten Nutzung von Datenverarbeitungssystemen:

- Authentifizierung durch persönliche Benutzerkonten mit Passwort
- Zugriff auf administrative Ebenen über SSH mit Schlüssel-Authentifizierung
- Speicherung von Passwörtern als gesalzener bcrypt-Hash
- Regelmäßige Sicherheitsupdates der eingesetzten Systeme
- Firewall-Konfiguration (UFW) zur Beschränkung offener Ports

1.3 Zugriffskontrolle

Maßnahmen zur Sicherstellung, dass Berechtigte ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können:

- Logische Mandantentrennung auf Anwendungs- und Datenbankebene
- Maximal 5 Mandanten pro Server-Instanz, um Trennung zu gewährleisten
- Rollen- und Rechtekonzept innerhalb der Anwendung
- Protokollierung administrativer Zugriffe

1.4 Trennungskontrolle

Maßnahmen zur getrennten Verarbeitung von Daten verschiedener Auftraggeber:

- Logische Trennung auf Datenbankebene (Mandanten-ID in Datensätzen)
- Bei CalDAV/CardDAV: separate Sammlungen pro Mandant
- Getrennte Backup-Datensätze pro Mandant

1.5 Pseudonymisierung und Verschlüsselung

- Übertragungsverschlüsselung durch TLS/HTTPS (Let's Encrypt Zertifikate)
- Sensible Daten (z. B. im Passwort-Tresor) werden symmetrisch verschlüsselt gespeichert

- Backups können auf Wunsch des Auftraggebers passwortgeschützt verschlüsselt erstellt werden

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

2.1 Weitergabekontrolle

- Verschlüsselte Datenübertragung (TLS 1.2 oder höher)
- Keine Datenübermittlung in Drittländer außerhalb der EU/EWR
- Protokollierung von Datenexporten innerhalb der Anwendung

2.2 Eingabekontrolle

- Protokollierung von Erstellung, Änderung und Löschung relevanter Datensätze
- Persönliche Benutzerkonten ermöglichen Nachvollziehbarkeit
- Unveränderbarkeit gebuchter Belege gemäß GoBD-Anforderungen (für WoA)

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

3.1 Verfügbarkeitskontrolle

- Tägliche automatische Backups mit 14 Tagen Aufbewahrung
- Backups werden am gleichen Standort wie die Produktivdaten gespeichert
- Monitoring der Server-Erreichbarkeit
- Redundante Internetanbindung in den Rechenzentren der Hosting-Anbieter
- Wiederherstellungstests in regelmäßigen Abständen

3.2 Rasche Wiederherstellbarkeit

- Dokumentierte Wiederherstellungsverfahren
- Wiederherstellung aus Backup typischerweise innerhalb von 24 Stunden möglich

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

4.1 Datenschutz-Management

- Regelmäßige Überprüfung der eingesetzten Sicherheitsmaßnahmen
- Verpflichtung aller Mitarbeitenden auf das Datengeheimnis (sofern vorhanden)
- Sensibilisierung im Umgang mit personenbezogenen Daten

4.2 Auftragskontrolle

- Schriftliche Verträge zur Auftragsverarbeitung mit allen Subunternehmern
- Regelmäßige Prüfung der Subunternehmer auf Datenschutzkonformität

4.3 Vorfallsmanagement

- Definierter Prozess zur Meldung von Datenschutzvorfällen an den Auftraggeber innerhalb von 48 Stunden
- Dokumentation von Vorfällen zur Aufarbeitung

Die hier beschriebenen Maßnahmen werden regelmäßig überprüft und dem Stand der Technik angepasst. Wesentliche Änderungen werden dem Auftraggeber mitgeteilt.

Anlage 2

Liste der Unterauftragsverarbeiter

Der Auftraggeber stimmt der Beauftragung der nachfolgend aufgeführten Unterauftragsverarbeiter zu:

Unterauftrags-verarbeiter	Anschrift	Leistung	Standort der Verarbeitung
IONOS SE	Elgendorfer Straße 57, 56410 Montabaur	Server-Hosting (VPS / Dedicated Server)	Deutschland
dogado GmbH	Antonio-Segni-Straße 11, 44263 Dortmund	Webhosting / Server-Hosting	Deutschland

Bei Änderungen oder Ergänzungen dieser Liste informiert der Auftragnehmer den Auftraggeber gemäß § 5 dieses Vertrages.

Hinweis zu Nebenleistungen

Folgende Dienstleister werden als Nebenleistungen im Sinne von § 5 Abs. 5 dieses Vertrages eingesetzt und gelten nicht als Unterauftragsverarbeiter im engeren Sinne:

- Telekommunikationsanbieter für die Internetanbindung
- Postdienstleister (sofern relevant)
- Anbieter für Zertifikate (Let's Encrypt)