



DATENSCHUTZ

Auftragsverarbeitungsvertrag

Standardvertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

VERSION	STAND	ANBIETER
2.0	19.10.2026	GOLLE Digital Solutions GmbH · HRB 139552 · AG Frankfurt am Main

Standardvertrag zur Auftragsverarbeitung nach Art. 28 DSGVO. Er gilt nach § 13 der AGB GOLLE IT, sobald GOLLE IT bei einem Auftrag personenbezogene Daten im Auftrag des Kunden verarbeitet. Stand 19.10.2026.

Vertrag zur Auftragsverarbeitung nach Art. 28 DSGVO

zwischen **dem im Hauptvertrag genannten Kunden** – Verantwortlicher – und der GOLLE Digital Solutions GmbH, Berger Straße 125, 60385 Frankfurt am Main, Amtsgericht Frankfurt am Main, HRB 139552 – Auftragsverarbeiter („GOLLE IT“).

§ 1 Gegenstand und Dauer

- (1) GOLLE IT verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen zur Erbringung der im Hauptvertrag vereinbarten Leistungen (etwa Hosting, Betrieb, Wartung, Support, Entwicklung mit Echtzeiten). Gegenstand, Art und Zweck der Verarbeitung, Datenarten und Kategorien betroffener Personen ergeben sich aus Anlage 1 oder dem Angebot. Soweit dort Angaben fehlen, gilt: Gegenstand ist die Erbringung der Leistungen des Hauptvertrags; die Verarbeitung umfasst Speichern, Sichern, Bereitstellen, Fehleranalyse, Wiederherstellung und Löschen; Datenarten sind die vom Verantwortlichen in die Anwendung eingebrachten Daten, insbesondere Stamm-, Kontakt-, Vertrags-, Nutzungs- und Protokolldaten; betroffen sind die Nutzer der Anwendung sowie Kunden, Interessenten und Beschäftigte des Verantwortlichen. Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) werden nur verarbeitet, wenn dies in Anlage 1 vereinbart ist.
- (2) Der Vertrag gilt für die Dauer des Hauptvertrags und darüber hinaus, solange GOLLE IT Daten des Verantwortlichen verarbeitet.

§ 2 Weisungen

- (1) GOLLE IT verarbeitet Daten nur auf dokumentierte Weisung des Verantwortlichen, auch in Bezug auf die Übermittlung in ein Drittland oder an eine internationale Organisation, es sei denn, das Recht

der EU oder Deutschlands verpflichtet GOLLE IT zu einer Verarbeitung; dann teilt GOLLE IT dies vorher mit, soweit zulässig. Der Hauptvertrag und dieser Vertrag sind die ersten Weisungen.

- (2) Weitere Weisungen erteilt der Verantwortliche in Textform. Mündliche Weisungen bestätigt er unverzüglich in Textform. Weisungsberechtigte und Empfänger nennt Anlage 1.
- (3) Hält GOLLE IT eine Weisung für rechtswidrig, informiert sie den Verantwortlichen unverzüglich und darf die Ausführung bis zur Bestätigung oder Änderung aussetzen.
- (4) Weisungen, die über die Leistungen des Hauptvertrags hinausgehen, vergütet der Verantwortliche nach Aufwand.

§ 3 Vertraulichkeit

GOLLE IT setzt nur Personen ein, die auf Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen und mit den einschlägigen Datenschutzvorschriften vertraut gemacht wurden.

§ 4 Sicherheit der Verarbeitung

- (1) GOLLE IT trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, die in Anlage 2 beschrieben sind.
- (2) GOLLE IT darf die Maßnahmen an den technischen Fortschritt anpassen, wenn das Schutzniveau nicht sinkt. Wesentliche Änderungen dokumentiert GOLLE IT.

§ 5 Unterauftragsverarbeiter

- (1) Der Verantwortliche genehmigt die in Anlage 3 genannten Unterauftragsverarbeiter.
- (2) GOLLE IT darf weitere Unterauftragsverarbeiter einsetzen oder bestehende ersetzen. GOLLE IT informiert den Verantwortlichen mindestens 30 Tage vorher in Textform. Der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund innerhalb dieser Frist widersprechen. Einigen sich die Parteien nicht, kann jede Seite die betroffene Leistung zum Zeitpunkt des Wechsels kündigen.
- (3) GOLLE IT erlegt Unterauftragsverarbeitern vertraglich dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind (Art. 28 Abs. 4 DSGVO), und haftet gegenüber dem Verantwortlichen für deren Pflichterfüllung.
- (4) Nicht als Unterauftragsverarbeitung gelten Nebenleistungen ohne Zugriff auf personenbezogene Daten (etwa Telekommunikation, Reinigung, Postdienste).

§ 6 Übermittlung in Drittländer

Eine Verarbeitung außerhalb der EU und des EWR erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, etwa durch einen Angemessenheitsbeschluss oder Standardvertragsklauseln. Anlage 3 nennt die jeweilige Grundlage.

§ 7 Unterstützung des Verantwortlichen

- (1) GOLLE IT unterstützt den Verantwortlichen mit geeigneten Maßnahmen bei der Beantwortung von Anträgen betroffener Personen. Anträge, die direkt bei GOLLE IT eingehen, leitet GOLLE IT unverzüglich weiter.
- (2) GOLLE IT unterstützt den Verantwortlichen bei den Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit, Meldungen, Datenschutz-Folgenabschätzung, vorherige Konsultation) unter Berücksichtigung der

Art der Verarbeitung und der verfügbaren Informationen.

- (3) Unterstützung, die über die gesetzlichen Pflichten hinausgeht oder vom Verantwortlichen veranlasst ist, wird nach Aufwand vergütet.

§ 8 Meldung von Datenschutzverletzungen

- (1) GOLLE IT meldet dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten unverzüglich, möglichst innerhalb von 24 Stunden nach Kenntnis.
- (2) Die Meldung enthält, soweit bekannt: Art der Verletzung, Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, wahrscheinliche Folgen, ergriffene und vorgeschlagene Maßnahmen sowie eine Kontaktstelle. Fehlende Angaben reicht GOLLE IT nach.

§ 9 Löschung und Rückgabe

- (1) Nach Ende der Leistungen gibt GOLLE IT die Daten nach Wahl des Verantwortlichen zurück oder löscht sie, sofern keine gesetzliche Pflicht zur Speicherung besteht. Für Herausgabe und Löschrufen gilt ergänzend Teil C Ziff. 8 der AGB.
- (2) Kopien in Datensicherungen werden mit Ablauf des Aufbewahrungsschemas nach Anlage 2 gelöscht, spätestens sechs Monate nach Löschung der Produktivdaten, soweit in Anlage 1 oder im Angebot nichts anderes vereinbart ist. Bis dahin bleiben sie verschlüsselt gespeichert und werden nicht weiter verarbeitet; eine Wiederherstellung erfolgt nur auf Weisung des Verantwortlichen. Auf Anforderung bestätigt GOLLE IT die Löschung in Textform.

§ 10 Nachweise und Kontrollen

- (1) GOLLE IT stellt dem Verantwortlichen alle Informationen zum Nachweis der Pflichten aus Art. 28 DSGVO zur Verfügung, vorrangig durch Dokumentationen, Selbstauskünfte und Zertifikate.
- (2) Der Verantwortliche oder ein von ihm beauftragter, zur Vertraulichkeit verpflichteter Prüfer, der kein Wettbewerber von GOLLE IT ist, darf Kontrollen durchführen. Vor-Ort-Kontrollen finden nach mindestens 30 Tagen Vorankündigung zu Geschäftszeiten und ohne konkreten Anlass höchstens einmal je Kalenderjahr statt.
- (3) Den Aufwand von GOLLE IT für Kontrollen trägt der Verantwortliche nach Aufwand, es sei denn, die Kontrolle deckt einen erheblichen Verstoß von GOLLE IT gegen diesen Vertrag auf.

§ 11 Pflichten des Verantwortlichen

Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung und der Übermittlung der Daten an GOLLE IT verantwortlich. Er informiert GOLLE IT unverzüglich, wenn er Fehler bei der Verarbeitung feststellt.

§ 12 Haftung

Die Haftung gegenüber betroffenen Personen richtet sich nach Art. 82 DSGVO. Im Verhältnis der Parteien gelten die Haftungsregeln des Hauptvertrags.

§ 13 Schlussbestimmungen

- (1) Bei Widersprüchen geht dieser Vertrag in Datenschutzfragen dem Hauptvertrag einschließlich des Angebots vor.

- (2) Dieser Vertrag kommt durch Einbeziehung in den Hauptvertrag nach § 13 der AGB von GOLLE IT oder durch Unterzeichnung zustande; beides wahrt die Form des Art. 28 Abs. 9 DSGVO. Änderungen bedürfen der Textform.
- (3) Es gilt deutsches Recht. Gerichtsstand ist der des Hauptvertrags.

VERANTWORTLICHER

GOLLE DIGITAL SOLUTIONS GMBH

Ort, Datum

Frankfurt am Main, den

Ort, Datum

Name, Funktion, Unterschrift

Fabian Golle, Geschäftsführer

Name, Funktion, Unterschrift

Anlage 1 – Angaben zum Auftrag

Wird je Auftrag ausgefüllt und dem Angebot beigelegt. Soweit Angaben fehlen, ergeben sich Gegenstand, Art und Zweck der Verarbeitung, Datenarten und betroffene Personen aus dem Hauptvertrag; projektspezifische Unterauftragsverarbeiter gibt es dann nicht.

Feld	Angabe
Hauptvertrag	
Gegenstand	
Art und Zweck der Verarbeitung	
Datenarten	
Besondere Kategorien (Art. 9 DSGVO)	nein / ja, folgende:
Betroffene Personen	
Ort der Verarbeitung	Produktivsysteme in Deutschland (Hetzner, Nürnberg/Falkenstein), Datensicherungen in Deutschland (Hetzner) und als verschlüsselte Kopie in Frankreich (Scaleway, Paris); im Übrigen Unterauftragsverarbeiter nach Anlage 3
Projektspezifische Unterauftragsverarbeiter	keine / folgende (Name, Sitz, Ort der Verarbeitung, Drittlandgrundlage):
Weisungsberechtigte beim Verantwortlichen	
Weisungsempfänger bei GOLLE IT	Fabian Golle, fabian@golle-it.de, sowie die im Angebot benannte Projektleitung
Datenschutzkontakt GOLLE IT	Fabian Golle, Geschäftsführer, fabian@golle-it.de
Datenschutzkontakt Verantwortlicher	

Anlage 2 – Technische und organisatorische Maßnahmen

Stand 19.10.2026.

Bereich	Maßnahmen
Rechenzentren und Zutritt	Produktivsysteme ausschließlich bei Hetzner Online GmbH in Nürnberg und Falkenstein; verschlüsselte Kopien der Datensicherungen zusätzlich bei Scaleway SAS in Paris (Frankreich). Beide Betreiber sind nach ISO 27001 zertifiziert, mit Zutrittskontrolle, Videoüberwachung und Sicherheitspersonal des Betreibers. GOLLE IT arbeitet ohne eigene Serverräume.
Zugang zu Systemen	Administrative Zugänge nur mit Mehr-Faktor-Authentifizierung; SSH nur mit Schlüsseln; Passwortmanager im Team; verschlüsselte Datenträger und automatische Bildschirmsperre auf Arbeitsgeräten.
Zugriffsrechte	Rollen- und Rechtekonzept nach dem Prinzip der geringsten Rechte; Zugriff auf Produktivdaten nur für zuständige Mitarbeiter; Entzug von Rechten beim Ausscheiden am letzten Arbeitstag.
Trennung	Mandanten logisch getrennt (eigene Namespaces im Kubernetes-Cluster, Ressourcenquoten); Datenbanken und Nutzerdateien in separaten Instanzen; getrennte Test-, Staging- und Produktivumgebungen.
Pseudonymisierung	Testdaten anonymisiert oder pseudonymisiert; Echtdaten in Entwicklung nur nach Vereinbarung.
Übertragung	Verschlüsselte Übertragung (TLS) für alle Anwendungen und Schnittstellen; Administration nur über verschlüsselte Verbindungen.
Eingabe- und Protokollkontrolle	Protokollierung von Anwendungs- und Systemereignissen, Fehler-Monitoring; Protokolle mit begrenzter Aufbewahrung von 30 Tagen.
Verfügbarkeit	Cluster über zwei Rechenzentren verteilt; Firewall, Layer-7-Loadbalancer mit DDoS-Schutz und Web Application Firewall; Überwachung rund um die Uhr mit automatischer Alarmierung.
Datensicherung	Tägliche Sicherung der Datenbanken, stündliche Sicherung des Object Storage. Sicherungen verschlüsselt (AES-256), Schlüssel ausschließlich bei GOLLE IT. Zusätzliche Kopie bei einem zweiten, vom Hosting unabhängigen Anbieter (Scaleway SAS, Paris) mit eigenen, auf die Sicherungen beschränkten Zugangsschlüsseln; Versionierung schützt die Sicherungen gegen Löschen oder Verschlüsseln von einem kompromittierten Server aus. Gestaffelte Aufbewahrung: 7 tägliche, 4 wöchentliche und 6 monatliche Stände. Automatische Überwachung jedes Sicherungslaufs mit Alarmierung bei Fehlschlag oder Ausbleiben; Wiederherstellungstests halbjährlich mit Protokoll.
Schwachstellen und Updates	Laufende Überwachung bekannter Schwachstellen (CVE) in eingesetzten Komponenten; Sicherheitspatches zeitnah nach Veröffentlichung, kritische innerhalb von 7 Tagen.
Vorfallmanagement	Dokumentierter Ablauf für Sicherheitsvorfälle mit Meldung an Kunden unverzüglich, möglichst innerhalb von 24 Stunden nach Kenntnis; Cyber-Krisenplan; Cyberversicherung.

Bereich	Maßnahmen
Personal	Verpflichtung auf Vertraulichkeit und Datenschutz; Schulungen jährlich; Verträge mit Freelancern inklusive Vertraulichkeit und Auftragsverarbeitung.
KI-Werkzeuge	Nutzung nur von Diensten, die Eingaben nicht zum Training verwenden und vertraglich zur Vertraulichkeit verpflichtet sind; personenbezogene Kundendaten nur in KI-Diensten, die als Unterauftragsverarbeiter genehmigt sind.
Überprüfung	Jährliche Überprüfung dieser Maßnahmen; Aufbau eines Informationssicherheits-Managementsystems in Anlehnung an ISO 27001; eine Zertifizierung wird geprüft.

Anlage 3 – Unterauftragsverarbeiter

Stand 19.10.2026. Neue oder geänderte Unterauftragsverarbeiter kündigt GOLLE IT nach § 5 an.

Unterauftragsverarbeiter	Sitz	Leistung	Ort der Verarbeitung, Grundlage
Hetzner Online GmbH	Gunzenhausen, Deutschland	Rechenzentrum, Server, Speicher	Deutschland (Nürnberg, Falkenstein)
Scaleway SAS	Paris, Frankreich	Speicherung der Datensicherungen	Frankreich (Paris), EU
Michał Krowiarz (Electrobits)	Wrocław, Polen	Entwicklung und Wartung, Zugriff auf Produktivsysteme	Polen, EU
Slack Technologies Limited	Dublin, Irland	Teamkommunikation; Kundendaten nur vereinzelt, etwa in Screenshots zur Fehleranalyse	EU und USA; EU-US Data Privacy Framework, Standardvertragsklauseln
Google Cloud EMEA Limited (Google Workspace)	Dublin, Irland	E-Mail und Dokumente; Kundendaten nur, wenn Kunden sie im Support übermitteln	EU und USA; EU-US Data Privacy Framework, Standardvertragsklauseln
KI-Anbieter	je Projekt	Nur projektbezogen, wenn in Anlage 1 genannt	Wie in Anlage 1 angegeben



GOLLE Digital Solutions GmbH · Berger Straße 125 · 60385 Frankfurt am Main · www.golle-it.de