

AUFTRAGSVERARBEITUNG NACH ART. 28 DSGVO

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

Hauptvertrag vom [Datum] · Projekt: [Projektbezeichnung] · Fassung vom [Datum]

zwischen

[Firmierung des Auftraggebers]

[Straße und Hausnummer] · [PLZ und Ort]

vertreten durch [Name, Funktion]

— nachfolgend „Auftraggeber“ (Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO) —

und

Gridout [Rechtsform]

[Straße und Hausnummer] · [PLZ und Ort]

vertreten durch die Geschäftsführer Sebastian Zilken und Carlo Schmidt

— nachfolgend „Auftragnehmer“ (Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO) —

Teil A — Vertragsbestimmungen

§1 Gegenstand, Umfang und Dauer

- (1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen auf Grundlage des Hauptvertrags vom [Datum] („Hauptvertrag“). Soweit dabei personenbezogene Daten des Auftraggebers verarbeitet werden, gilt ergänzend dieser Vertrag.
- (2) Gegenstand, Art, Zweck und Dauer der Verarbeitung, die Art der Daten sowie die Kategorien betroffener Personen ergeben sich aus Anlage 1.
- (3) Dieser Vertrag beginnt mit Aufnahme der Verarbeitung und endet mit Beendigung des Hauptvertrags. Die Pflichten zur Löschung und Rückgabe nach §10 bestehen darüber hinaus fort.
- (4) Die Verarbeitung findet ausschließlich in Mitgliedstaaten der Europäischen Union oder in Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum statt. Eine Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und der Einhaltung der Voraussetzungen der Art. 44 ff. DSGVO.

§2 Weisungsrecht des Auftraggebers

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist nach Unionsrecht oder dem Recht eines Mitgliedstaats zur Verarbeitung verpflichtet.
- (2) Weisungen erfolgen grundsätzlich in Textform. Mündlich erteilte Weisungen bestätigt der Auftraggeber unverzüglich in Textform.
- (3) Weisungsberechtigt auf Seiten des Auftraggebers sind: [Name, Funktion, Kontakt]. Weisungsempfänger auf Seiten des Auftragnehmers sind: [Sebastian Zilken / Carlo Schmidt, Kontakt].
- (4) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, weist er den Auftraggeber unverzüglich darauf hin. Er ist berechtigt, die Ausführung auszusetzen, bis der Auftraggeber sie bestätigt oder ändert.

§3 Pflichten des Auftragnehmers

- (1) Der Auftragnehmer verarbeitet die Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers.
- (2) Der Auftragnehmer stellt sicher, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
- (3) Der Auftragnehmer ergreift die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Diese sind in Anlage 2 beschrieben. Er darf sie fortentwickeln, sofern das vereinbarte Schutzniveau nicht unterschritten wird.
- (4) Der Auftragnehmer benennt eine für den Datenschutz zuständige Ansprechperson: [Name und Kontakt]. Eine Pflicht zur Bestellung eines Datenschutzbeauftragten besteht [nicht / ausweislich Art. 37 DSGVO].
- (5) Der Auftragnehmer führt ein Verzeichnis aller Kategorien von im Auftrag durchgeführten Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.
- (6) Der Auftragnehmer berichtigt, löscht oder schränkt die Verarbeitung der Daten ein, wenn der Auftraggeber dies weist.

§4 Unterauftragsverhältnisse

- (1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter hinzuzuziehen. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage 3 aufgeführt und werden hiermit genehmigt.
- (2) Beabsichtigt der Auftragnehmer, einen weiteren Unterauftragsverarbeiter hinzuzuziehen oder einen bestehenden auszutauschen, teilt er dies dem Auftraggeber mindestens [vier] Wochen vorher in Textform mit. Der Auftraggeber kann innerhalb von [zwei] Wochen aus wichtigem datenschutzrechtlichem Grund widersprechen.
- (3) Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten, die ihn selbst nach diesem Vertrag treffen.
- (4) Nicht als Unterauftragsverhältnis im Sinne dieser Regelung gelten Nebenleistungen, die der Auftragnehmer bei Dritten in Anspruch nimmt, etwa Telekommunikationsleistungen oder Wartung, sofern dabei kein regelmäßiger Zugriff auf personenbezogene Daten des Auftraggebers erfolgt.

§5 Unterstützung bei Betroffenenrechten

- (1) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen betroffener Personen nach Kapitel III der DSGVO nachzukommen.
- (2) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser das Anliegen unverzüglich an den Auftraggeber weiter und wird nicht selbst tätig.
- (3) Der Aufwand für die Unterstützung ist mit der Vergütung nach dem Hauptvertrag abgegolten, soweit er nicht auf einer nicht vom Auftragnehmer zu vertretenden Ursache beruht.

§6 Unterstützung bei Sicherheit, Meldepflichten und Folgenabschätzung

- (1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in Art. 32 bis 36 DSGVO genannten Pflichten, unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen.
- (2) Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens jedoch innerhalb von [24] Stunden nach Kenntniserlangung, damit der Auftraggeber die Frist nach Art. 33 Abs. 1 DSGVO einhalten kann.
- (3) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen und stimmt sich dabei mit dem Auftraggeber ab.

§7 Nachweise und Kontrollrechte

- (1) Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der in Art. 28 DSGVO genannten Pflichten erforderlich sind.
- (2) Der Auftraggeber ist berechtigt, sich von der Einhaltung dieses Vertrags zu überzeugen. Der Nachweis kann auch durch Selbstauskunft, aktuelle Testate oder Zertifizierungen der eingesetzten Rechenzentren geführt werden.
- (3) Prüfungen vor Ort werden mit angemessener Vorlaufzeit von mindestens [zwei] Wochen und während der üblichen Geschäftszeiten angekündigt. Sie dürfen den Betriebsablauf nicht unverhältnismäßig stören.

§8 Weisungsgebundene Verarbeitung durch Beschäftigte

- (1) Der Auftragnehmer setzt für die Verarbeitung ausschließlich Personen ein, die auf die Vertraulichkeit verpflichtet und mit den einschlägigen Datenschutzvorschriften vertraut gemacht wurden.
- (2) Der Auftragnehmer schult die betreffenden Personen in angemessenen Abständen und dokumentiert dies.

§9 Haftung

- (1) Für die Haftung gelten die Regelungen des Hauptvertrags sowie Art. 82 DSGVO.
- (2) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Rechte betroffener Personen verantwortlich.

§10 Löschung und Rückgabe nach Beendigung

- (1) Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragnehmer nach Wahl des Auftraggebers alle personenbezogenen Daten oder gibt sie zurück, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht.
- (2) Der Auftraggeber teilt seine Wahl spätestens [vier] Wochen vor Beendigung in Textform mit. Trifft er keine Wahl, erfolgt zunächst die Rückgabe und anschließend die Löschung.
- (3) Die Löschung erfolgt innerhalb von [vier] Wochen nach Beendigung, bei Sicherungskopien spätestens mit Ablauf des vereinbarten Aufbewahrungszeitraums. Die Löschung wird auf Verlangen in Textform bestätigt.
- (4) Der Aufwand für die Herausgabe der Daten in einem vom Standard abweichenden Format wird nach dem im Hauptvertrag vereinbarten Satz vergütet.

§11 Schlussbestimmungen

- (1) Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform. Dies gilt auch für die Aufhebung dieses Schriftformerfordernisses.
- (2) Sollten einzelne Bestimmungen unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.
- (3) Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Regelungen dieses Vertrags vor, soweit die Verarbeitung personenbezogener Daten betroffen ist.
- (4) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist, soweit zulässig vereinbar, [Ort].

Anlagen

Nr.	Dokument
1	Beschreibung der Verarbeitung
2	Technische und organisatorische Maßnahmen nach Art. 32 DSGVO
3	Genehmigte Unterauftragsverarbeiter

[Ort], den [Datum]

[Ort], den [Datum]

Auftraggeber — Name, Funktion

Gridout — Sebastian Zilken / Carlo Schmidt

Beschreibung der Verarbeitung

Projekt: [Projektbezeichnung] · Auftraggeber: [Firmierung]

Gegenstand der Verarbeitung

Erstellung, Bereitstellung, Betrieb und Pflege einer individuellen Datenbankanwendung für den Auftraggeber gemäß Hauptvertrag.

Art und Zweck der Verarbeitung

- Speicherung und Bereitstellung der vom Auftraggeber und seinen Nutzern eingegebenen Daten in der Anwendung
- Übernahme von Bestandsdaten aus vorhandenen Dateien oder Systemen des Auftraggebers in die Anwendung
- technische Pflege, Fehlerbehebung und Weiterentwicklung der Anwendung
- Erstellung und Rücksicherung von Datensicherungen
- Betrieb der Server- und Datenbankumgebung, soweit vom Auftragnehmer übernommen

Kategorien betroffener Personen

[Zutreffendes im Einzelfall festlegen — Beispiele:]

- Beschäftigte des Auftraggebers (Nutzer der Anwendung)
- Kunden, Interessenten und deren Ansprechpartner
- Lieferanten und Dienstleister des Auftraggebers
- Teilnehmende an Veranstaltungen oder Qualifizierungen

Arten personenbezogener Daten

[Zutreffendes im Einzelfall festlegen — Beispiele:]

- Stammdaten (Name, Anschrift, Kundennummer)
- Kontaktdaten (Telefon, E-Mail)
- Vertrags- und Abrechnungsdaten
- Nutzungs- und Protokolldaten der Anwendung (Anmeldung, Änderungsverlauf)
- [Besondere Kategorien nach Art. 9 DSGVO: nur eintragen, wenn tatsächlich verarbeitet — dann sind erhöhte Schutzmaßnahmen erforderlich]

Dauer der Verarbeitung

Für die Laufzeit des Hauptvertrags, anschließend gemäß §10 dieses Vertrags.

Ort der Verarbeitung

[Zutreffendes wählen:] Rechenzentrum [Anbieter] in [Ort], Deutschland bzw. Europäische Union. Zugriffe zu Wartungszwecken erfolgen ausschließlich aus dem Gebiet der Europäischen Union.

Technische und organisatorische Maßnahmen

nach Art. 32 DSGVO

Projekt: [Projektbezeichnung] · Hosting-Variante: [Cloud / Strato / beim Auftraggeber]

Die nachstehenden Maßnahmen beschreiben das Schutzniveau, das der Auftragnehmer unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs und der Zwecke der Verarbeitung gewährleistet.

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

Maßnahme	Umsetzung bei Gridout
Zutrittskontrolle	Die Verarbeitung erfolgt in Rechenzentren des jeweiligen Hosting-Anbieters. Diese verfügen über Zutrittssicherung, Videoüberwachung und dokumentierte Besucherverwaltung und sind nach ISO/IEC 27001 zertifiziert; bei den Cloud-Anbietern liegt zusätzlich ein Testat nach dem BSI-Kriterienkatalog C5 vor.
Zugangskontrolle	Zugang zu Servern ausschließlich über verschlüsselte Verbindungen (SSH mit Schlüsselpaar, kein Passwortzugang). Verwaltungszugänge sind personengebunden und werden bei Projektende deaktiviert. [Zwei-Faktor-Authentifizierung ergänzen, sofern eingerichtet]
Zugriffskontrolle	Innerhalb der Anwendung gilt ein abgestuftes Rollen- und Rechtekonzept; Nutzer sehen und bearbeiten ausschließlich die für ihre Aufgabe erforderlichen Daten. Der Datenbankzugriff erfolgt über die Anwendung oder gesondert abgesicherte administrative Zugänge.
Trennungskontrolle	Daten unterschiedlicher Auftraggeber werden in getrennten Datenbanken bzw. getrennten Instanzen verarbeitet. Test- und Entwicklungsumgebungen sind von der Produktivumgebung getrennt.
Pseudonymisierung und Verschlüsselung	Übertragung ausschließlich über TLS (HTTPS). Kennwörter werden ausschließlich als Hashwert mit Streuwert gespeichert, nicht im Klartext. Wo möglich werden pseudonyme Kennungen anstelle von Klardaten verwendet.

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

Maßnahme	Umsetzung bei Gridout
Weitergabekontrolle	Eine Weitergabe personenbezogener Daten an Dritte erfolgt nur auf Weisung des Auftraggebers oder im Rahmen der in Anlage 3 genehmigten Unterauftragsverarbeitung. Datenträger werden nicht zum Datenaustausch verwendet.
Eingabekontrolle	Die Anwendung protokolliert Anmeldungen sowie Änderungen an Datensätzen mit Zeitpunkt und auslösendem Benutzerkonto. Serverseitig werden parametrisierte Datenbankabfragen verwendet; ergänzend bestehen Schutzmaßnahmen gegen Cross-Site-Scripting und automatisierte Missbrauchsversuche.

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

Maßnahme	Umsetzung bei Gridout
Verfügbarkeitskontrolle	Tägliche automatisierte Datensicherung mit einer Aufbewahrung von [Anzahl] Tagen. Die Sicherungen werden getrennt vom Produktivsystem vorgehalten.
Rasche Wiederherstellbarkeit	Die Wiederherstellbarkeit der Sicherungen wird mindestens [halbjährlich] durch einen Rücksicherungstest überprüft und dokumentiert.
Belastbarkeit	Überwachung der Erreichbarkeit und der Systemauslastung mit automatischer Benachrichtigung bei Störungen. Schutzmaßnahmen gegen verbreitete Angriffsmuster sind Bestandteil des Anwendungsstandards.

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

Maßnahme	Umsetzung bei Gridout
Datenschutz-Management	Führung eines Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO. Verpflichtung aller mit der Verarbeitung befassten Personen auf Vertraulichkeit. Löschkonzept mit festen Fristen.
Vorfallsbearbeitung	Festgelegter Ablauf für den Umgang mit Verletzungen des Schutzes personenbezogener Daten einschließlich Meldung an den Auftraggeber innerhalb der in §6 genannten Frist.
Datenschutzfreundliche Voreinstellungen	Erhebung ausschließlich der für den jeweiligen Zweck erforderlichen Daten. Rollen werden nach dem Grundsatz der geringstmöglichen Berechtigung vergeben.
Auftragskontrolle	Schriftliche Auftragserteilung, Bindung an dokumentierte Weisungen, sorgfältige Auswahl der Unterauftragsverarbeiter unter Datenschutz Gesichtspunkten und deren vertragliche Verpflichtung.
Regelmäßige Überprüfung	[Turnus für die Überprüfung dieser Maßnahmen ergänzen — z. B. jährlich sowie anlassbezogen bei wesentlichen Änderungen der Infrastruktur]

ANLAGE 3 ZUM AUFTRAGSVERARBEITUNGSVERTRAG

Genehmigte Unterauftragsverarbeiter

Stand: [Datum] · Projekt: [Projektbezeichnung]

Die nachfolgenden Unternehmen werden zum Zeitpunkt des Vertragsschlusses als Unterauftragsverarbeiter eingesetzt. Nicht benötigte Zeilen sind vor Verwendung zu streichen.

Unternehmen	Sitz	Leistung	Ort der Verarbeitung
[Anbieter Hosting, z. B. STRATO AG]	[Sitz, z. B. Berlin, DE]	Bereitstellung und Betrieb der Server- und Speicherinfrastruktur	[Rechenzentrum in Deutschland]
[Microsoft Deutschland GmbH]	[Sitz]	Bereitstellung der Cloud-Infrastruktur (Azure)	[Region Frankfurt am Main, DE]
[Amazon Web Services EMEA SARL]	[Sitz]	Bereitstellung der Cloud-Infrastruktur (AWS)	[Region Frankfurt am Main, DE]

Hinweis zu Anbietern mit Konzernsitz außerhalb der EU: Bei Microsoft und Amazon Web Services handelt es sich um Tochtergesellschaften US-amerikanischer Konzerne. Die Verarbeitung erfolgt ausschließlich in Rechenzentren innerhalb der Europäischen Union; eine Übermittlung in Drittländer findet nicht statt. Bei besonders sensiblen Datenbeständen empfiehlt der Auftragnehmer die Variante Strato oder den Betrieb in eigener Infrastruktur des Auftraggebers.

Eine jeweils aktuelle Fassung dieser Liste wird auf Anfrage in Textform zur Verfügung gestellt.

Hinweis: Dieser Entwurf dient der Orientierung und ersetzt keine Rechtsberatung. Farblich hervorgehobene Textstellen in eckigen Klammern sind vor Verwendung auszufüllen. Wir empfehlen, diesen Vertrag gemeinsam mit AGB und Hauptvertrag von einem Fachanwalt für IT-Recht prüfen zu lassen.