

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

gemäß Art. 28 DSGVO Fassung 1.1, Stand 28. August 2026

Vertragsparteien

Verantwortlicher (nachfolgend „Verantwortlicher“)

Feld	Angabe
Firma / Name	_____
Anschrift	_____
Vertreten durch	_____
Kontakt für Datenschutzfragen	_____

und

Auftragsverarbeiter (nachfolgend „Auftragsverarbeiter“)

Feld	Angabe
Firma / Name	Brala, Yannick Seidel (Einzelunternehmen)
Anschrift	Wolfshöhe 28, 04668 Grimma, Deutschland
Vertreten durch	Yannick Seidel
Kontakt für Datenschutzfragen	support@brala.app

nachfolgend einzeln „Partei“, gemeinsam „Parteien“.

Präambel

Die Parteien haben einen Vertrag über die Nutzung der Software Brala geschlossen, die als Software as a Service über brala.app bereitgestellt wird (nachfolgend „Hauptvertrag“). Grundlage des Hauptvertrages sind die Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters in ihrer jeweils geltenden Fassung.

Bei der Erbringung der Leistungen aus dem Hauptvertrag verarbeitet der Auftragsverarbeiter personenbezogene Daten, für die der Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO verantwortlich ist. Diese Verarbeitung erfolgt im Auftrag und nach Weisung des Verantwortlichen. Zur Erfüllung der Anforderungen des Art. 28 Abs. 3 DSGVO schließen die Parteien den nachfolgenden Vertrag (nachfolgend „Vertrag“ oder „AV-Vertrag“).

§ 1 Gegenstand, Geltung und Rangfolge

1. Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung personenbezogener Daten, die der Auftragsverarbeiter zur Erfüllung des Hauptvertrages im Auftrag des Verantwortlichen vornimmt.
2. Gegenstand, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen sowie die Dauer der Verarbeitung ergeben sich aus **Anlage 1**, die Bestandteil dieses Vertrages ist.
3. Dieser Vertrag gilt für die gesamte Dauer des Hauptvertrages sowie für alle Verarbeitungen, die der Auftragsverarbeiter nach dessen Beendigung noch nach § 12 vorzunehmen hat.
4. Soweit dieser Vertrag Regelungen zur Verarbeitung personenbezogener Daten trifft, gehen diese den Regelungen des Hauptvertrages und der Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters vor. Im Übrigen bleiben Hauptvertrag und Allgemeine Geschäftsbedingungen unberührt. Abweichende Regelungen des Verantwortlichen, insbesondere dessen eigene Einkaufs- oder Vertragsbedingungen, werden nicht Vertragsbestandteil, auch wenn ihnen im Einzelfall nicht ausdrücklich widersprochen wird.
5. Der Vertrag kommt in Textform zustande. Er gilt als geschlossen, sobald beide Parteien ihn unterzeichnet oder in Textform bestätigt haben.

§ 2 Verantwortlichkeit und Abgrenzung

1. Der Verantwortliche ist im Rahmen dieses Vertrages allein verantwortlich für die Rechtmäßigkeit der Verarbeitung, insbesondere für das Vorliegen einer Rechtsgrundlage nach Art. 6 DSGVO, für die Erfüllung der Informationspflichten nach Art. 12 bis 14 DSGVO gegenüber den betroffenen Personen sowie für die Wahrung von deren Rechten. Der Auftragsverarbeiter beurteilt nicht, ob der Verantwortliche die von ihm eingegebenen Daten verarbeiten darf.
2. Nicht Gegenstand dieses Vertrages sind Verarbeitungen, die der Auftragsverarbeiter zu eigenen Zwecken und in eigener Verantwortlichkeit vornimmt. Dazu gehören insbesondere:
 - a) die Verarbeitung der Vertrags-, Rechnungs- und Zahlungsdaten des Verantwortlichen zur Begründung, Durchführung und Abrechnung des Hauptvertrages,
 - b) die Protokollierung des Serverbetriebs zum Zweck der IT-Sicherheit und Fehleranalyse,
 - c) die cookielose, anonyme Reichweitenmessung des Angebots,
 - d) die Bearbeitung von Support- und Kontaktanfragen.Die Einzelheiten dieser Verarbeitungen ergeben sich aus der Datenschutzerklärung des Auftragsverarbeiters unter brala.app/datenschutz.
3. Verarbeitet der Auftragsverarbeiter personenbezogene Daten entgegen diesem Vertrag zu eigenen Zwecken oder bestimmt er Zwecke und Mittel der Verarbeitung selbst, ist er insoweit nach Art. 28 Abs. 10 DSGVO als Verantwortlicher anzusehen.

§ 3 Weisungsrecht des Verantwortlichen

1. Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation. Etwas anderes gilt nur, wenn der Auftragsverarbeiter nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet ist; in diesem Fall teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
2. Der Hauptvertrag einschließlich dieses Vertrages und die dort beschriebene Nutzung der Software durch den Verantwortlichen stellen die initiale Weisung dar. Weitere Weisungen erteilt der Verantwortliche in Textform, in dringenden Fällen mündlich mit unverzüglicher Bestätigung in Textform. Der Auftragsverarbeiter dokumentiert die Weisungen.
3. Weisungsbefugt auf Seiten des Verantwortlichen sind die in **Anlage 4** benannten Personen. Änderungen teilt der Verantwortliche in Textform mit. Ohne eine solche Benennung gelten die im Kundenkonto hinterlegten Administratoren als weisungsbefugt.
4. Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, teilt er dies dem Verantwortlichen unverzüglich mit. Er ist berechtigt, die Ausführung der betreffenden Weisung bis zu deren Bestätigung oder Änderung durch den Verantwortlichen auszusetzen.
5. Weisungen, die über den im Hauptvertrag vereinbarten Leistungsumfang hinausgehen und beim Auftragsverarbeiter einen nicht nur unerheblichen Mehraufwand verursachen, vergütet der Verantwortliche nach dem jeweils gültigen Stundensatz des Auftragsverarbeiters. Der Auftragsverarbeiter weist auf die Vergütungspflicht vor Ausführung hin.

§ 4 Pflichten des Auftragsverarbeiters

1. Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur im Rahmen dieses Vertrages und der Weisungen des Verantwortlichen.
2. Der Auftragsverarbeiter verarbeitet die Daten innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums. Eine Verarbeitung in einem Drittland findet nur unter den Voraussetzungen des § 7 dieses Vertrages statt.
3. Der Auftragsverarbeiter gewährleistet, dass sich alle zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Er verarbeitet die Daten derzeit ausschließlich selbst und ist auf die Vertraulichkeit verpflichtet. Setzt er Beschäftigte, freie Mitarbeiter oder sonstige Hilfspersonen ein, verpflichtet er diese vor Aufnahme ihrer Tätigkeit in Textform zur Vertraulichkeit und weist sie in die einschlägigen datenschutzrechtlichen Anforderungen ein. Die Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.
4. Der Auftragsverarbeiter trifft die Maßnahmen nach § 5 dieses Vertrages.
5. Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Maßgabe der §§ 8 und 9 dieses Vertrages.

6. Der Auftragsverarbeiter hat keinen Datenschutzbeauftragten bestellt; die Voraussetzungen des Art. 37 DSGVO und des § 38 BDSG liegen nicht vor. Anlaufstelle für Datenschutzfragen ist support@brala.app. Der Auftragsverarbeiter zeigt dem Verantwortlichen die Bestellung eines Datenschutzbeauftragten unaufgefordert an.
7. Der Auftragsverarbeiter führt ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und stellt es der Aufsichtsbehörde auf Anfrage zur Verfügung.
8. Der Auftragsverarbeiter berichtigt, löscht oder schränkt die Verarbeitung der Daten nur auf Weisung des Verantwortlichen ein, soweit er nicht gesetzlich zu einem anderen Vorgehen verpflichtet ist. Die Nutzung der in der Software vorgesehenen Funktionen durch den Verantwortlichen gilt insoweit als Weisung.
9. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn eine Aufsichtsbehörde eine Maßnahme gegen ihn richtet, die die Verarbeitung nach diesem Vertrag betrifft.

§ 5 Technische und organisatorische Maßnahmen

1. Der Auftragsverarbeiter trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Der Stand dieser Maßnahmen bei Vertragsschluss ergibt sich aus **Anlage 2**, die Bestandteil dieses Vertrages ist. Der Verantwortliche hat sich vor Vertragsschluss von der Angemessenheit dieser Maßnahmen überzeugt.
2. Die Maßnahmen unterliegen dem technischen Fortschritt. Der Auftragsverarbeiter ist berechtigt, sie anzupassen, solange das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen dokumentiert er und teilt sie dem Verantwortlichen auf Anfrage mit.
3. Der Auftragsverarbeiter überprüft die Wirksamkeit der Maßnahmen regelmäßig, mindestens jährlich, sowie anlassbezogen.

§ 6 Unterauftragsverarbeiter

1. Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung nach Art. 28 Abs. 2 Satz 2 DSGVO, weitere Auftragsverarbeiter hinzuzuziehen. Die bei Vertragsschluss hinzugezogenen Unterauftragsverarbeiter sind in **Anlage 3** aufgeführt und genehmigt.
2. Keine Unterauftragsverarbeitung im Sinne dieser Regelung sind Nebenleistungen, die der Auftragsverarbeiter bei Dritten in Anspruch nimmt, wie Telekommunikationsleistungen, Postdienste, Reinigung, Wartung von Endgeräten oder die Prüfung und Entsorgung von Datenträgern. Der Auftragsverarbeiter trifft auch insoweit angemessene Vorkehrungen zum Schutz der Daten.
3. Der Auftragsverarbeiter zeigt dem Verantwortlichen jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters mindestens 30 Tage vor deren Wirksamwerden in Textform an. Die Anzeige kann auch durch Aktualisierung einer öffentlich abrufbaren Liste erfolgen, wenn der Auftragsverarbeiter den Verantwortlichen zusätzlich in Textform auf die Änderung hinweist.
4. Der Verantwortliche kann der Änderung innerhalb von 14 Tagen nach Zugang der Anzeige aus wichtigem, datenschutzrechtlich begründetem Anlass in Textform widersprechen. Der Wider-

spruch ist zu begründen. Widerspricht der Verantwortliche nicht fristgerecht, gilt die Änderung als genehmigt; auf diese Folge weist der Auftragsverarbeiter in der Anzeige hin.

5. Widerspricht der Verantwortliche fristgerecht und begründet, sucht der Auftragsverarbeiter nach einer für beide Seiten zumutbaren Lösung. Ist eine solche nicht möglich und kann der Auftragsverarbeiter die Leistung ohne den betreffenden Unterauftragsverarbeiter nicht mit zumutbarem Aufwand erbringen, ist jede Partei berechtigt, den Hauptvertrag mit einer Frist von 30 Tagen zum Monatsende zu kündigen. Bereits im Voraus gezahlte Entgelte erstattet der Auftragsverarbeiter zeitanteilig.
6. Der Auftragsverarbeiter wählt den Unterauftragsverarbeiter sorgfältig unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen aus. Er erlegt dem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf, die ihm nach diesem Vertrag obliegen, insbesondere hinreichende Garantien nach Art. 28 Abs. 4 DSGVO.
7. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Unterauftragsverarbeiters.

§ 7 Verarbeitung in Drittländern

1. Eine Verarbeitung personenbezogener Daten in einem Drittland findet nur statt, wenn die besonderen Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind, insbesondere auf Grundlage eines Angemessenheitsbeschlusses der Europäischen Kommission oder von Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO.
2. Der bei Vertragsschluss vorgesehene Drittlandbezug und dessen Rechtsgrundlage sind in **Anlage 3** ausgewiesen. Der Verantwortliche genehmigt diese Übermittlungen und erteilt dem Auftragsverarbeiter die erforderliche Weisung nach § 3 Abs. 1.
3. Der Auftragsverarbeiter weist dem Verantwortlichen die Grundlage der Übermittlung auf Anforderung nach.

§ 8 Unterstützung bei Betroffenenrechten

1. Wendet sich eine betroffene Person mit einem Antrag auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit oder Widerspruch unmittelbar an den Auftragsverarbeiter, leitet dieser den Antrag unverzüglich an den Verantwortlichen weiter und beantwortet ihn nicht selbst. Er weist die betroffene Person darauf hin, dass der Verantwortliche zuständig ist, soweit ihm dieser bekannt ist.
2. Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung solcher Anträge nachzukommen, soweit dies dem Verantwortlichen nicht mit den Funktionen der Software selbst möglich ist (Art. 28 Abs. 3 lit. e DSGVO).
3. Für Unterstützungsleistungen, die über die Bereitstellung der Softwarefunktionen hinausgehen und nicht auf einem Umstand beruhen, den der Auftragsverarbeiter zu vertreten hat, gilt § 3 Abs. 5

entsprechend.

§ 9 Unterstützung bei Sicherheit, Meldepflichten und Folgenabschätzung

1. Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten, insbesondere bei der Sicherheit der Verarbeitung, der Meldung von Verletzungen des Schutzes personenbezogener Daten, der Benachrichtigung betroffener Personen, der Datenschutz-Folgenabschätzung und der vorherigen Konsultation. Die Unterstützung erfolgt unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen.
2. Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten, die die auftragsweise verarbeiteten Daten betrifft, unverzüglich nach Bekanntwerden, spätestens jedoch innerhalb von 48 Stunden. Dasselbe gilt bei einem begründeten Verdacht sowie bei schwerwiegenden Störungen des Betriebsablaufs.
3. Die Meldung enthält, soweit dem Auftragsverarbeiter bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO, insbesondere eine Beschreibung der Art der Verletzung, die Kategorien und die ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen sowie die ergriffenen oder vorgeschlagenen Maßnahmen. Liegen nicht alle Angaben vor, liefert der Auftragsverarbeiter sie unverzüglich nach.
4. Der Auftragsverarbeiter ergreift unverzüglich die zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen erforderlichen Maßnahmen und stimmt sich hierzu mit dem Verantwortlichen ab.
5. Meldungen nach dieser Vorschrift und die dabei ergriffenen Maßnahmen begründen kein Anerkenntnis eines Verschuldens oder einer Pflichtverletzung.

§ 10 Nachweise und Kontrollrechte

1. Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten erforderlich sind, und ermöglicht Überprüfungen einschließlich Inspektionen (Art. 28 Abs. 3 lit. h DSGVO).
2. Der Nachweis erfolgt vorrangig durch geeignete Unterlagen, insbesondere durch die Dokumentation der technischen und organisatorischen Maßnahmen, durch aktuelle Selbstauskünfte oder durch Testate, Zertifizierungen oder Prüfberichte unabhängiger Stellen, auch solcher der Unterauftragsverarbeiter. Der Auftragsverarbeiter beantwortet Fragebögen des Verantwortlichen zum Datenschutz innerhalb angemessener Frist.
3. Genügen diese Nachweise im Einzelfall nicht, kann der Verantwortliche nach vorheriger Anmeldung mit einer Frist von vier Wochen während der üblichen Geschäftszeiten eine Kontrolle beim Auftragsverarbeiter durchführen oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen lassen. Die Kontrolle darf den Betriebsablauf nicht unangemessen beeinträchtigen und die Betriebs- und Geschäftsgeheimnisse des Auftragsverarbeiters sowie die Rechte anderer Kunden nicht verletzen. Der Prüfer darf kein Wettbewerber des Auftragsverarbeiters sein.

4. Vor-Ort-Kontrollen finden höchstens einmal je Kalenderjahr statt. Zusätzliche Kontrollen sind zulässig, wenn ein besonderer Anlass besteht, insbesondere nach einer Verletzung des Schutzes personenbezogener Daten oder auf Anordnung einer Aufsichtsbehörde.
5. Der Aufwand des Auftragsverarbeiters für Kontrollen nach Absatz 3 und für die Beantwortung von Fragebögen, die über eine einmalige jährliche Auskunft hinausgehen, ist nach § 3 Abs. 5 zu vergüten, es sei denn, die Kontrolle beruht auf einem Umstand, den der Auftragsverarbeiter zu vertreten hat.
6. Der Verantwortliche dokumentiert das Ergebnis der Kontrolle und übermittelt dem Auftragsverarbeiter eine Kopie.

§ 11 Haftung

1. Für die Haftung der Parteien gilt Art. 82 DSGVO.
2. Im Innenverhältnis gelten ergänzend die Haftungsregelungen des Hauptvertrages. Eine Beschränkung der Haftung gegenüber betroffenen Personen oder Aufsichtsbehörden ist damit nicht verbunden.
3. Wird der Auftragsverarbeiter von einer betroffenen Person oder einer Aufsichtsbehörde in Anspruch genommen, weil der Verantwortliche gegen seine Pflichten nach § 2 Abs. 1 verstoßen oder eine rechtswidrige Weisung erteilt hat, stellt der Verantwortliche den Auftragsverarbeiter von diesen Ansprüchen einschließlich der notwendigen Kosten der Rechtsverteidigung frei, soweit den Auftragsverarbeiter kein eigenes Verschulden trifft. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über die Inanspruchnahme und stimmt die Rechtsverteidigung mit ihm ab.

§ 12 Beendigung, Löschung und Rückgabe

1. Dieser Vertrag endet mit der Beendigung des Hauptvertrages. Eine gesonderte Kündigung ist ausgeschlossen; unberührt bleibt das Recht jeder Partei zur außerordentlichen Kündigung des Hauptvertrages aus wichtigem Grund.
2. Ein wichtiger Grund für den Verantwortlichen liegt insbesondere vor, wenn der Auftragsverarbeiter schwerwiegend gegen wesentliche Pflichten aus diesem Vertrag verstößt, eine Weisung nicht ausführt oder eine Kontrolle nach § 10 verweigert.
3. Nach Beendigung des Hauptvertrages löscht der Auftragsverarbeiter die auftragsweise verarbeiteten Daten nach Wahl des Verantwortlichen oder gibt sie zurück (Art. 28 Abs. 3 lit. g DSGVO). Der Verantwortliche teilt seine Wahl bis zum Ablauf der Frist nach Absatz 4 in Textform mit. Trifft er keine Wahl, werden die Daten gelöscht.
4. Der Auftragsverarbeiter hält die Daten nach Beendigung des Hauptvertrages 30 Tage vor. In dieser Frist stellt er sie dem Verantwortlichen auf dessen Anforderung in einem gängigen elektronischen Format zur Verfügung. Ein unmittelbarer Zugriff über die Software besteht nach Beendigung nicht. Nach Ablauf der Frist werden die Daten gelöscht.
5. Verlangt der Verantwortliche die Löschung vor Ablauf der Frist nach Absatz 4 oder löscht er sein Konto, werden die Daten unverzüglich gelöscht.

6. Von der Löschung ausgenommen sind Daten, für die eine gesetzliche Aufbewahrungspflicht besteht. Diese Daten werden für die Dauer der Aufbewahrungsfrist gesperrt und ausschließlich zu dem Zweck verarbeitet, der die Aufbewahrung gebietet; sie werden nach Ablauf der Frist gelöscht.
7. Daten in Sicherungskopien werden mit dem Ablauf des jeweiligen Sicherungszyklus gelöscht. Der Zyklus beträgt derzeit 14 Tage für die tägliche Datensicherung; für Voll-Abbilder des Servers gilt der Zyklus des in Anlage 3 genannten Hostingdienstleisters. Bis zur Löschung bleiben diese Daten den Maßnahmen nach § 5 unterworfen.
8. Der Auftragsverarbeiter bestätigt die Löschung dem Verantwortlichen auf Anforderung in Textform.
9. Ein Zurückbehaltungsrecht an den auftragsweise verarbeiteten Daten und den zugehörigen Datenträgern steht dem Auftragsverarbeiter nicht zu; § 273 BGB und § 369 HGB sind insoweit ausgeschlossen.

§ 13 Schlussbestimmungen

1. Änderungen und Ergänzungen dieses Vertrages einschließlich seiner Anlagen bedürfen der Textform. Dies gilt auch für die Aufhebung dieses Formerfordernisses.
2. Der Auftragsverarbeiter ist berechtigt, diesen Vertrag anzupassen, soweit dies aufgrund einer Änderung der Rechtslage, einer Entscheidung einer Aufsichtsbehörde oder eines Gerichts erforderlich ist. Er teilt die Änderung dem Verantwortlichen mindestens sechs Wochen vor Wirksamwerden in Textform mit. Widerspricht der Verantwortliche nicht innerhalb von sechs Wochen nach Zugang, gilt die Änderung als angenommen; auf diese Folge weist der Auftragsverarbeiter in der Mitteilung hin. Widerspricht der Verantwortliche, ist jede Partei berechtigt, den Hauptvertrag mit einer Frist von 30 Tagen zum Monatsende zu kündigen; bereits im Voraus gezahlte Entgelte erstattet der Auftragsverarbeiter zeitanteilig.
3. Sollte eine Bestimmung dieses Vertrages unwirksam oder undurchführbar sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien ersetzen die unwirksame Bestimmung durch eine wirksame Regelung, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt. Entsprechendes gilt für Regelungslücken.
4. Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.
5. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist der Sitz des Auftragsverarbeiters, sofern der Verantwortliche Kaufmann, eine juristische Person des öffentlichen Rechts oder ein öffentlich-rechtliches Sondervermögen ist. Der Auftragsverarbeiter ist berechtigt, auch am allgemeinen Gerichtsstand des Verantwortlichen zu klagen.

Verantwortlicher

Ort, Datum: _____

Unterschrift: _____

Name, Funktion: _____

Auftragsverarbeiter

Ort, Datum: _____

Unterschrift: _____

Name, Funktion: Yannick Seidel, Inhaber

Anlage 1: Gegenstand, Art und Zweck der Verarbeitung

1. Gegenstand

Bereitstellung der Software Brala als Software as a Service zur Erstellung von Brandlastberechnungen nach DIN 18230 und zur Erzeugung der zugehörigen Dokumente, einschließlich Speicherung der vom Verantwortlichen eingegebenen Projektdaten und Verwaltung der Nutzerkonten seiner Nutzer.

2. Art und Zweck der Verarbeitung

Verarbeitung	Zweck
Erheben, Speichern, Ändern, Auslesen und Löschen von Projekt- und Berechnungsdaten	Durchführung der vom Verantwortlichen veranlassten Berechnungen und Verwaltung seiner Projekte
Erzeugen von Dokumenten im DOCX-Format aus diesen Daten	Bereitstellung der Berechnungsergebnisse in weiterverarbeitbarer Form
Speichern und Verwalten von Nutzerkonten, Authentifizierung, Sitzungsverwaltung	Zugangskontrolle und Zuordnung der Projekte zum jeweiligen Konto des Verantwortlichen
Speichern eigener Dokumentvorlagen des Verantwortlichen (nur im Tarif Ingenieur)	Erzeugung der Dokumente im Layout des Verantwortlichen
Sicherung der Daten (Backup)	Wiederherstellbarkeit nach einem Ausfall

Die Verarbeitung erfolgt automatisiert. Ein manueller Zugriff des Auftragsverarbeiters auf Inhaltsdaten erfolgt nur zur Fehleranalyse und Störungsbeseitigung, auf Anforderung oder Weisung des Verantwortlichen sowie soweit gesetzlich geboten. Eine automatisierte Entscheidungsfindung einschließlich Profiling im Sinne des Art. 22 DSGVO findet nicht statt.

3. Art der personenbezogenen Daten

- Bestandsdaten der Nutzer des Verantwortlichen: Name, dienstliche E-Mail-Adresse, Kontokennung, Rolle im Konto
- Anmelde- und Nutzungsdaten: Anmeldezeitpunkte, Sitzungskennungen, Kennwörter ausschließlich als Hashwert beim Unterauftragsverarbeiter für die Authentifizierung
- Projekt- und Berechnungsdaten, soweit sie personenbezogene Angaben enthalten: Projektbezeichnung, Objektadresse, Angaben zum Bauherrn oder Auftraggeber, Namen von Ansprechpartnern, Bearbeitervermerke, Berechnungsparameter
- Inhalte vom Verantwortlichen hochgeladener Dokumentvorlagen, soweit sie personenbezogene Angaben enthalten

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO und Daten nach Art. 10 DSGVO sind nicht Gegenstand der Verarbeitung. Der Verantwortliche gibt solche Daten nicht in die Software ein.

4. Kategorien betroffener Personen

- Beschäftigte und sonstige Nutzer des Verantwortlichen, die die Software nutzen
- Bauherren, Auftraggeber und deren Ansprechpartner, soweit der Verantwortliche entsprechende Angaben eingibt
- weitere natürliche Personen, soweit der Verantwortliche Angaben zu ihnen in Projektdaten oder Vorlagen einträgt

5. Dauer der Verarbeitung

Die Verarbeitung dauert bis zur Beendigung des Hauptvertrages; danach gilt § 12 dieses Vertrages.

Anlage 2: Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Stand: 28. August 2026. Die Maßnahmen gelten für die Verarbeitung durch den Auftragsverarbeiter. Für die in Anlage 3 genannten Unterauftragsverarbeiter gelten deren eigene, vertraglich vereinbarte Maßnahmen; deren Nachweise hält der Auftragsverarbeiter vor.

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

Zutrittskontrolle. Der Auftragsverarbeiter betreibt keine eigenen Rechenzentren. Die Server stehen in einem Rechenzentrum des in Anlage 3 genannten Hostingdienstleisters in Frankfurt am Main. Für die physische Sicherheit gelten dessen Maßnahmen (Zutritt nur für berechtigtes Personal, Videoüberwachung, Zugangsprotokollierung). Arbeitsplatzgeräte des Auftragsverarbeiters befinden sich in nicht öffentlich zugänglichen Räumen.

Zugangskontrolle. Zugriff auf den Server ausschließlich über SSH mit Schlüsselpaar; Anmeldung mit Kennwort ist deaktiviert. Automatische Sperrung wiederholt fehlschlagender Anmeldeversuche (fail2ban). Paketfilter auf dem Server (nur die Ports 22, 443 und 80) und zusätzlich eine vom Server unabhängige Firewall auf Ebene des Hostingdienstleisters. Automatische Einspielung sicherheitsrelevanter Aktualisierungen des Betriebssystems. Arbeitsplatzgeräte sind verschlüsselt und durch Kennwort gesichert.

Zugriffskontrolle. Der Zugang zur Anwendung erfolgt über den in Anlage 3 genannten Authentifizierungsdienst. Kennwörter werden ausschließlich dort und nur als Hashwert gespeichert; der Auftragsverarbeiter hat keinen Zugriff auf Kennwörter im Klartext. Berechtigungen sind rollenbasiert. Administrative Zugriffe auf Server und Datenbank sind allein dem Inhaber möglich. Der Grundsatz der geringstmöglichen Berechtigung wird beachtet.

Trennungskontrolle. Die Daten verschiedener Kunden werden in der Anwendung logisch getrennt; jeder Nutzer erhält ausschließlich Zugriff auf die Daten seines eigenen Kontos. Die Trennung wird bei jedem Zugriff auf Anwendungsebene erzwungen. Produktiv- und Entwicklungsumgebung sind getrennt; für Entwicklung und Test werden keine Echtdateien von Kunden verwendet.

Pseudonymisierung und Datenminimierung. Es werden nur die für die Vertragserfüllung erforderlichen Daten erhoben. Zahlungsdaten werden nicht beim Auftragsverarbeiter, sondern ausschließlich beim Zahlungsdienstleister gespeichert; lokal werden nur Kennungen des Zahlungsdienstleisters vorgehalten (Kunden-, Abo- und Zahlungsmittel-Kennung), aus denen sich keine Karten- oder Kontodaten ergeben. Die Reichweitenmessung arbeitet ohne Cookies und ohne Zusammenführung mit Nutzerkonten.

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

Weitergabekontrolle. Sämtliche Verbindungen zwischen Nutzergerät und Anwendung sind transportverschlüsselt (HTTPS/TLS, Zertifikate über Let's Encrypt, automatische Erneuerung). Verbindungen zwischen Anwendung und Datenbank sowie zu den Unterauftragsverarbeitern erfolgen verschlüsselt. E-Mail-Versand erfolgt transportverschlüsselt. Ein Transport physischer Datenträger findet nicht statt.

Eingabekontrolle. Änderungen an Projektdaten sind dem jeweiligen Nutzerkonto zugeordnet und mit Zeitstempel versehen. Zugriffe auf den Server werden protokolliert; die Protokolle sind nicht öffentlich zugänglich und werden nach sieben Tagen überschrieben. Administrative Eingriffe erfolgen ausschließlich über nachvollziehbare, versionierte Auslieferungen des Anwendungsstandes.

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

Datensicherung. Tägliche automatische Sicherung der Datenbank und der Datenablagen mit einer Vorhaltezeit von 14 Tagen. Zusätzlich wöchentliches Voll-Abbild des Servers beim Hostingdienstleister.

Betrieb. Dienste laufen in Containern mit automatischem Neustart bei Ausfall. Der Hostingdienstleister überwacht die Verfügbarkeit der Infrastruktur.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

- Jährliche Überprüfung dieses Maßnahmenkatalogs sowie der Datenschutzverträge und Subprozessorenlisten der Unterauftragsverarbeiter, zusätzlich anlassbezogen bei Änderungen.
- Fortlaufende Einspielung von Sicherheitsaktualisierungen für Betriebssystem und Abhängigkeiten.
- Führung eines Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO.
- Dokumentierter Ablauf für den Fall einer Verletzung des Schutzes personenbezogener Daten einschließlich der Meldefristen nach § 9 dieses Vertrages.

5. Auftragskontrolle (Art. 28 DSGVO)

Mit allen Unterauftragsverarbeitern bestehen Verträge nach Art. 28 DSGVO. Die jeweils geltende Fassung wird mit Stand dokumentiert und mindestens jährlich neu geprüft. Neue Unterauftragsverarbeiter werden vor dem Einsatz auf ihre Eignung und auf das Vorliegen eines wirksamen Vertrages geprüft.

6. Löschung

Die Daten werden nach den in § 12 dieses Vertrages genannten Fristen gelöscht. Die Löschung wird vom Auftragsverarbeiter durchgeführt und auf Anforderung bestätigt. Sicherungskopien werden mit Ablauf des jeweiligen Sicherungszyklus überschrieben.

Anlage 3: Genehmigte Unterauftragsverarbeiter

Stand: 26. August 2026. Die jeweils aktuelle Fassung dieser Liste stellt der Auftragsverarbeiter auf Anforderung zur Verfügung.

Unterauftragsverarbeiter	Sitz	Leistung	Ort der Verarbeitung	Drittlandbezug und Grundlage
Hostinger International Ltd., 61 Lordou Vironos str., 6023 Larnaca, Zypern	Zypern, operativ Litauen	Betrieb des Servers (VPS), Speicherung der Projekt- und Berechnungsdaten, Datensicherung, E-Mail-Infrastruktur	Deutschland (Frankfurt am Main)	Kein eigener Transfer. Der Dienstleister setzt eigene Unterauftragsverarbeiter mit möglichem Drittlandbezug ein; abgesichert über Standardvertragsklauseln (Anhang zum Datenschutzvertrag des Dienstleisters).
Clerk, Inc., 660 King Street Unit 345, San Francisco, CA 94107, USA	USA	Authentifizierung, Verwaltung der Nutzerkonten und Sitzungen	USA	USA. Grundlage: EU-US Data Privacy Framework (Selbstzertifizierung des Dienstleisters), ergänzend Standardvertragsklauseln der Module 1 und 2 nach dem Datenschutzvertrag des Dienstleisters.

Nachrichtlich, kein Unterauftragsverarbeiter dieses Vertrages: Stripe Payments Europe, Limited, One Wilton Park, Wilton Place, Dublin 2, D02 FX04, Irland, wickelt die Zahlungen für den Vertrag zwischen den Parteien ab. Diese Verarbeitung nimmt der Auftragsverarbeiter in eigener Verantwortlichkeit nach § 2 Abs. 2 lit. a vor; auftragsweise verarbeitete Daten des Verantwortlichen werden dorthin nicht übermittelt.

Anlage 4: Weisungsbefugte Personen des Verantwortlichen

Name	Funktion	E-Mail	Telefon
_____	_____	_____	_____
_____	_____	_____	_____

Ohne Eintragung gelten die im Kundenkonto hinterlegten Administratoren als weisungsbefugt (§ 3 Abs. 3).