EasyBench

Vertrag zur Auftragsverarbeitung

gemäß Art. 28 DSGVO für die Nutzung der Webanwendung „EasyBench“

Vertrag zwischen

Auftraggeber

den Nutzern der Webanwendung „EasyBench“, die EasyBench als Unternehmer zur Verarbeitung personenbezogener Daten im eigenen Verantwortungsbereich nutzen,
nachfolgend jeweils „Auftraggeber“

und

Auftragnehmer

Leon Gremer, handelnd unter „EasyBench - Inhaber Leon Gremer“
An der Brauerei 5
56575 Weißenthurm
Deutschland
E-Mail: info@easybench.app
nachfolgend „Auftragnehmer“

Geltungsbereich
Auftragsverarbeitung im Rahmen der SaaS-Webanwendung EasyBench

Dokumentstand
08.06.2026

Hinweis zur Online-Einbeziehung: Dieser Vertrag ist als einheitlicher Online-Vertrag für alle Auftraggeber ausgestaltet. Er wird Bestandteil des jeweiligen SaaS-Hauptvertrages, wenn der Auftraggeber ihn im Registrierungs- oder Bestellprozess akzeptiert. Eine gesonderte handschriftliche Unterzeichnung durch den Auftraggeber ist nicht vorgesehen.

Inhaltsverzeichnis

1. Präambel und Rangverhältnis

Der Auftragnehmer stellt den Auftraggebern die cloudbasierte Webanwendung "EasyBench" als Software-as-a-Service für Malerbetriebe bereit. Im Rahmen der Nutzung können Auftraggeber personenbezogene Daten in eigener datenschutzrechtlicher Verantwortlichkeit in EasyBench eingeben, speichern, bearbeiten, exportieren und löschen lassen.

Dieser Vertrag regelt die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des jeweiligen Auftraggebers im Sinne von Art. 28 DSGVO. Er konkretisiert die datenschutzrechtlichen Pflichten der Parteien für alle Verarbeitungsvorgänge, bei denen der Auftragnehmer personenbezogene Daten nicht zu eigenen Zwecken, sondern auf dokumentierte Weisung des Auftraggebers verarbeitet.

Der SaaS-Hauptvertrag, die Allgemeinen Geschäftsbedingungen des Auftragnehmers und dieser Vertrag bilden zusammen die vertragliche Grundlage der Leistungserbringung. Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen die Bestimmungen dieses Vertrages für Fragen der Auftragsverarbeitung vor. Für kaufmännische, abrechnungsbezogene, eigene Sicherheits-, Vertrags- und Nachweisverarbeitungen des Auftragnehmers gilt dieser Vertrag nur, soweit der Auftragnehmer hierbei tatsächlich als Auftragsverarbeiter handelt.

Die Anlagen sind Bestandteil dieses Vertrages. Anlage 1 beschreibt insbesondere Gegenstand, Art, Zweck und Dauer der Verarbeitung sowie Datenarten und betroffene Personen. Anlage 2 enthält die genehmigten Unterauftragnehmer. Anlage 3 beschreibt die technischen und organisatorischen Maßnahmen des Auftragnehmers.

2. Begriffsbestimmungen und Rollen der Parteien

"Auftraggeber" sind die Nutzer der Webanwendung "EasyBench", soweit sie EasyBench als Unternehmer einsetzen und dabei personenbezogene Daten im eigenen Verantwortungsbereich in der Webanwendung verarbeiten. Mehrere Auftraggeber schließen jeweils rechtlich eigenständig einen gleichlautenden Vertrag mit dem Auftragnehmer ab.

"Auftragnehmer" ist Leon Gremer, handelnd unter "EasyBench - Inhaber Leon Gremer".

"Hauptvertrag" bezeichnet den jeweiligen Vertrag über die Nutzung der Webanwendung EasyBench einschließlich der Allgemeinen Geschäftsbedingungen und der Leistungsbeschreibung.

"Mandant" bezeichnet den logisch abgegrenzten Unternehmensbereich eines Auftraggebers innerhalb der Webanwendung EasyBench.

"Mandantendaten" sind alle personenbezogenen Daten und sonstigen Inhalte, die der Auftraggeber oder dessen berechtigte Benutzer im Mandantenbereich eingeben, importieren, speichern, erzeugen oder verarbeiten lassen, soweit diese Daten nicht ausschließlich eigenen Verarbeitungszwecken des Auftragnehmers dienen.

"Weisung" ist jede dokumentierte Anordnung des Auftraggebers zur Verarbeitung personenbezogener Daten. Weisungen ergeben sich insbesondere aus diesem Vertrag, dem Hauptvertrag, der Nutzung der bereitgestellten Funktionen, den Einstellungen im Benutzerkonto, Export- und Löschanforderungen sowie aus schriftlichen oder in Textform erteilten Einzelweisungen.

Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO für die durch ihn in EasyBench verarbeiteten Mandantendaten. Der Auftragnehmer ist insoweit Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 und Art. 28 DSGVO.

3. Gegenstand, Umfang und Dauer der Verarbeitung

Gegenstand des Auftrags ist die technische Bereitstellung, der Betrieb, die Sicherung, Wartung und Weiterentwicklung der Webanwendung EasyBench einschließlich Authentifizierungsdienst, API, Datenbank, Dokumentenspeicher, Exportfunktionen, Support, transaktionalem E-Mail-Versand, Backups und Löschprozessen.

Die Verarbeitung erfolgt insbesondere unter den Domains https://easybench.app, https://auth.easybench.app und https://api.easybench.app. Die administrative Speicheroberfläche https://minio.easybench.app ist ausschließlich für administrative Zugriffe des Auftragnehmers bestimmt.

Der Umfang der Verarbeitung richtet sich nach dem Hauptvertrag, den vom Auftraggeber gebuchten Funktionen und den innerhalb der Webanwendung eingegebenen Daten. Der Auftragnehmer verarbeitet personenbezogene Daten nur, soweit dies zur Bereitstellung, Sicherung, Wartung, Unterstützung,

Fehlerbehebung, Exportierung, Löschung oder Wiederherstellung der vereinbarten Leistungen erforderlich ist.

Die Verarbeitung beginnt mit Abschluss des Hauptvertrages beziehungsweise mit Registrierung und Einrichtung eines Mandanten. Sie endet grundsätzlich mit Abschluss der Löschung nach Beendigung des Hauptvertrages oder der Testphase, soweit keine gesetzlichen Speicherpflichten, Nachweispflichten oder Rechtsverteidigungsinteressen entgegenstehen.

Bei kostenpflichtigen Abonnements endet mit Vertragsende der produktive Zugriff. Für 90 Kalendertage ab Vertragsende stellt der Auftragnehmer einen eingeschränkten Zugriff auf Export- und Datenabruffunktionen bereit. Nach Ablauf dieser Frist werden die Mandantendaten aus den Produktivsystemen gelöscht.

Bei kostenlosen Testphasen bleiben Mandantendaten nach Ablauf der Testphase für 30 Kalendertage im eingeschränkten Exportzugang verfügbar. Danach werden sie aus den Produktivsystemen gelöscht, sofern kein kostenpflichtiges Abonnement abgeschlossen wurde.

In rotierenden Backups können bereits gelöschte Daten für höchstens weitere sieben Tage enthalten sein. Administrative Snapshots werden ausschließlich zu Rollback-Zwecken erstellt und spätestens mit dem nächsten Deployment beziehungsweise der nächsten veröffentlichten Version gelöscht, sobald der Sicherungszweck entfallen ist.

4. Art, Zweck, Datenarten und Kategorien betroffener Personen

Art und Zweck der Verarbeitung ergeben sich im Einzelnen aus Anlage 1. Die Verarbeitung umfasst insbesondere das Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Bereitstellung, Übermitteln, Abgleichen, Einschränken, Löschen und Vernichten personenbezogener Daten im Sinne von Art. 4 Nr. 2 DSGVO.

Der Zweck der Verarbeitung ist die Bereitstellung einer SaaS-Anwendung für Malerbetriebe, insbesondere zur Verwaltung von Kunden, Ansprechpartnern, Baustellen, Angeboten, Aufmaßen, Rechnungen, Rechnungspositionen, Bankverbindungen, Zahlungsinformationen, Logos, Notizen, Mitarbeiterdaten, Rollen und Berechtigungen.

Die Kategorien personenbezogener Daten umfassen insbesondere Namen, Kontaktdaten, Firmen- und Objektanschriften, Projekt- und Baustellendaten, Rechnungs- und Angebotsdaten, Zahlungsinformationen, Bankverbindungen, Mitarbeiter- und Rollendaten, Kommunikations- und Notizdaten, Logos sowie technische Nutzungs-, Sitzungs-, Export- und Protokolldaten.

Kategorien betroffener Personen sind insbesondere Kunden und Interessenten des Auftraggebers, Ansprechpartner, Mitarbeiter und sonstige Beschäftigte des Auftraggebers, eingeladene Benutzer, externe Steuerberater oder sonstige vom Auftraggeber eingebundene Personen sowie sonstige Personen, deren Daten der Auftraggeber in EasyBench verarbeitet.

Die planmäßige Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO ist nicht Gegenstand der Leistung. Der Auftraggeber darf solche Daten nur verarbeiten, wenn hierfür eine eigenständige Rechtsgrundlage besteht, die Verarbeitung für den Einsatz von EasyBench erforderlich ist und die Nutzung der Anwendung hierfür angemessen ist. Freitextfelder, Notizen und hochgeladene Inhalte sind vom Auftraggeber entsprechend kontrolliert zu verwenden.

5. Weisungen des Auftraggebers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf Grundlage dokumentierter Weisungen des Auftraggebers, sofern er nicht nach Unionsrecht oder dem Recht der Mitgliedstaaten zu einer anderen Verarbeitung verpflichtet ist. 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.

Die erstmalige Weisung ergibt sich aus diesem Vertrag, dem Hauptvertrag, den dort beschriebenen Leistungen sowie der konkreten Nutzung der Webanwendung durch den Auftraggeber und seine berechtigten Benutzer.

Einzelweisungen können in Textform erteilt werden. Weisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, können eine gesonderte Vereinbarung und Vergütung erfordern.

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Auffassung ist, dass eine Weisung gegen Datenschutzrecht verstößt. Der Auftragnehmer ist berechtigt, die Ausführung der betreffenden Weisung bis zur Bestätigung, Änderung oder Rücknahme durch den Auftraggeber auszusetzen, soweit dies zur Vermeidung eines Datenschutzverstosses erforderlich ist.

Weisungen zur Löschung oder Herausgabe von Daten während eines laufenden kostenpflichtigen Abonnements können abgelehnt werden, soweit die Daten für die Vertragserfüllung, Systemsicherheit, gesetzliche Pflichten oder den ordnungsgemäßen Betrieb zwingend erforderlich sind. Nach Vertragsende gelten die vereinbarten Export- und Löschfristen.

6. Pflichten des Auftragnehmers

Der Auftragnehmer verpflichtet sich, personenbezogene Daten nur im Rahmen dieses Vertrages und der dokumentierten Weisungen des Auftraggebers zu verarbeiten.

Der Auftragnehmer stellt sicher, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Der Auftragnehmer trifft die in Anlage 3 beschriebenen technischen und organisatorischen Maßnahmen und überprüft diese regelmäßig. Die Maßnahmen dürfen weiterentwickelt und angepasst werden, sofern das vereinbarte Schutzniveau nicht wesentlich unterschritten wird.

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, soweit diese Pflichten die Auftragsverarbeitung betreffen.

Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen betroffener Personen auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit oder Widerspruch.

Der Auftragnehmer führt ein Verzeichnis der Verarbeitungstätigkeiten als Auftragsverarbeiter, soweit er hierzu gesetzlich verpflichtet ist.

Der Auftragnehmer hat personenbezogene Daten gegen unbefugte Kenntnisnahme, Verlust, Veränderung und Zerstörung zu schützen. Absolute Sicherheit kann technisch nicht garantiert werden; maßgeblich ist ein dem Risiko angemessenes Schutzniveau.

7. Technische und organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen des Auftragnehmers sind in Anlage 3 beschrieben. Sie orientieren sich an Art. 32 DSGVO und umfassen insbesondere Zugriffskontrolle, Zugangskontrolle, Berechtigungskonzepte, Mandantentrennung, Transportverschlüsselung, Sicherungskopien, Protokollierung, Wiederherstellbarkeit und Verfügbarkeit.

Die Parteien sind sich einig, dass technische und organisatorische Maßnahmen einem technischen Wandel unterliegen. Der Auftragnehmer darf alternative angemessene Maßnahmen umsetzen, sofern diese das bisherige Schutzniveau nicht unterschreiten.

Wesentliche Verschlechterungen des Schutzniveaus sind dem Auftraggeber mitzuteilen, soweit sie für die Auftragsverarbeitung relevant sind.

Der Auftraggeber ist für die sichere Nutzung der Anwendung in seinem Verantwortungsbereich verantwortlich. Dazu gehören insbesondere die Vergabe geeigneter Rollen, die Auswahl berechtigter Benutzer, die Sicherung eigener Endgeräte und die Prüfung der Rechtmäßigkeit der von ihm eingegebenen Daten.

8. Vertraulichkeit und Personal

Der Auftragnehmer setzt für die regelmäßige Administration der produktiven Systeme grundsätzlich nur Personen ein, die zur Vertraulichkeit verpflichtet wurden. Als Einzelunternehmer verarbeitet der Auftragnehmer Daten im Regelbetrieb persönlich.

Externe Dienstleister oder Unterauftragnehmer erhalten Zugriff auf personenbezogene Daten nur, soweit dies für die vereinbarte Leistung erforderlich ist und die Voraussetzungen dieses Vertrages eingehalten werden.

Der Auftragnehmer weist Personen mit Zugriff auf personenbezogene Daten auf die datenschutzrechtlichen Pflichten hin und beschränkt Zugriffe auf das erforderliche Maß.

Die Vertraulichkeitspflichten bestehen auch nach Beendigung des Auftrags fort.

9. Unterauftragnehmer

Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung zum Einsatz der in Anlage 2 genannten Unterauftragnehmer.

Der Auftragnehmer darf weitere Unterauftragnehmer einsetzen oder bestehende Unterauftragnehmer ersetzen, wenn der Auftraggeber vorher in Textform oder über einen dauerhaft abrufbaren elektronischen Hinweis informiert wird und ihm eine angemessene Frist zum Widerspruch aus wichtigem datenschutzrechtlichem Grund eingeräumt wird. Eine Frist von 30 Kalendertagen gilt regelmäßig als angemessen, sofern nicht aus Sicherheits-, Rechts- oder Betriebsgründen eine kürzere Frist erforderlich ist.

Widerspricht der Auftraggeber aus wichtigem datenschutzrechtlichem Grund, werden die Parteien eine zumutbare Lösung suchen. Ist eine Fortsetzung der Leistung ohne den betreffenden Unterauftragnehmer für den Auftragnehmer wirtschaftlich oder technisch nicht zumutbar, kann der Auftragnehmer den Hauptvertrag unter Wahrung der vereinbarten Export- und Löschregelungen beenden.

Der Auftragnehmer schliesst mit Unterauftragnehmern Vereinbarungen, die diesen im Wesentlichen dieselben Datenschutzpflichten auferlegen, die dem Auftragnehmer nach diesem Vertrag obliegen.

Nicht als Unterauftragnehmer im Sinne dieses Vertrages gelten Personen oder Stellen, die Daten ausschließlich in eigener Verantwortlichkeit des Auftragnehmers verarbeiten, etwa Zahlungsdienstleister für die Abonnementzahlung, Buchhaltungssysteme für eigene Rechnungen oder Steuerberater, soweit sie nicht Mandantendaten im Auftrag des Auftraggebers verarbeiten.

10. Drittlandübermittlungen

Die zentrale Produktiv- und Backup-Infrastruktur wird am Hetzner-Standort Nürnberg innerhalb der Europäischen Union betrieben.

Eine Übermittlung von Mandantendaten in Drittländer erfolgt nicht planmäßig. Soweit ein Unterauftragnehmer oder Supportdienst in einem Einzelfall Zugriff aus einem Drittland ermöglichen sollte, stellt der Auftragnehmer sicher, dass die Voraussetzungen der Art. 44 ff. DSGVO eingehalten werden, insbesondere durch Angemessenheitsbeschluss, EU-U.S. Data Privacy Framework, Standardvertragsklauseln oder eine andere geeignete Garantie.

Produktive Mandantendaten werden nicht planmäßig an GitHub, JetBrains, Mend.io, Stripe, PayPal oder Lexware als Unterauftragnehmer der SaaS-Verarbeitung übertragen. Zahlungen, Buchhaltung und Entwicklungswerkzeuge betreffen grundsätzlich eigene Verarbeitungen des Auftragnehmers und nicht die Auftragsverarbeitung von Mandantendaten.

11. Unterstützung des Auftraggebers

Der Auftragnehmer unterstützt den Auftraggeber im Rahmen des Zumutbaren bei der Erfüllung datenschutzrechtlicher Pflichten, soweit diese die Auftragsverarbeitung betreffen und soweit dem Auftragnehmer die hierfür erforderlichen Informationen vorliegen.

Dies umfasst insbesondere technische Auskünfte zur Verarbeitung, Unterstützung bei Auskunfts- und Löschersuchen, Informationen zu Unterauftragnehmern, Unterstützung bei der Untersuchung von Sicherheitsvorfällen sowie die Bereitstellung von Informationen zu den technischen und organisatorischen Maßnahmen.

Anfragen betroffener Personen, die erkennbar Mandantendaten eines Auftraggebers betreffen, beantwortet der Auftragnehmer nicht eigenständig inhaltlich, sondern leitet diese an den Auftraggeber weiter oder stimmt die weitere Bearbeitung mit diesem ab.

Für Unterstützungsleistungen, die über den vertraglich geschuldeten Umfang hinausgehen oder durch rechtswidrige, unvollständige oder unverhältnismäßige Weisungen des Auftraggebers verursacht werden, kann der Auftragnehmer eine angemessene Vergütung verlangen, soweit dies im Einzelfall vereinbart wird.

12. Meldung von Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer informiert den Auftraggeber unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist, die Mandantendaten des Auftraggebers betrifft.

Die Mitteilung enthält, soweit zu diesem Zeitpunkt verfügbar, insbesondere eine Beschreibung des Vorfalls, die betroffenen Daten- und Personenkategorien, die ungefähre Zahl betroffener Personen und Datensätze,

wahrscheinliche Folgen, bereits ergriffene oder vorgeschlagene Maßnahmen sowie einen Ansprechpartner für Rückfragen.

Der Auftragnehmer wird angemessene Maßnahmen zur Begrenzung möglicher nachteiliger Folgen ergreifen und den Auftraggeber im Rahmen des Zumutbaren bei dessen Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO unterstützen.

Die Entscheidung über Meldungen an Aufsichtsbehörden oder Benachrichtigungen betroffener Personen obliegt grundsätzlich dem Auftraggeber als Verantwortlichem, soweit nicht der Auftragnehmer selbst gesetzlich zu einer Meldung verpflichtet ist.

13. Löschung, Rückgabe, Exportfrist und Nachweise

Während der Vertragslaufzeit kann der Auftraggeber Daten über die bereitgestellten Funktionen exportieren, bearbeiten und löschen, soweit dies technisch vorgesehen und vertraglich vereinbart ist.

Nach Ende eines kostenpflichtigen Abonnements stellt der Auftragnehmer für 90 Kalendertage einen eingeschränkten Export- und Datenabrufzugang bereit. Nach Ablauf dieser Frist löscht der Auftragnehmer die Mandantendaten aus den Produktivsystemen.

Nach Ende einer kostenlosen Testphase stellt der Auftragnehmer für 30 Kalendertage einen eingeschränkten Exportzugang bereit. Danach werden die Mandantendaten aus den Produktivsystemen gelöscht, sofern kein kostenpflichtiges Abonnement abgeschlossen wurde.

Verlangt der Auftraggeber nach Vertragsende eine vorzeitige Löschung und verzichtet damit auf weiteren Datenabruf, kann die Exportfrist beendet und der Löschprozess eingeleitet werden.

Nach Abschluss der Löschung versendet der Auftragnehmer eine Löschbestätigung per E-Mail. In rotierenden Backups können gelöschte Daten für höchstens sieben weitere Tage enthalten sein. Diese Backups werden ausschließlich zur Wiederherstellung nach technischen Störungen oder Sicherheitsvorfällen verwendet.

Der Auftragnehmer speichert Exportprotokolle und Löschbestätigungen für zwei Jahre. Das Exportprotokoll enthält insbesondere eine technische Protokollkennung, Mandantenkennung, Dateinamen, Hashwert, Anzahl enthaltener Dateien und Rechnungen, Gesamtgröße in Byte und Erstellungszeitpunkt. Inhalte der exportierten Dokumente werden im Exportprotokoll nicht gespeichert.

Daten, die der Auftragnehmer in eigener Verantwortlichkeit aus gesetzlichen Gründen oder zur Rechtsverteidigung speichern muss, insbesondere eigene Rechnungen, Zahlungsbelege, Vertragsunterlagen und Nachweisdaten, bleiben von der Löschung der Mandantendaten unberührt. Diese Daten werden nach Ablauf der jeweiligen gesetzlichen Fristen gelöscht.

14. Kontrollen und Nachweise

Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung, soweit diese Informationen die konkrete Auftragsverarbeitung betreffen.

Der Nachweis kann insbesondere durch Bereitstellung dieses Vertrages, der Anlagen, der aktuellen Unterauftragnehmerliste, Beschreibungen der technischen und organisatorischen Maßnahmen, Datenschutz- und Sicherheitsdokumentationen, Auskünfte, Zertifikate, Prüfergebnisse oder geeignete Selbstauskünfte erfolgen.

Vor-Ort-Kontrollen sind nur nach vorheriger Abstimmung, mit angemessener Ankündigungsfrist, während üblicher Geschäftszeiten und ohne Gefährdung von Sicherheit, Betriebsablauf, Vertraulichkeit anderer Auftraggeber oder Rechten Dritter zulässig. Sie dürfen nur durch fachkundige und zur Vertraulichkeit verpflichtete Personen durchgeführt werden.

Der Auftraggeber hat Kontrollen auf das erforderliche Maß zu beschränken. Der Auftragnehmer kann für Kontrollen, die über die Bereitstellung vorhandener Nachweise hinausgehen, eine angemessene Vergütung verlangen, sofern der Kontrollbedarf nicht durch einen vom Auftragnehmer zu vertretenden Datenschutzverstoss verursacht wurde.

Ergebnisse von Kontrollen und dabei erhaltene Informationen sind vertraulich zu behandeln und dürfen nur für Datenschutz- und Compliance-Zwecke im Zusammenhang mit diesem Vertrag verwendet werden.

15. Pflichten des Auftraggebers

Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Mandantendaten, für die Wahrung der Rechte betroffener Personen und für die Erteilung rechtmäßiger Weisungen verantwortlich.

Der Auftraggeber stellt sicher, dass er personenbezogene Daten nur verarbeitet, soweit hierfür eine Rechtsgrundlage besteht, Informationspflichten erfüllt wurden und die Daten für die Nutzung von EasyBench geeignet sind.

Der Auftraggeber ist für die Verwaltung seiner Benutzer, Rollen, Berechtigungen und Endgeräte verantwortlich. Er hat Zugangsdaten geheim zu halten, sichere Passwörter zu verwenden, unbefugte Zugriffe unverzüglich mitzuteilen und Benutzer zu entfernen, sobald deren Zugriff nicht mehr erforderlich ist.

Der Auftraggeber darf keine Daten in EasyBench einstellen, deren Verarbeitung gegen geltendes Recht, Rechte Dritter, behördliche Anordnungen oder vertragliche Vereinbarungen verstößt.

Der Auftraggeber ist für eigene Sicherungen und Exporte verantwortlich, soweit diese für seine gesetzlichen Aufbewahrungs- oder Nachweispflichten erforderlich sind. Die Bereitstellung von Backups durch den Auftragnehmer ersetzt keine eigenverantwortliche Archivierung des Auftraggebers, insbesondere nicht handels- oder steuerrechtliche Aufbewahrungspflichten des Auftraggebers.

Der Auftraggeber hat den Auftragnehmer unverzüglich zu informieren, wenn er Fehler, Sicherheitslücken, unbefugte Zugriffe oder sonstige Datenschutzrisiken im Zusammenhang mit EasyBench feststellt.

16. Haftung, Freistellung und Kostentragung

Die Haftung der Parteien richtet sich nach den gesetzlichen Vorschriften und dem Hauptvertrag, soweit dieser Vertrag keine spezielleren Regelungen für die Auftragsverarbeitung enthält.

Der Auftraggeber stellt den Auftragnehmer von Ansprüchen frei, die auf einer rechtswidrigen Weisung, einer unzulässigen Dateneingabe, einer Verletzung von Informationspflichten, einer unzulässigen Verarbeitung durch den Auftraggeber oder einer Verletzung der Pflichten des Auftraggebers aus diesem Vertrag beruhen, soweit der Auftragnehmer den Schaden nicht selbst zu vertreten hat.

Der Auftragnehmer haftet für eigenes Verschulden und für Verstöße gegen spezifische Pflichten als Auftragsverarbeiter nach den gesetzlichen Vorschriften. Eine weitergehende Haftung nach dem Hauptvertrag bleibt unberührt.

Kosten für außerordentliche Weisungen, umfangreiche Sonderauskünfte, Sonderlöschungen, Migrationen oder Kontrollen können gesondert vereinbart werden, soweit sie nicht bereits vom vertraglich geschuldeten Leistungsumfang umfasst sind oder durch ein pflichtwidriges Verhalten des Auftragnehmers erforderlich wurden.

17. Laufzeit, Beendigung und Fortgeltung

Dieser Vertrag tritt mit Abschluss des Hauptvertrages beziehungsweise mit seiner elektronischen Akzeptanz durch den Auftraggeber in Kraft.

Der Vertrag endet, wenn die Auftragsverarbeitung beendet ist, insbesondere nach Ablauf des Hauptvertrages, Abschluss der Exportfrist und Abschluss der Löschung der Mandantendaten, soweit keine gesetzlichen Pflichten oder Nachweisinteressen eine weitere Verarbeitung einzelner Daten rechtfertigen.

Die Pflichten zur Vertraulichkeit, zum Nachweis, zur Löschung, zur Rechtsverteidigung und zur Wahrung von Geschäftsgeheimnissen gelten fort, soweit ihre Natur dies erfordert.

Endet der Hauptvertrag, bleibt dieser Vertrag für die Export-, Rückgabe-, Lösch- und Nachweisphase anwendbar.

18. Schlussbestimmungen

Änderungen und Ergänzungen dieses Vertrages bedürfen mindestens der Textform oder einer elektronischen Bereitstellung mit dokumentierter Zustimmung, soweit nicht zwingendes Recht eine strengere Form verlangt.

Der Auftragnehmer kann diesen Vertrag anpassen, soweit dies aufgrund geänderter Rechtslage, technischer Weiterentwicklung, Änderungen der Dienste, geänderter Unterauftragnehmer oder zur Aufrechterhaltung eines angemessenen Datenschutzniveaus erforderlich ist. Der Auftraggeber wird hierüber in angemessener Weise informiert. Wesentliche nachteilige Änderungen werden nicht ohne angemessene Vorankündigung wirksam, soweit keine dringenden Sicherheits- oder Rechtsgründe entgegenstehen.

Sollten einzelne Bestimmungen dieses Vertrages unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien werden die unwirksame Regelung durch eine wirksame Regelung ersetzen, die dem wirtschaftlichen und datenschutzrechtlichen Zweck am nächsten kommt.

Es gilt das Recht der Bundesrepublik Deutschland, soweit dem keine zwingenden datenschutzrechtlichen Vorschriften entgegenstehen.

Weißenthurm, 08.06.2026

Ort, Datum

EasyBench - Inhaber Leon Gremer

Auftragnehmer

Anlage 1 - Gegenstand des Auftrags

Thema	Beschreibung
Gegenstand des Auftrags	Betrieb, Bereitstellung, Wartung, Sicherung, Support, Export und Löschung der SaaS-Webanwendung EasyBench für Malerbetriebe einschließlich Authentifizierung, API, Datenbank, Dokumentenspeicher, Mandantenverwaltung und Exportfunktionen.
Leistungsumgebung	Öffentliche Website und SEO-Seiten unter https://easybench.app; Authentifizierung unter https://auth.easybench.app; API unter https://api.easybench.app; administrative Speicherverwaltung unter https://minio.easybench.app nur für den Auftragnehmer.
Art der Verarbeitung	Erheben, Erfassen, Speichern, Ordnen, Organisieren, Anzeigen, Bearbeiten, Ändern, Auslesen, Abfragen, Verwenden, Bereitstellen, Exportieren, Übermitteln im Rahmen des Dienstes, Sichern, Wiederherstellen, Einschränken, Löschen und Vernichten.
Zweck der Verarbeitung	Bereitstellung einer SaaS-Anwendung zur digitalen Verwaltung von Malerbetrieben, insbesondere Kundenverwaltung, Angebote, Rechnungen, Aufmass, E-Rechnungsfunktionen, Rollen- und Benutzerverwaltung, Steuerberaterzugang, Export und Anbieterwechsel.
Dauer	Für die Dauer des Hauptvertrages; nach kostenpflichtigem Vertragsende zusätzlich 90 Kalendertage eingeschränkter Exportzugang; nach Testphase 30 Kalendertage Exportzugang; danach Löschung aus Produktivsystemen; Backup-Rotation max. 7 Tage; Exportprotokolle und Löschbestätigungen 2 Jahre.
Hosting	Hetzner Cloud Server am Standort Nürnberg, Deutschland; Hetzner Backups, Snapshots und Firewalls.
Test- und Entwicklungsumgebung	Der Auftragnehmer testet derzeit lokal und nicht mit produktiven Kundendaten. Produktive Mandantendaten werden nicht planmäßig in Entwicklungs- oder Quellcode-Systeme übertragen.

Datenarten	Beispiele
Stammdaten	Name, Firma, Anschrift, E-Mail-Adresse, Telefonnummer, Ansprechpartner, Kunden- und Lieferantenbeziehungen.
Objekt- und Projektdaten	Baustellen- und Objektanschriften, Aufmasse, Leistungsbeschreibungen, Projektnotizen.
Dokumenten- und Rechnungsdaten	Angebote, Rechnungen, Rechnungspositionen, E-Rechnungsdaten, Preise, Mengen, Steuersätze, Rechnungsnummern.
Zahlungs- und Bankdaten	Bankverbindungen, Zahlungsinformationen, Zahlungsstatus, soweit vom Auftraggeber für eigene Rechnungen in EasyBench hinterlegt.
Benutzer- und Rolleninformationen	Benutzername, E-Mail-Adresse, Rollen, Berechtigungen, eingeladene Benutzer, Steuerberaterzugang.
Technische Daten	Sitzungsdaten, aktive IP-Adresse, Browser-Zeitzone, Authentifizierungsstatus, technische Protokolldaten, Exportprotokolle.
Sonstige Inhalte	Logos, Notizen und fachliche Inhalte, die der Auftraggeber in EasyBench eingibt.

Kategorien betroffener Personen	Beschreibung
Kunden und Interessenten des Auftraggebers	Endkunden, Ansprechpartner, Eigentümer, Mieter oder sonstige Beteiligte an Bau- und Malerprojekten, soweit der Auftraggeber deren Daten in EasyBench verarbeitet.
Beschäftigte und Mitarbeiter des Auftraggebers	Mitarbeiter, interne Benutzer, Rollenträger, Ansprechpartner und sonstige vom Auftraggeber eingebundene Personen.

Kategorien betroffener Personen	Beschreibung
Externe Beteiligte	Steuerberater, Buchhalter, externe Ansprechpartner oder sonstige berechtigte Benutzer des Auftraggebers.
Sonstige Personen	Personen, deren Daten der Auftraggeber in Freitexten, Notizen, Dokumenten oder Rechnungsinhalten verarbeitet.

Besondere Kategorien personenbezogener Daten

Die planmäßige Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO ist nicht Gegenstand der Leistung. Die Anwendung ist nicht für die gezielte Verarbeitung solcher Daten bestimmt. Der Auftraggeber hat durch geeignete Nutzung und interne Vorgaben sicherzustellen, dass solche Daten nicht oder nur auf eigener rechtlicher Grundlage verarbeitet werden.

Abgrenzung eigener Verarbeitungen des Auftragnehmers

Nicht Gegenstand der Auftragsverarbeitung sind eigene Verarbeitungen des Auftragnehmers, insbesondere Vertragsabschluss, Abrechnung, Zahlungsabwicklung für das EasyBench-Abonnement, eigene Buchhaltung, steuerrechtliche Aufbewahrung, Missbrauchsabwehr, Rechtsverteidigung und Kommunikation mit dem Auftraggeber, soweit der Auftragnehmer hierbei über Zwecke und Mittel entscheidet.

Anlage 2 - Unterauftragnehmer

Unterauftragnehmer	Sitz	Leistung	Datenkategorien	Ort der Verarbeitung / Hinweise
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen, Deutschland	Cloud Server, Netzwerk, Firewall, Hosting, Backups, Snapshots	Mandantendaten, Datenbankinhalte, Dokumente, technische Protokolle, Sicherungskopien	Rechenzentrumsstandort Nürnberg, Deutschland; AVV abgeschlossen.
Brevo GmbH	Köpenicker Str. 126, 10179 Berlin, Deutschland	Versand transaktionaler E-Mails, insbesondere Registrierung, Sicherheit, Vertragsstatus, Exportfristen und Löschbestätigungen	E-Mail-Adresse, Absenderadresse, Betreff, E-Mail-Inhalt, technische Versand- und Zustelldaten	Deutschland/EU; Oeffnungs- und Klicktracking ist deaktiviert; AVV abgeschlossen.
STRATO GmbH	Otto-Ostrowski-Strasse 7, 10249 Berlin, Deutschland	Domain, DNS, E-Mail-Postfach und Weiterleitung für Supportkommunikation	E-Mail-Adressen, Kommunikationsinhalte und Metadaten, soweit Auftraggeber Mandantendaten in Supportmails übermitteln	Deutschland/EU; AVV, soweit erforderlich.
TeamViewer Germany GmbH	Bahnhofsplatz 2, 73033 Göppingen, Deutschland	Fallweiser Fernsupport nach vorheriger Abstimmung und Freigabe durch den Auftraggeber	Sitzungs- und Verbindungsdaten sowie sichtbare Inhalte während einer freigegebenen Support-Sitzung	Nur bei Bedarf; keine Aufzeichnung durch den Auftragnehmer; AVV vor produktivem Einsatz abzuschließen.

Nicht regelmäßige Unterauftragnehmer für Mandantendaten

Stripe, PayPal, Lexware Office, GitHub, JetBrains/IntelliJ und Mend.io werden nach aktuellem Stand nicht planmäßig als Unterauftragnehmer für Mandantendaten eingesetzt. Stripe und PayPal betreffen die Zahlungsabwicklung des EasyBench-Abonnements in eigener Verantwortlichkeit beziehungsweise nach eigener Rollenverteilung. Lexware Office betrifft die Buchhaltung des Auftragnehmers. GitHub, JetBrains/IntelliJ und Mend.io betreffen Entwicklung und Schwachstellenprüfung ohne planmäßige Übertragung produktiver Mandantendaten.

Änderungen bei Unterauftragnehmern

Der Auftragnehmer informiert Auftraggeber über beabsichtigte Änderungen der Unterauftragnehmer in Textform oder über einen dauerhaft abrufbaren elektronischen Hinweis. Auftraggeber können aus wichtigem datenschutzrechtlichem Grund innerhalb der mitgeteilten Frist widersprechen. Erfolgt kein fristgerechter Widerspruch, gilt die Änderung als genehmigt, soweit sie dem Auftraggeber zumutbar ist und kein wesentlich geringeres Datenschutzniveau entsteht.

Anlage 3 - Technische und organisatorische Maßnahmen des Auftragnehmers

1. Vertraulichkeit - Zugangskontrolle

- Produktivsysteme werden auf Hetzner Cloud Servern am Standort Nürnberg betrieben.
- Administrative Zugriffe sind auf den Auftragnehmer und erforderliche Dienstleister beschränkt.
- Zugriffe auf die administrative Speicherverwaltung unter https://minio.easybench.app sind nicht öffentlich für Kunden bestimmt.
- Firewall-Regeln von Hetzner und eigene Netzwerkkonfigurationen begrenzen erreichbare Dienste.
- Rate Limiting und Brute-Force-Schutz werden über Traefik umgesetzt.
- Zugriffsdaten und Geheimnisse werden nicht im Quellcode veröffentlicht und sind nur für den Betrieb berechtigten Personen zugänglich.

2. Vertraulichkeit - Benutzer- und Zugriffskontrolle

- Authentifizierung erfolgt über eine selbst betriebene Keycloak-Instanz.
- Passwörter werden nicht im Klartext gespeichert, sondern durch Keycloak mit Argon2 gehasht.
- E-Mail-Bestätigung bei Registrierung dient der Verifikation der E-Mail-Adresse; eine allgemeine Zwei-Faktor-Authentifizierung für spätere Kunden-Logins wird derzeit nicht angeboten.
- Zugriffe innerhalb der Anwendung werden rollenbasiert gesteuert.
- Auftraggeber können Benutzer einladen und Rollen vergeben.
- Benutzer- und Mandantenzuordnung beschränken Zugriffe auf den jeweiligen Mandanten.
- IP-Adressen werden nur für aktive Sessions gespeichert und mit Beendigung der Sitzung gelöscht.

3. Vertraulichkeit - Mandantentrennung

- Logische Mandantentrennung erfolgt über Tenant-ID.
- PostgreSQL Row Level Security wird zur zusätzlichen Absicherung der Mandantentrennung eingesetzt.
- Anwendungsseitige Request-Filter prüfen Mandantenkontext und Berechtigungen.
- Unit- und Integrationstests prüfen die Einhaltung der Mandantentrennung.
- Berechtigungen und Rollen werden fachlich eingeschränkt, insbesondere für Mitarbeiter- und Steuerberaterzugriffe.

4. Integrität

- Übertragung personenbezogener Daten erfolgt über HTTPS/TLS.
- Datenbank und Objektspeicher werden in der geschützten Serverumgebung betrieben.
- PostgreSQL-Audit-Logs protokollieren relevante Datenbankvorgänge im Rahmen der technischen Möglichkeiten.
- Exportdateien können über Hashwerte im Exportprotokoll auf Integrität geprüft werden.
- Sicherheitsupdates für Ubuntu 24.04 und die Quarkus-Anwendung werden manuell geprüft und eingespielt.
- Abhängigkeiten werden durch IntelliJ- und Mend.io-gestützte Schwachstellenprüfungen im Entwicklungsprozess kontrolliert.

5. Verfügbarkeit und Belastbarkeit

- Hetzner Cloud Server, Firewalls, Backups und Snapshots werden für den Betrieb eingesetzt.
- Tägliche Backups mit bis zu sieben Sicherungsständen werden vorgehalten.
- Administrative Snapshots können Rollbacks ermöglichen und werden spätestens mit dem nächsten Deployment beziehungsweise der nächsten veröffentlichten Version gelöscht.
- Manuelle Wiederherstellungstests werden durchgeführt.
- Der Dienst ist über TLS-gesicherte Endpunkte erreichbar; Wartungs-, Sicherheits- und Kapazitätsmaßnahmen können vorübergehende Einschränkungen erfordern.

6. Wiederherstellbarkeit

- Backups ermöglichen eine Wiederherstellung nach technischen Störungen oder Sicherheitsvorfällen.
- Backups sind ausschließlich für Notfall- und Wiederherstellungszwecke bestimmt.
- Bei Wiederherstellung aus Backups werden bereits abgelaufene Löschpflichten erneut berücksichtigt und betroffene Daten unverzüglich gelöscht.
- Manuelle Wiederherstellungstests dienen der Überprüfung der Wiederherstellungsfähigkeit.

7. Verfahren zur regelmäßigen Überprüfung

- Regelmäßige Überprüfung von Unterauftragnehmern ist vorgesehen.
- Technische Abhängigkeiten werden auf bekannte Schwachstellen geprüft.
- Das Löschkonzept wird dokumentiert und weiterentwickelt.
- Berechtigungen, Rollen, RLS-Regeln und Request-Filter werden im Rahmen der Entwicklung und Tests geprüft.
- Änderungen an sicherheitsrelevanten Komponenten werden vor produktivem Einsatz geprüft.

8. Datensparsamkeit, Löschung und Zweckbindung

- Mandantendaten werden nur für Bereitstellung, Support, Wartung, Export, Sicherheit und Löschung der Anwendung verarbeitet.
- Produktive Mandantendaten werden nach Vertragsende entsprechend der 90-tägigen Exportfrist gelöscht; Testmandanten nach 30 Tagen Exportfrist.
- Gelöschte Daten können in rotierenden Backups höchstens sieben Tage enthalten sein.
- Exportprotokolle und Löschbestätigungen werden zwei Jahre gespeichert.
- Produktive Mandantendaten werden nicht für Werbung, Profilbildung oder Verkauf an Dritte genutzt.

9. Auftragskontrolle

- Verarbeitungen erfolgen nach Hauptvertrag, AVV, dokumentierten Weisungen und Nutzung der Funktionen durch den Auftraggeber.
- Unterauftragnehmer werden nur gemäß Anlage 2 beziehungsweise nach dem vereinbarten Änderungsverfahren eingesetzt.
- Supportzugriffe erfolgen anlassbezogen und nur soweit erforderlich.
- Fernsupport per TeamViewer erfolgt nur nach vorheriger Abstimmung und ausdrücklicher Freigabe durch den Benutzer; Sitzungen werden durch den Auftragnehmer nicht aufgezeichnet.

10. Entwicklungs- und Testumgebung

- Der Auftragnehmer testet derzeit lokal.
- Produktive Mandantendaten werden nicht planmäßig in lokale Testumgebungen, GitHub, IntelliJ/JetBrains oder Mend.io übertragen.
- Code- und Abhängigkeitsprüfungen erfolgen ohne planmäßige Übermittlung produktiver Kundendaten.
- Sofern technische Ausschnitte zur Fehleranalyse erforderlich werden, werden diese soweit möglich anonymisiert oder pseudonymisiert und auf das erforderliche Minimum beschränkt.

11. Hinweise zum aktuellen technischen Stand

Eine zusätzliche anwendungsseitige Verschlüsselung sämtlicher ruhender Inhaltsdaten ist derzeit nicht umgesetzt. Der Schutz erfolgt insbesondere durch Server- und Netzwerksicherheit, Zugriffsbeschränkungen, Mandantentrennung, TLS-Transportverschlüsselung und Backups. Eine vollständige Zwei-Faktor-Authentifizierung für Kundenkonten ist derzeit nicht verfügbar; die Registrierung wird per E-Mail bestätigt.