Vereinbarung zur Auftragsverarbeitung für Zero2Five

Stand: 18. Oktober 2026

Diese Vereinbarung regelt die Verarbeitung personenbezogener Daten, die openbrain im Rahmen von Zero2Five tatsächlich im Auftrag des Auftraggebers durchführt. Sie umfasst den Vertragstext und die Anlagen 1 bis 3. Die individuellen Angaben zum Auftraggeber und zum Abschluss werden im zugehörigen Abschlussdatensatz festgehalten.

1 Parteien und Abschluss

1.1 Auftragnehmer ist die openbrain GmbH, Puchgasse 1 / Top 1A, 1220 Wien, Österreich, Firmenbuchnummer FN 484872 y, im Folgenden „openbrain“. Kontakt für Datenschutz, Weisungen und Vorfälle: agentur@openbrain.at.

1.2 Auftraggeber ist das im Abschlussdatensatz bezeichnete Unternehmen mit vollständigem Firmennamen einschließlich Rechtsform und Geschäftsanschrift. Erfasst werden außerdem Name, Funktion und bestätigte Kontakt-E-Mail der handelnden Person, die Konto- oder Firmen-ID sowie Vertragsfassung, Abschlusszeitpunkt und Vorgangskennung.

1.3 openbrain bietet die bereitgestellte vollständige Vertragsfassung einschließlich Anlagen verbindlich zum Abschluss an. Die vertretungsbefugte Person des Auftraggebers nimmt dieses Angebot durch eine gesonderte, ausdrückliche und nicht vorausgewählte elektronische Bestätigung an. Der Auftraggeber erhält den Abschlussnachweis mit dem bestätigten Vertragstext und den Anlagen zum Herunterladen und Speichern. Alternativ ist eine beiderseitige Unterzeichnung möglich. Eine Papier-Rücksendung ist beim elektronischen Abschluss nicht erforderlich.

1.4 Eine bloße Veröffentlichung dieser Vereinbarung, die Kenntnisnahme von Datenschutzhinweisen oder eine Zahlung ersetzen den AVV-Abschluss nicht. Der Rahmenvertrag wird vor der ersten von ihm erfassten Verarbeitung geschlossen. Die Erklärung wird getrennt von der erfolgreichen Bezahlung eines Pakets dokumentiert; ein fehlgeschlagener Kauf erteilt keine zusätzliche Verarbeitungsberechtigung.

1.5 Die Vereinbarung ergänzt die jeweilige Leistungsvereinbarung, insbesondere Kaufbedingungen oder Partnervereinbarung. Sie kann weitere Domains und Aufträge derselben Vertragsfirma abdecken, soweit Parteien, genehmigter Verarbeitungsumfang und Bedingungen unverändert passen. Andere juristische Personen sind nur bei eigenem Abschluss oder ausdrücklicher wirksamer Einbeziehung erfasst.

2 Rollen und Anwendungsbereich

2.1 Maßgeblich sind die tatsächlichen Zwecke, Entscheidungsbefugnisse und Weisungsverhältnisse. Die Kontobezeichnung „Kunde“, „Agentur“ oder „Partner“ bestimmt die datenschutzrechtliche Rolle nicht allein.

2.2 Ist der Auftraggeber Verantwortlicher, verarbeitet openbrain die erfassten personenbezogenen Daten als dessen Auftragsverarbeiter. Handelt der Auftraggeber selbst als Auftragsverarbeiter seines Kunden, wird openbrain als weiterer Auftragsverarbeiter eingesetzt; die Vereinbarung gilt entsprechend innerhalb dieser Verarbeitungskette.

2.3 Der Auftraggeber ordnet die Rolle je Auftrag oder Projekt zu. Handelt er für einen Verantwortlichen, stellt er vor Beginn sicher, dass dessen Auftrag, rechtmäßige Weisungen und erforderliche Genehmigungen die Einschaltung von openbrain und der genehmigten weiteren Auftragsverarbeiter abdecken. Er dokumentiert diese Grundlage und legt auf begründete Anforderung geeignete Nachweise vor. Ein direkter Vertrag zwischen openbrain und jedem Endkunden ist nicht allein wegen dieser Unterbeauftragung erforderlich.

2.4 Die Vereinbarung gilt nicht für Verarbeitungen zu eigenen Zwecken einer Partei, insbesondere deren eigene Vertrags-, Rechnungs- und Nutzerkontenverwaltung oder eigenständig bestimmte Missbrauchsabwehr. Hierfür gelten die jeweiligen eigenen Pflichten und Datenschutzhinweise. Bei tatsächlich gemeinsamer Festlegung von Zwecken und Mitteln ist gegebenenfalls eine gesonderte Regelung nach Art. 26 DSGVO erforderlich.

2.5 Die gezielte Verarbeitung besonderer Datenkategorien nach Art. 9 DSGVO, von Daten nach Art. 10 DSGVO, privater Zugangsdaten, nicht öffentlicher Kundenbestände sowie von Gesundheits- und Personalakten ist nicht Gegenstand des Standardauftrags. Öffentliche Zugänglichkeit schließt solche Daten nicht aus. Werden entsprechende Risikoinhalte erkannt, wird die betroffene Verarbeitung ausgesetzt und mit dem Auftraggeber abgestimmt.

3 Gegenstand und Grenzen der Verarbeitung

3.1 Gegenstand ist die beauftragte Analyse einer begrenzten Stichprobe öffentlich erreichbarer Webseiten ausgewählter Domains mit Zero2Five. Zweck, Tätigkeiten, Datenarten, betroffene Personen und Speicherphase ergeben sich aus Anlage 1 und den zulässigen Einzelaufträgen.

3.2 Die Verarbeitung beginnt nach wirksamem Abschluss und Vorliegen der erforderlichen Berechtigungen. Die Vereinbarung erfasst auch die vereinbarte Speicherung für die historische Berichtsansicht und Ergebnisvergleiche sowie die anschließende Rückgabe oder Löschung.

3.3 openbrain verwendet Auftragsdaten nicht für eigene Werbung, eigenes Modelltraining, fremde Analyseaufträge oder einen allgemein geteilten Ergebniscache. Eine konto- oder firmenübergreifende Wiederverwendung für andere Auftraggeber ist ausgeschlossen. Eine Veröffentlichung von Kundenfällen bedarf einer gesonderten Berechtigung.

4 Weisungen und Pflichten des Auftraggebers

4.1 openbrain verarbeitet Auftragsdaten nur auf dokumentierte Weisung. Anfangsweisungen ergeben sich aus dieser Vereinbarung und Anlage 1. Berechtigte spätere Analyseaufträge mit Domain, Entität und zulässigen Parametern sind Einzelweisungen innerhalb dieses Rahmens. Weitergehende Weisungen erfolgen in Textform über die benannten Ansprechpartner.

4.2 Ist openbrain aufgrund von Unionsrecht oder mitgliedstaatlichem Recht zu einer darüber hinausgehenden Verarbeitung verpflichtet, informiert openbrain den Auftraggeber vorher, soweit dies nicht gesetzlich untersagt ist.

4.3 Hält openbrain eine Weisung für datenschutzrechtswidrig, wird der Auftraggeber unverzüglich informiert. Die betroffene Weisung wird bis zur Klärung ausgesetzt. Bei ungeklärter Berechtigung oder erkennbar sensiblen Daten kann openbrain betroffene Aufträge zurückweisen.

4.4 Der Auftraggeber sorgt im Rahmen seiner Rolle für zulässige Zwecke, Rechtsgrundlagen, erforderliche Informationen an betroffene Personen und die Befugnis zur beauftragten Analyse. Er begrenzt Eingaben auf das Erforderliche, hält seine Ansprechpartner aktuell und meldet ausgeschiedene Berechtigte unverzüglich. Die Verantwortung für rechtmäßige Weitergabe heruntergeladener Berichte liegt bei ihm.

5 Vertraulichkeit und Sicherheit

5.1 openbrain stellt sicher, dass mit Auftragsdaten befasste Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Der Zugriff erfolgt nur entsprechend den erforderlichen Aufgaben und Berechtigungen. Die Vertraulichkeit gilt nach Ende der Tätigkeit fort.

5.2 openbrain verpflichtet sich zu den risikogerechten Maßnahmen nach Art. 32 DSGVO und Anlage 2. Die Maßnahmen werden für die erfasste Verarbeitung eingerichtet und während ihrer Dauer aufrechterhalten. Die Vereinbarung enthält keine Zusicherung einer Zertifizierung, eines externen Sicherheitsaudits oder einer vollständigen Erkennung sensibler Inhalte.

5.3 Maßnahmen können technisch weiterentwickelt werden, sofern das vereinbarte Schutzniveau nicht sinkt. Wesentliche Änderungen werden dokumentiert und erforderlichenfalls mit dem Auftraggeber abgestimmt.

6 Weitere Auftragsverarbeiter und Übermittlungen

6.1 Der Auftraggeber genehmigt allgemein den Einsatz der in Anlage 3 bezeichneten weiteren Auftragsverarbeiter, soweit sie für den jeweiligen Auftrag tatsächlich benötigt werden und ihre Einbindung in der Verarbeitungskette gedeckt ist. openbrain verpflichtet sie durch verbindliche Vereinbarungen auf die für ihre Tätigkeit einschlägigen Datenschutzpflichten und prüft hinreichende Garantien. Die Verantwortung von openbrain nach Art. 28 Abs. 4 DSGVO bleibt bestehen.

6.2 Über beabsichtigte Hinzunahmen oder Ersetzungen informiert openbrain den Auftraggeber aktiv mindestens 30 Kalendertage vor dem Einsatz. Die Information nennt Anbieter, Tätigkeit, Datenumfang, relevante Verarbeitungsorte und Drittlandgarantien. Wesentliche Änderungen des genehmigten Einsatzes werden entsprechend behandelt. Eine stille Änderung einer Website genügt nicht.

6.3 Der Auftraggeber kann innerhalb dieser Frist aus nachvollziehbaren Datenschutzgründen widersprechen. Die Parteien suchen eine rechtskonforme Alternative. Ist diese nicht verfügbar, wird die betroffene Verarbeitung mit dem neuen Anbieter nicht begonnen oder eingestellt. Der betroffene Leistungsteil kann entsprechend beendet werden; zwingende Rechte bleiben unberührt. Erforderlichenfalls wird ein Einsatz ausgesetzt, bis das Informations- und Widerspruchsverfahren eingehalten werden kann.

6.4 Übermittlungen oder Zugriffe außerhalb des EWR erfolgen nur im dokumentierten Weisungsrahmen und unter Einhaltung von Kapitel V DSGVO. Soweit erforderlich, werden geeignete Garantien, ergänzende Maßnahmen und eine Bewertung der Transferumstände vorgesehen. Diese AVV ist selbst kein Transferinstrument. Eine ausschließliche Verarbeitung in Österreich oder der EU wird nicht zugesichert.

6.5 Ein KI-Ausweichanbieter darf nur im genehmigten Umfang verwendet werden. Eine technische Ausweichfunktion begründet keine Genehmigung eines zusätzlichen Anbieters. Fehlt eine zulässige Alternative, unterbleibt die betroffene KI-Auswertung. Auftragsdaten dürfen nicht für ein vom Auftraggeber nicht gedecktes Modelltraining freigegeben werden.

7 Betroffenenrechte und Unterstützung

7.1 Erhält openbrain ein Ersuchen zu Auftragsdaten, wird es unverzüglich an den benannten Ansprechpartner weitergeleitet und nicht eigenständig beantwortet, sofern keine rechtliche Verpflichtung oder Weisung besteht. Eigene Verantwortlichkeitsbereiche bleiben davon unberührt.

7.2 openbrain unterstützt unter Berücksichtigung von Verarbeitungsart und verfügbaren Informationen bei Auskunft, Berichtigung, Einschränkung, Herausgabe und Löschung sowie bei Sicherheitsmaßnahmen, Datenschutz-Folgenabschätzungen und erforderlichen vorherigen Konsultationen. Die Unterstützung erfolgt ohne vermeidbare Verzögerung unter Berücksichtigung der gesetzlichen Fristen des Verantwortlichen.

7.3 Der Auftraggeber benennt eine erreichbare Stelle für Weisungen und Vorfälle. Ohne gesonderte Benennung ist dies die bestätigte Kontaktadresse der handelnden Person im Abschlussdatensatz. Änderungen werden unverzüglich mitgeteilt. Bei Unterbeauftragung sorgt der Auftraggeber für die rechtzeitige Weiterleitung entlang der Verarbeitungskette.

7.4 Gesetzlich geschuldete Mitwirkung wird nicht von Gebühren oder Vorauszahlungen abhängig gemacht. Darüber hinausgehende, nicht bereits vergütete Sonderleistungen können gesondert vereinbart werden.

8 Datenschutzverletzungen

8.1 openbrain informiert den Auftraggeber unverzüglich nach Bekanntwerden einer Verletzung des Schutzes der Auftragsdaten, spätestens binnen 48 Stunden, an die benannte Kontaktstelle per E-Mail. Unvollständige Erstinformationen werden ohne vermeidbare Verzögerung ergänzt.

8.2 Mitgeteilt werden, soweit verfügbar: Art und Zeitraum des Vorfalls, betroffene Daten und Personengruppen, ungefähre Mengen, Ansprechpartner, voraussichtliche Folgen sowie getroffene oder vorgeschlagene Maßnahmen. openbrain unterstützt Sicherung, Aufklärung, Abhilfe und erforderliche Meldungen.

8.3 Die gesetzliche Meldefrist des Verantwortlichen ist keine Wartefrist für openbrain. Eine Meldung im Namen des Auftraggebers erfolgt nur bei entsprechender Beauftragung. Im Fall einer Unterbeauftragung ist die rechtzeitige Weiterleitung an den Verantwortlichen sicherzustellen.

9 Nachweise und Kontrollen

9.1 openbrain stellt die für den Nachweis der Pflichterfüllung erforderlichen Informationen bereit und ermöglicht Überprüfungen einschließlich Inspektionen durch den Auftraggeber oder einen von ihm beauftragten unabhängigen Prüfer und trägt dazu bei.

9.2 Kontrollen werden mit angemessener Vorankündigung unter Schutz anderer Kunden, Geschäftsgeheimnisse und der Systemsicherheit koordiniert. Erforderliche dringende Prüfungen und behördliche Befugnisse bleiben unberührt. Dokumente, Fragebögen und vorhandene Prüfberichte können vorrangig genutzt werden, ohne erforderliche weitere Kontrollen auszuschließen.

9.3 Handelt der Auftraggeber als Auftragsverarbeiter, erhält er unter angemessener Vertraulichkeit auch die Nachweise, die er seinem Verantwortlichen gegenüber benötigt.

10 Laufzeit sowie Rückgabe und Löschung

10.1 Die Vereinbarung gilt ab Abschluss, solange openbrain personenbezogene Auftragsdaten für den Auftraggeber verarbeitet oder speichert. Sie kann mit einer Frist von 30 Tagen in Textform gekündigt werden; das Recht zur Kündigung aus wichtigem Grund bleibt unberührt. Nach Beendigung der Leistung gelten die notwendigen Schutz-, Rückgabe- und Löschpflichten fort.

10.2 Nach Ende der Verarbeitungsleistungen werden die vorhandenen personenbezogenen Auftragsdaten nach dokumentierter Wahl des Verantwortlichen zurückgegeben oder gelöscht. Bei Unterbeauftragung wird dessen Wahl über den Auftraggeber weitergegeben. Eine Rückgabe wird nicht pauschal auf freigeschaltete PDF-Berichte beschränkt. Nach der Rückgabe werden verbleibende Kopien gelöscht, soweit keine gesetzliche Pflicht zur Speicherung besteht. Vor Ablauf einer vorgesehenen Bereinigung erhält der Auftraggeber Gelegenheit, seine Wahl mitzuteilen; zulässige frühere Löschweisungen bleiben vorrangig.

10.3 Der PDF-Download ist eine zusätzliche Selbstbedienungsfunktion. Soweit er für die vollständige Rückgabe nicht genügt oder nicht angeboten wird, erfolgt die Anfrage an agentur@openbrain.at. Nach Identitäts- und Berechtigungsprüfung stellt openbrain die noch vorhandenen, dem Auftrag zuordenbaren Auftragsdaten auf geeignetem geschütztem Weg in einem vereinbarten gängigen Format bereit. Zugangsschlüssel, fremde Daten und der Programmcode sind nicht Teil dieser Rückgabe. Bereits ordnungsgemäß gelöschte oder nicht gespeicherte Rohdaten müssen nicht rekonstruiert werden. Ein automatisches Exportportal wird nicht zugesagt.

10.4 Operative Sicherungsarchive werden regulär nach 30 Tagen bereinigt. Dienstseitige Wiederherstellungs- und Löschprozesse können darüber hinausreichen; für Dropbox Advanced gilt die in Anlage 3 beschriebene zusätzliche Wiederherstellbarkeit. Solche Kopien werden ausschließlich geschützt zu Sicherungszwecken vorgehalten und nicht für laufende Analysen genutzt. Erforderliche Maßnahmen zur früheren endgültigen Löschung werden auf berechtigte Weisung im Rahmen der verfügbaren Anbieterfunktionen veranlasst. Bei Wiederherstellung werden bereits erfolgte Löschungen erneut umgesetzt, bevor betroffene Daten produktiv genutzt werden.

10.5 Rückgabe, Löschung, noch ausstehende Sicherungsbereinigungen und gesetzliche Ausnahmen werden nachvollziehbar dokumentiert. Eine fortdauernde Speicherung zur Erfüllung gesetzlicher Pflichten wird auf

erforderliche Daten begrenzt und hinsichtlich Rechtsgrundlage, Zugriff und Ende festgehalten. Eigene Rechnungs- und Vertragsnachweise rechtfertigen keine pauschale Aufbewahrung von Analyseinhalten.

10.6 Vom Auftraggeber selbst heruntergeladene Berichte und Daten in seinen Systemen bleiben in seiner Verantwortung. Eine Kontolöschung ruft diese Kopien nicht zurück.

11 Vorrang sowie Änderungen und Recht

11.1 Bei Widersprüchen zu kaufmännischen Bedingungen geht diese Vereinbarung für die Auftragsverarbeitung vor. Haftungsregeln des Hauptvertrags beschränken keine zwingenden gesetzlichen Verantwortlichkeiten, behördlichen Befugnisse oder Rechte betroffener Personen.

11.2 Änderungen der Vereinbarung oder ihrer Anlagen werden in Textform vereinbart. Eine neue Webfassung oder ein weiterer Kauf ändert einen bestehenden Rahmenvertrag nicht automatisch. Das gesonderte Verfahren für weitere Auftragsverarbeiter nach Punkt 6 bleibt anwendbar.

11.3 Die Vereinbarung wird bei wesentlichen Änderungen von Leistung, Datenflüssen, Risiken oder Rechtslage überprüft. Bestätigte Fassungen bleiben nachvollziehbar.

11.4 Es gilt österreichisches Recht unter Ausschluss seiner Verweisungsnormen. Für Streitigkeiten zwischen Unternehmern ist, soweit zulässig und sachlich zuständig, das Handelsgericht Wien vereinbart. Zwingende Zuständigkeiten und Rechte betroffener Personen bleiben unberührt.

Anlage 1 Auftragsbeschreibung

1.1 Zweck ist die Einschätzung der technischen, strukturellen, semantischen und inhaltlichen Voraussetzungen einer Website für Such- und KI-Systeme anhand des Zero2Five-Modells einschließlich Quellenbelegen und priorisierter Maßnahmen. Die Analyse einer Stichprobe ist keine vollständige Domainprüfung, Zertifizierung oder Messung tatsächlicher Sichtbarkeit in KI-Antworten.

1.2 Tätigkeiten sind der Abruf öffentlich erreichbarer Seiten, Extraktion und erforderliche technische Aufbereitung, KI-gestützte Auswertung, Bewertung, Speicherung und berechtigte Anzeige der Auftrags- und Ergebnisdaten, gegebenenfalls PDF-Erzeugung auf Abruf, Support, Sicherung sowie Rückgabe und Löschung. Der konkrete Umfang ergibt sich aus den Einzelaufträgen und der ausgewiesenen Analysebasis. PDF-Downloads sind nur in den dafür vorgesehenen berechtigten Bereichen verfügbar; das Beratertool bietet keinen PDF-Export.

1.3 Betroffene Personen sind berufliche Ansprechpartner, Beschäftigte, Verantwortliche, Autoren und Fachpersonen sowie sonstige im öffentlichen Websiteinhalt genannte natürliche Personen, soweit ihre Angaben für den Prüfzweck erforderlich sind.

1.4 Datenarten sind Domain und URLs, Unternehmens- und Markenbezeichnungen, öffentlich sichtbare Textausschnitte, Überschriften, Metadaten, strukturierte Angaben, Namen und berufliche Rollen, vorhandene Kontaktdaten, Verknüpfungen, Belegstellen, Analysekennungen, Parameter, Ergebnisse und Zeitpunkte. Nicht vorgesehen sind die in Punkt 2.5 ausgeschlossenen Inhalte.

1.5 Kunden- und Agenturkonten erhalten Zugriff nur auf konkret berechtigte Berichte. Aktive Mitglieder einer Partnerfirma können die Analysen ihrer Firma sehen; dadurch entsteht kein Zugriff auf andere Firmen oder Kundenkäufe. Interne Rollen besitzen für erforderlichen Betrieb, Support, Sicherheit und berechtigte Freischaltungen weitergehende Rechte, deren Nutzung auf den jeweiligen Zweck zu begrenzen ist.

1.6 Handelt der Auftraggeber für Kunden, dokumentiert er je Auftrag den Verantwortlichen, Projekt oder Domain, seine Beauftragung, die erforderliche Genehmigungskette, Weisungsumfang und Gültigkeit. Diese Auftragsübersicht kann außerhalb der Plattform geführt werden und wird auf begründete Anforderung vorgelegt.

1.7 Freigeschaltete Berichte bleiben nach Paketende für die historische Ansicht und Ergebnisvergleiche verfügbar, solange das Konto aktiv ist und eine zulässige Speicherweisung besteht. Bei Kunden- und Agenturkonten wird nach drei Jahren ohne nachvollziehbare Nutzung eine Bereinigung eingeleitet. Ausgangspunkt ist der spätere Zeitpunkt aus letzter Nutzung beziehungsweise erfolgreicher Anmeldung und Ende des letzten Pakets. Aktive Pakete und laufende Analysen werden ausgenommen.

1.8 Vor der automatischen Bereinigung wird eine Erinnerung an die Konto-E-Mail-Adresse versandt. Nach erfolgreicher Übergabe an den E-Mail-Dienst werden weitere 30 Tage eingeräumt. Eine erfolgreiche Anmeldung oder erneute Nutzung startet die Drei-Jahres-Frist neu; das bloße Anfordern eines Zugangslinks genügt nicht. Fehlgeschlagener oder unklarer Versand und erkennbare Rückläufer werden manuell geprüft. Daraus folgt keine Berechtigung zu unbegrenzter Speicherung.

1.9 Eine konkrete frühere Lösch- oder Beendigungsweisung bleibt wirksam und wird durch andere Kontonutzung nicht aufgehoben. Bei Agenturen darf eine aktive Beziehung die Beendigung eines einzelnen Kundenauftrags nicht übergehen. Partnerfirmen und ihre gemeinsam benötigten Analysen werden hinsichtlich Vertragsende und Bereinigung gesondert behandelt. Eine unbegrenzte Online-Speicherung wird nicht zugesagt.

Anlage 2 Technische und organisatorische Maßnahmen

openbrain verpflichtet sich für die erfasste Verarbeitung zu den folgenden Maßnahmen. Physische Infrastruktur und Rechenzentrumsbetrieb werden durch den Hostinganbieter erbracht; anwendungsbezogene Berechtigungen und Abläufe liegen im Verantwortungsbereich von openbrain.

Bereich	Maßnahmen
Transport	HTTPS für die Anwendung; geschützter Mailtransport entsprechend der eingesetzten SMTP-Konfiguration.
Authentifizierung	Kunden und Agenturen: zeitlich begrenzte Magic Links mit ausdrücklicher Bestätigung und befristete Sitzungen. Partner und interne Nutzer: individuelle Konten; Partnerpasswörter mindestens acht Zeichen.
Passwörter	Gesalzene PBKDF2-SHA256-Hashes; keine Klartextspeicherung von Nutzerpasswörtern.
Zugriffsrechte	Serverseitige Prüfung von Rolle, Firma und konkreter Analyse. Keine Zugriffsrechte allein durch Branding oder Domainkenntnis; keine automatische Firmenzuordnung nach E-Mail-Domain.
Trennung der Auftragsdaten	Private Kunden-, Agentur- und Paketanalysen werden nicht als allgemeiner Ergebniscache für andere Nutzer wiederverwendet. Eigentümer- und Firmenprüfung auch bei direkten Job- und Ergebnislinks.
Berichte	Download nur mit konkreter Berechtigung; PDF-Erzeugung im Arbeitsspeicher ohne zusätzliche serverseitige PDF-Kopie. Berichtsbenachrichtigungen mit geschütztem Link und erforderlicher Anmeldung, ohne PDF-Anhang oder Öffnungstracker.
Formulare	CSRF-Prüfungen und rollenabhängige Sperren bei geschützten Aktionen; Behandlung wiederholter Übermittlungen.
Missbrauchsschutz	Anfrage-, Job- und Parallelitätslimits sowie konten- oder firmenbezogene Nutzungsgrenzen. Für Teile der Begrenzung gekürzte IP-Hashes; diese gelten nicht pauschal als anonym.
Protokollierung	Erforderliche Analyse-, Kauf-, Job-, Freischalt- und Versanddaten einschließlich Zeitpunkten und Entscheidungen. Kein zugesagtes vollständiges Audit jedes internen Lesezugriffs.
Sicherung	Tägliche lokale Sicherung in privatem Verzeichnis; rclone-Crypt-Verschlüsselung von Inhalt und Dateinamen vor Dropbox-Upload; Rückprüfung gegen das lokale Archiv. Operativer Aufbewahrungszyklus 30 Tage.
Überwachung und Wiederherstellung	Fehlerbenachrichtigung des Backupjobs; Wiederherstellung in einen gesonderten Ordner und Rückholprüfung der externen Kopie. Bereits erfolgte Löschungen vor erneuter produktiver Nutzung beachten.
Löschung und Rückgabe	Berechtigungsprüfung und kontrollierter manueller Ablauf für Rückgabe und Löschbegehren. Kontobereinigung mit Vorschau beziehungsweise erneuter Fristprüfung; getrennte Behandlung notwendiger Zahlungsnachweise.

Bereich	Maßnahmen
Vertragsnachweis	Ausdrückliche elektronische Bestätigung mit Firmen- und Vertreterangaben, Zeitpunkt, Fassung und vollständiger Textkopie. Geschützter Nachweiszugriff; eine Prüfsumme ersetzt keine qualifizierte Signatur oder Vollmachtsprüfung.
Staging und Pflege	Getrennte Testumgebung mit eigener Konfiguration und Daten, Zugangsschutz, Suchmaschinen-Sperre, eingeschränktem Mailversand und Testzahlungen; versionierte Updates und automatisierte Tests.
Organisation	Vertraulichkeitsverpflichtungen, aufgabenbezogene Berechtigungen, Entzug ausgeschiedener Zugänge, sichere Schlüsselverwahrung sowie Verfahren für Weisungen, Vorfälle und Betroffenenanfragen.

Nicht zugesichert werden eine Zwei-Faktor-Anmeldung, ein externes Sicherheitsaudit, ein automatischer Gesamtexport, eine automatische Löschung ganzer Firmenbereiche oder eine umfassende Erkennung sensibler Inhalte vor der KI-Übermittlung. Das Backupskript verschlüsselt lokale Sicherungsarchive nicht zusätzlich. Eine Verschlüsselung des Hostingspeichers wird nicht pauschal zugesagt. Das vereinbarte Schutzniveau wird bei technischen Änderungen aufrechterhalten.

Anlage 3 Weitere Auftragsverarbeiter

Die folgende Liste bezeichnet die für den jeweiligen Dienst genehmigten Anbieter. Die Einschaltung beschränkt sich auf den tatsächlich beauftragten und benötigten Umfang. openbrain stellt auf berechtigte Anforderung Informationen zu den für den konkreten Einsatz maßgeblichen Verarbeitungsorten, weiteren Unterbeauftragten und Transfergarantien bereit. Die Genehmigung ersetzt nicht die Einhaltung der Pflichten nach Punkt 6.

3.1 Mittwald Hosting

Mittwald CM Service GmbH & Co. KG, Königsberger Straße 4–6, 32339 Espelkamp, Deutschland. Tätigkeit: Betrieb der Anwendung, Datenbanken, erforderlichen Uploads, Analyseergebnisse, lokalen Sicherungen und technischen Protokolle. Der vorgelegte Hosting-AVV mit Anlagen vom 13.12.2019 sieht die vereinbarte Leistungserbringung in EU/EWR vor; eine Drittlandverlagerung bedarf der dort geregelten vorherigen Zustimmung und rechtlichen Voraussetzungen. Die Speicherung der Anwendungsdaten richtet sich nach Anlage 1 und Punkt 10; technische Hostingprotokolle unterliegen ihren dienstbezogenen Fristen. Physische Schutzmaßnahmen ergeben sich aus den Hosting-TOM.

3.2 OpenAI API

OpenAI Ireland Ltd. für den direkten API-Vertrag des im EWR ansässigen Auftragnehmers. Das API-Geschäftskonto wird auf openbrain GmbH geführt. Tätigkeit: KI-gestützte Auswertung erforderlicher ausgewählter Websiteinhalte, Entitäts- und Prüfparameter sowie Erzeugung der Auswertung. Maßgeblich sind der API-Vertrag und das einbezogene DPA. Eine Verarbeitung beziehungsweise Weiterübermittlung außerhalb des EWR, insbesondere in die USA, kann stattfinden; hierfür gelten die erforderlichen Garantien nach Punkt 6.4. API-Inhalte werden im Standardbetrieb nicht zum Modelltraining verwendet. Speicher- und Missbrauchsprotokollfristen hängen vom Dienst und den Optionen ab; standardmäßige Missbrauchslogs können grundsätzlich bis zu 30 Tage und in rechtlich oder sicherheitsbedingt begründeten Ausnahmefällen länger bestehen. Zero Data Retention wird nicht pauschal zugesagt.

3.3 Anthropic API

Anthropic Ireland, Limited für den direkten API-Vertrag mit openbrain GmbH. Tätigkeit: entsprechende KI-Auswertung erforderlicher Analyseinhalte, auch als genehmigte Alternative zum Primäranbieter. Maßgeblich sind die Commercial Terms und das einbezogene DPA einschließlich einschlägiger Transferregelungen. Ein ausschließlicher EU-Verarbeitungsort wird nicht zugesichert; Drittlandverarbeitungen unterliegen Punkt 6.4. Die Commercial Terms schließen Modelltraining mit den dort erfassten Kundeninhalten aus. Für API-Ein- und Ausgaben gilt grundsätzlich die veröffentlichte 30-Tage-Löschung, vorbehaltlich dienstbezogener, vertraglicher, sicherheitsbedingter oder gesetzlicher Ausnahmen. Eine besondere Vereinbarung zur sofortigen Löschung wird nicht zugesagt.

3.4 Magenta Mailversand

T-Mobile Austria GmbH, Rennweg 97–99, 1030 Wien, Österreich. Genutztes Produkt: „Domaingebühr“ mit enthaltenem Maildienst. Tätigkeit: Versand der erforderlichen Anmelde-, System-, Erinnerungs- und Berichtsbenachrichtigungen über mail.mymagenta.business mit der Absenderkennung service@gefunden-werden.at. Verarbeitet werden erforderliche Empfängeradressen, Nachrichtentexte, Links und gegebenenfalls Domain-, Entitäts- und Berichtsangaben. Der reguläre Benachrichtigungsablauf versendet keine PDF-Berichtsanhänge. Notwendige Transport- und Zustellprotokolle sind von den in der Anwendung gespeicherten

Analysen zu unterscheiden. Eine ausschließliche Speicherung oder Verarbeitung aller Maildaten in Österreich wird nicht zugesichert.

3.5 Dropbox Business Advanced

Dropbox International Unlimited Company für das Business-Team des im EWR ansässigen Auftragnehmers. Genutzter Tarif: Dropbox Business Advanced. Tätigkeit: externe Ablage der vor Upload mit rclone Crypt verschlüsselten Sicherungen; technische Konto- und Übertragungsmetadaten sind davon gesondert zu betrachten. Maßgeblich sind der Business-Vertrag und das zugehörige DPA. Drittlandverarbeitung beziehungsweise Zugriffe, insbesondere unter Einbindung von Dropbox, Inc. in den USA, unterliegen Punkt 6.4. Die Verschlüsselung ersetzt die Prüfung der vertraglichen und rechtlichen Voraussetzungen nicht.

Aktive Backuparchive werden im regulären eigenen Sicherungszyklus nach 30 Tagen entfernt. Für Dropbox Advanced besteht standardmäßig eine zusätzliche Wiederherstellbarkeit gelöschter Dateien von bis zu 365 Tagen nach deren gewöhnlicher Löschung. Die Einleitung einer endgültigen Löschung kann die Wiederherstellbarkeit früher beenden; die technische Beseitigung kann anschließend weitere Zeit benötigen. Die 30-Tage-Bereinigung ist deshalb keine Zusage, dass sämtliche dienstseitigen Kopien nach 30 Tagen endgültig beseitigt sind. Die Einschränkungen und Weisungsrechte nach Punkt 10.4 bleiben maßgeblich.

3.6 Microsoft 365 bei auftragsbezogenem Support

Soweit personenbezogene Auftragsdaten für berechtigten Support, Weisungen oder Rückgabeanfragen über das Postfach agentur@openbrain.at verarbeitet werden, wird hierfür der vorhandene Microsoft-365-Dienst unter Einbindung von Microsoft Ireland Operations Limited eingesetzt. Dieser Einsatz ist auf die erforderliche Kommunikation beschränkt; die reguläre Websiteanalyse und deren Ergebnisspeicherung erfolgen nicht in diesem Postfach. Maßgeblich sind die einschlägigen Microsoft-365-Vertrags- und Datenschutzbedingungen; erforderliche Drittlandgarantien richten sich nach Punkt 6.4. Reine eigene Vertrags- und Geschäftskorrespondenz von openbrain fällt dagegen unter Punkt 2.4. Die Weiterleitung einer E-Mail ändert diese Abgrenzung nicht.

Stripe wird nicht allein aufgrund der Zahlungsabwicklung zum weiteren Auftragsverarbeiter für analysierte Websiteinhalte. Eigene Zahlungs- und Rechnungsdaten werden nach dem jeweiligen tatsächlichen Verantwortlichkeitsverhältnis behandelt. Zusätzliche Dienste, die Auftragsdaten erhalten, werden nur unter Einhaltung des Verfahrens nach Punkt 6 einbezogen.

Elektronischer Abschlussdatensatz

Zum Abschluss werden der vollständige Firmenname einschließlich Rechtsform und Geschäftsanschrift, Name und Funktion der handelnden Person sowie ihre bestätigte Kontakt-E-Mail erfasst. Der Nachweis enthält die ausdrückliche Bestätigung der Vertretungsbefugnis, die Konto- oder Firmen-ID, Leistungs- und Vorgangsbezug, Abschlusszeitpunkt mit Zeitzone sowie die bestätigte Fassung mit Stand 18. Oktober 2026 einschließlich aller drei Anlagen. Der vollständige Text wird gemeinsam mit dem Nachweis zum Speichern bereitgestellt. Der Rollen- und Genehmigungsbezug je Einzelauftrag richtet sich nach Punkt 2 und Anlage 1.6.

Mit der gesonderten elektronischen Bestätigung erklärt die handelnde Person, dass sie für das bezeichnete Unternehmen zum Abschluss befugt ist und diese Vereinbarung einschließlich Anlagen annimmt. Soweit das Unternehmen als Auftragsverarbeiter handelt, bestätigt sie das Vorliegen der erforderlichen Weisungen und Genehmigungen für die Beauftragung von openbrain und der genehmigten weiteren Auftragsverarbeiter. Eine bloße Kenntnisnahme von Datenschutzinformationen genügt hierfür nicht.