Vereinbarung zur Auftragsverarbeitung

Diese Vereinbarung zur Auftragsverarbeitung regelt die Rechte und Pflichten des Verantwortlichen („Kunde“) und der VISUAL WORLD GmbH („Auftragsverarbeiter“) im Rahmen der Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO („Vereinbarung“).

Diese Vereinbarung dient der Umsetzung der Anforderungen der Datenschutz-Grundverordnung (DSGVO) sowie sonstiger anwendbarer Datenschutzvorschriften.

Im Falle von Widersprüchen zwischen dieser Vereinbarung und dem zugrunde liegenden Hauptvertrag gehen die Regelungen dieser Vereinbarung ausschließlich hinsichtlich datenschutzrechtlicher Anforderungen an die Auftragsverarbeitung vor. Im Übrigen bleiben die Regelungen des Hauptvertrages, insbesondere zu Leistungsumfang, Vergütung, Haftung und Kündigung, unberührt.

Sofern in dieser Vereinbarung nichts Abweichendes geregelt ist, gelten die Begriffsbestimmungen der DSGVO sowie des zugrunde liegenden Hauptvertrages.

Der Kunde stimmt den Bedingungen dieser Vereinbarung im eigenen Namen sowie im Namen verbundener Unternehmen zu, soweit diese an der Verarbeitung personenbezogener Daten im Rahmen der Nutzung der Leistungen des Auftragsverarbeiters beteiligt sind.

Rollen der Parteien und verbundene Unternehmen

- Der Auftraggeber ist Verantwortlicher im Sinne der DSGVO hinsichtlich der personenbezogenen Daten, die dem Auftragnehmer zur Verarbeitung im Auftrag überlassen werden.
- Verbundene Unternehmen des Auftraggebers können die Leistungen des Auftragnehmers ebenfalls nutzen. Der Auftraggeber und seine verbundenen Unternehmen handeln dabei jeweils als eigenständige Verantwortliche oder gemeinsam Verantwortliche im Sinne der DSGVO.
- Soweit der Auftraggeber personenbezogene Daten verbundener Unternehmen verarbeitet, handelt er diesen gegenüber als Auftragsverarbeiter. Der Auftragnehmer handelt insoweit als Unterauftragsverarbeiter des Auftraggebers.
- Die datenschutzrechtliche Verantwortlichkeit für die Rechtmäßigkeit der Verarbeitung verbleibt jeweils bei dem Verantwortlichen, der die personenbezogenen Daten erhebt oder verarbeitet.

1.Dauer

Die Dauer dieser Vereinbarung entspricht der Dauer der zwischen den Parteien bestehenden Leistungsvereinbarung bzw. des zugrunde liegenden Hauptvertrages.

Die Verpflichtungen zur Vertraulichkeit sowie gesetzliche Aufbewahrungs- und Nachweispflichten bleiben über die Beendigung dieser Vereinbarung hinaus bestehen.

2.Gegenstand der Verarbeitung, Kategorien personenbezogener Daten und betroffener Personen

2.1.Gegenstand der Verarbeitung

Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten im Rahmen der zwischen den Parteien abgeschlossenen Vereinbarung über die Bereitstellung von Software zum Zugriff über das Internet (SaaS), einschließlich damit verbundener Support-, Wartungs-, Hosting-, Administrations- und technischer Dienstleistungen des Auftragsverarbeiters.

Diese Vereinbarung findet Anwendung auf sämtliche Tätigkeiten, bei denen der Auftragsverarbeiter im Rahmen der Leistungserbringung mit personenbezogenen Daten des Verantwortlichen in Berührung kommt oder diese im Auftrag verarbeitet.

Der Umfang der konkreten Datenverarbeitung wird maßgeblich durch die Nutzung der Software und die Konfiguration durch den Verantwortlichen bestimmt und kann je nach eingesetzten Funktionen variieren.

2.1.1.Kategorien personenbezogener Daten

Folgende Datenarten bzw. Datenkategorien sind abhängig von der Nutzung der Software sowie der durch den Verantwortlichen aktivierten Funktionen regelmäßig Gegenstand der Verarbeitung:

- Personalstammdaten (Name, Vorname, Anschrift2, Geburtsdatum2, Alter2, Geschlecht2, Familienstand2, Angaben zu schulpflichtigen Kindern2)
- Nutzer- und Identifikationsdaten (Nutzername = Firmen-E-Mail-Adresse, Transponder-Identifikationsnummer1)
- Kommunikationsdaten (Telefon2, Firmen-E-Mail-Adresse)
- Bilder (Profilbild2)
- Arbeitszeit-, Planungs- und Organisationsdaten (Arbeitszeiten, Zeitstempel, Buchungsdaten, Abwesenheiten, Urlaubspläne, Schichtpläne, Team- und Abteilungszugehörigkeiten)
- Projekt- und Tätigkeitsdaten (z. B. Projekte, Projekttätigkeiten, abrechenbare Zeiten, Tätigkeitszuordnungen)
- Beschäftigungs- und Organisationsdaten (z. B. Rolle/Funktion, Mitarbeiternummer2, Einstellungsdatum, Austrittsdatum, Einsatzorte[2])
- Lokalisierungsdaten (GPS-/Geolokationsdaten[3])
- Protokoll- und Nutzungsdaten (z. B. Login-Daten, technische System- und Zugriffsinformationen)
- durch den Verantwortlichen individuell eingegebene Inhalte und Freitextdaten

Soweit durch den Verantwortlichen verarbeitet, können auch besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO betroffen sein, insbesondere gesundheitsbezogene Informationen im Zusammenhang mit Krankmeldungen oder Abwesenheiten.

[1] Optional bei Nutzung eines Terminals mit Transponderfunktion.

[2] Optional und nur soweit durch den Verantwortlichen bereitgestellt.

[3] Optional bei Nutzung mobiler Anwendungen und nur soweit die Funktion durch den Verantwortlichen aktiviert wurde. GPS-/Standortdaten können innerhalb der Anwendung deaktiviert werden.

2.1.2.Kategorien betroffener Personen

Von der Verarbeitung können insbesondere folgende Personengruppen betroffen sein:

- Beschäftigte
- ehemalige Beschäftigte
- Bewerber
- Freelancer und sonstige Beauftragte
- Ansprechpartner des Verantwortlichen
- Administratoren und berechtigte Nutzer

2.1.3.Ort der Verarbeitung und Drittlandtransfers

Die Verarbeitung personenbezogener Daten erfolgt grundsätzlich innerhalb der Europäischen Union (EU) bzw. des Europäischen Wirtschaftsraums (EWR).

Soweit personenbezogene Daten in einem Drittstaat verarbeitet oder dorthin übermittelt werden, erfolgt dies ausschließlich unter Einhaltung der Art. 44 ff. DSGVO.

Soweit der Auftragsverarbeiter oder von ihm eingesetzte Unterauftragsverarbeiter personenbezogene Daten außerhalb der EU oder des EWR verarbeiten, stellt der Auftragsverarbeiter im Rahmen seines Einflussbereichs sicher, dass die Anforderungen der Art. 44 ff. DSGVO eingehalten werden und geeignete Garantien bestehen.

Dies kann insbesondere erfolgen durch:

- Angemessenheitsbeschlüsse gemäß Art. 45 DSGVO,
- Standardvertragsklauseln der Europäischen Kommission,
- ergänzende technische und organisatorische Schutzmaßnahmen,
- sonstige gesetzlich zulässige Transfermechanismen.

3.Vertraulichkeit

Der Auftragsverarbeiter gewährleistet die Vertraulichkeit der verarbeiteten personenbezogenen Daten gemäß Art. 28 Abs. 3 lit. b, Art. 29 sowie Art. 32 Abs. 4 DSGVO.

Der Auftragsverarbeiter setzt ausschließlich Personen zur Verarbeitung personenbezogener Daten ein, die:

- auf Vertraulichkeit verpflichtet wurden,
- über die einschlägigen datenschutzrechtlichen Anforderungen informiert wurden,
- angemessene Datenschutz- und Informationssicherheitsschulungen erhalten haben.

Der Auftragsverarbeiter stellt sicher, dass sämtliche ihm unterstellten Personen sowie eingesetzte Dienstleister personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen verarbeiten, soweit keine gesetzliche Verpflichtung zur Verarbeitung besteht.

Zugriffe auf personenbezogene Daten im Rahmen von Support-, Wartungs- oder Fernzugriffstätigkeiten erfolgen ausschließlich zweckgebunden und nachvollziehbar.

Die Verpflichtung zur Vertraulichkeit besteht auch nach Beendigung der jeweiligen Tätigkeit fort.

4. Pflichten des Kunden

4.1.Der Kunde ist als Verantwortlicher für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten sowie für die Einhaltung der datenschutzrechtlichen Anforderungen bei der Nutzung der Software verantwortlich. Dies umfasst insbesondere die Prüfung der Rechtsgrundlagen, Informationspflichten gegenüber betroffenen Personen sowie etwaige arbeitsrechtliche oder mitbestimmungsrechtliche Anforderungen.

4.2.Der Kunde ist dafür verantwortlich, die Software nur im Rahmen der geltenden Datenschutzvorschriften zu nutzen und die hierfür erforderlichen Konfigurationen, Berechtigungen und Einstellungen vorzunehmen.

4.3.Der Kunde hat den Auftragsverarbeiter unverzüglich zu informieren, wenn er im Hinblick auf die Verarbeitung personenbezogener Daten Fehler, Unregelmäßigkeiten oder Verstöße gegen Datenschutzvorschriften feststellt.

4.4.Der Kunde benennt dem Auftragsverarbeiter bei Bedarf eine oder mehrere Ansprechpersonen für Datenschutzfragen und Weisungen im Rahmen dieser Vereinbarung.

4.5.Soweit der Kunde besondere Funktionen wie GPS-/Standortdaten, Freitextfelder, Krankmeldungen oder sonstige sensible Angaben nutzt, ist der Kunde für die datenschutzrechtliche Zulässigkeit dieser Nutzung verantwortlich.

5.Weisungen

5.1.Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Kunden, soweit diese Weisungen in den Anwendungsbereich der Software und der vertraglich vereinbarten Leistungen fallen.

5.2.Weisungen können insbesondere durch vertragliche Vereinbarungen, Einstellungen innerhalb der Software, dokumentierte Einzelweisungen oder sonstige Mitteilungen in Textform erfolgen.

5.3.Der Auftragsverarbeiter wird den Kunden unverzüglich darauf hinweisen, wenn eine Weisung nach seiner Auffassung gegen datenschutzrechtliche Vorschriften verstößt. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung auszusetzen, bis sie durch den Kunden bestätigt, geändert oder zurückgenommen wird.

5.4.Der Kunde benennt die weisungsbefugten Personen innerhalb der Software oder auf anderem dokumentierten Weg. Soweit keine weisungsbefugte Person benannt wurde, gelten nur Personen als weisungsbefugt, die zur gesetzlichen Vertretung des Kunden berechtigt sind oder deren Bevollmächtigung nachgewiesen wurde.

6.Pflichten des Auftragsverarbeiter

6.1.Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich im Rahmen dieser Vereinbarung, des Hauptvertrages und dokumentierter Weisungen des Kunden.

6.2.Der Auftragsverarbeiter stellt sicher, dass die Verarbeitung personenbezogener Daten im Einklang mit den Anforderungen der DSGVO erfolgt, soweit diese Anforderungen den Auftragsverarbeiter betreffen.

6.3.Der Auftragsverarbeiter benennt eine Ansprechperson für Datenschutzfragen. Soweit ein Datenschutzbeauftragter bestellt ist, werden dessen Kontaktdaten in geeigneter Weise veröffentlicht oder dem Kunden auf Anfrage mitgeteilt.

6.4.Der Auftragsverarbeiter unterstützt den Kunden im Rahmen des Zumutbaren bei der Erfüllung seiner Pflichten nach der DSGVO, insbesondere bei Betroffenenrechten, Datenschutzverletzungen, Datenschutz-Folgenabschätzungen und Anfragen von Aufsichtsbehörden.

6.5.Soweit Unterstützungsleistungen des Auftragsverarbeiters über die vertraglich vereinbarten Leistungen hinausgehen und einen zusätzlichen Aufwand verursachen, kann der Auftragsverarbeiter hierfür eine angemessene Vergütung nach den jeweils geltenden Vergütungssätzen verlangen.

Dies gilt insbesondere für außergewöhnliche Auditaufwände, individuelle Datenmigrationen, Sonderauswertungen, umfangreiche Unterstützungsleistungen im Zusammenhang mit Datenschutz-Folgenabschätzungen oder Betroffenenanfragen sowie sonstige nicht vertraglich geschuldete Zusatzleistungen.

6.6.Der Auftragsverarbeiter informiert den Kunden unverzüglich über Kontrollhandlungen, Anfragen oder Maßnahmen einer Aufsichtsbehörde, soweit diese die Verarbeitung personenbezogener Daten im Rahmen dieser Vereinbarung betreffen und keine gesetzliche oder behördliche Pflicht zur Vertraulichkeit entgegensteht.

7. Überprüfungen und Auditrechte

7.1.Der Kunde ist berechtigt, die Einhaltung der datenschutzrechtlichen Vorschriften sowie der Regelungen dieser Vereinbarung durch den Auftragsverarbeiter in angemessenem Umfang selbst oder durch beauftragte Dritte zu überprüfen.

Dies kann insbesondere erfolgen durch:

- Einholung von Auskünften,
- Einsichtnahme in relevante Dokumentationen,
- Sicherheits- und Datenschutznachweise,
- Remote-Audits,
- Vor-Ort-Prüfungen im erforderlichen Umfang.

Der Auftragsverarbeiter unterstützt den Kunden hierbei in angemessenem Umfang und stellt die zur Durchführung der Überprüfung erforderlichen Informationen zur Verfügung.

7.2.Der Kunde hat sicherzustellen, dass eingesetzte Prüfer zur Vertraulichkeit verpflichtet sind und keine unmittelbaren Wettbewerber des Auftragsverarbeiters darstellen.

Überprüfungen sind auf den zur Kontrolle der Einhaltung dieser Vereinbarung erforderlichen Umfang zu beschränken. Betriebs- und Geschäftsgeheimnisse des Auftragsverarbeiters sowie personenbezogene Daten anderer Kunden sind angemessen zu schützen.

7.3.Der Auftragsverarbeiter ist berechtigt, geeignete Nachweise zur Einhaltung der technischen und organisatorischen Maßnahmen sowie der datenschutzrechtlichen Anforderungen bereitzustellen. Hierzu zählen insbesondere:

- Zertifizierungen,
- Auditberichte,
- Sicherheitskonzepte,
- TOM-Dokumentationen,
- Nachweise unabhängiger Prüfungen.

Soweit geeignete Nachweise vorliegen, sollen diese bei der Durchführung von Überprüfungen angemessen berücksichtigt werden.

8. Technische und organisatorische Maßnahmen – Verweis

8.1.Der Auftragsverarbeiter trifft die erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 lit. c sowie Art. 32 DSGVO.

8.2.Die konkreten technischen und organisatorischen Maßnahmen ergeben sich aus Anlage 1 zu dieser Vereinbarung.

8.3.Der Auftragsverarbeiter ist berechtigt, die technischen und organisatorischen Maßnahmen unter Berücksichtigung des technischen Fortschritts weiterzuentwickeln, sofern das Schutzniveau nicht unterschritten wird.

8.4.Wesentliche Änderungen der Maßnahmen werden dokumentiert.

8.5.Der Auftragsverarbeiter überprüft die Wirksamkeit der technischen und organisatorischen Maßnahmen regelmäßig.

9.Unterauftragsverhältnisse

9.1.Der Auftragsverarbeiter ist berechtigt, weitere Auftragsverarbeiter („Unterauftragsverarbeiter“) zur Erfüllung der vertraglichen Leistungen einzusetzen.

Nicht als Unterauftragsverhältnisse im Sinne dieser Vereinbarung gelten Dienstleistungen, die der Auftragsverarbeiter als reine Nebenleistung in Anspruch nimmt, insbesondere Telekommunikationsleistungen, Post- und Transportdienstleistungen, Wartungsleistungen oder sonstige unterstützende Hilfsleistungen, sofern hierbei kein unmittelbarer Zugriff auf personenbezogene Daten des Kunden erfolgt.

9.2.Der Auftragsverarbeiter stellt sicher, dass sämtliche Unterauftragsverarbeiter durch schriftliche oder elektronische Vereinbarungen entsprechend den Anforderungen des Art. 28 DSGVO verpflichtet werden.

9.3.Die aktuell eingesetzten Unterauftragsverarbeiter ergeben sich aus Anlage 2 zu dieser Vereinbarung.

9.4.Der Auftragsverarbeiter informiert den Kunden über beabsichtigte Änderungen hinsichtlich der Hinzuziehung oder des Austauschs von Unterauftragsverarbeitern in angemessener Form und mit angemessener Vorlaufzeit.

Der Kunde kann einer solchen Änderung aus wichtigem datenschutzrechtlichem Grund widersprechen.

9.5.Soweit Unterauftragsverarbeiter personenbezogene Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums verarbeiten, stellt der Auftragsverarbeiter sicher, dass die Anforderungen der Art. 44 ff. DSGVO eingehalten werden und geeignete Garantien bestehen.

10.Betroffenenrechte

10.1.Wendet sich eine betroffene Person hinsichtlich ihrer Rechte gemäß Kapitel III DSGVO unmittelbar an den Auftragsverarbeiter, wird der Auftragsverarbeiter die betroffene Person an den Kunden verweisen, sofern eine Zuordnung zum Kunden möglich ist.

Der Auftragsverarbeiter wird ohne Weisung des Kunden keine eigenständige inhaltliche Bearbeitung von Betroffenenanfragen vornehmen, soweit keine gesetzliche Verpflichtung hierzu besteht.

10.2.Der Kunde erkennt an, dass die Software Funktionen zur eigenständigen Verwaltung personenbezogener Daten sowie zur Unterstützung datenschutzrechtlicher Pflichten bereitstellt.

Dies umfasst insbesondere Funktionen zur:

- Auskunft,
- Berichtigung,
- Löschung,
- Einschränkung der Verarbeitung,
- Datenexportierung,
- Verwaltung von Nutzer- und Beschäftigtendaten.

Soweit der Kunde eine Anfrage betroffener Personen nicht eigenständig bearbeiten kann, unterstützt der Auftragsverarbeiter den Kunden im angemessenen Umfang bei der Erfüllung seiner datenschutzrechtlichen Pflichten.

10.3.Der Kunde bleibt für die fristgerechte und rechtmäßige Bearbeitung von Betroffenenanfragen verantwortlich.

Eine Verantwortlichkeit des Auftragsverarbeiters besteht nicht, soweit Verstöße gegen datenschutzrechtliche Verpflichtungen ausschließlich durch den Kunden verursacht wurden.

11.Informations- und Mitteilungspflichten

11.1.Der Auftragsverarbeiter informiert den Kunden unverzüglich, nachdem ihm eine Verletzung des Schutzes personenbezogener Daten bekannt geworden ist, die personenbezogene Daten des Kunden betrifft.

11.2.Die Mitteilung erfolgt unter Berücksichtigung der Anforderungen des Art. 33 DSGVO und enthält soweit verfügbar insbesondere:

- Art der Datenschutzverletzung,
- betroffene Datenkategorien,

- mögliche Auswirkungen,
- bereits ergriffene oder vorgeschlagene Gegenmaßnahmen.

11.3.Der Auftragsverarbeiter unterstützt den Kunden im angemessenen Umfang bei der Erfüllung etwaiger Melde- und Benachrichtigungspflichten nach Art. 33 und Art. 34 DSGVO.

12.Herausgabe und Löschung von Daten

12.1.Nach Beendigung der Auftragsverarbeitung ist der Auftragsverarbeiter verpflichtet, die ihm im Rahmen der Verarbeitung bereitgestellten personenbezogenen Daten nach Maßgabe dieser Vereinbarung herauszugeben oder zu löschen.

Die Auftragsverarbeitung endet grundsätzlich mit Ablauf oder Beendigung des zugrunde liegenden Vertrages.

12.2.Nach Vertragsende bleiben die personenbezogenen Daten grundsätzlich für einen Zeitraum von bis zu 30 Tagen in einem eingeschränkten Lesezugriff („Read-only“) verfügbar, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

Innerhalb dieser Frist kann der Kunde:

- die Herausgabe der personenbezogenen Daten in einem strukturierten und maschinenlesbaren Format verlangen oder
- soweit technisch vorgesehen, die Daten eigenständig exportieren oder herunterladen.

Die Verantwortung für die rechtzeitige Sicherung und den Export der Daten liegt beim Kunden.

12.3.Erteilt der Kunde vor Ablauf der Frist gemäß Ziffer 12.2 eine verbindliche Löschungsanweisung in Textform, ist der Auftragsverarbeiter berechtigt und verpflichtet, die betreffenden Daten vorzeitig zu löschen, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

12.4.Erfolgt innerhalb der Frist gemäß Ziffer 12.2 weder eine Anforderung zur Herausgabe noch eine Löschungsanweisung durch den Kunden, ist der Auftragsverarbeiter berechtigt, die personenbezogenen Daten nach Ablauf der Frist zu löschen.

12.5.Daten in Sicherungs- und Archivsystemen werden im Rahmen der bestehenden technischen Prozesse gelöscht oder überschrieben, sobald dies regulär möglich ist.

13.Haftung

13.1.Die Parteien haften gegenüber betroffenen Personen nach Maßgabe des Art. 82 DSGVO für Schäden, die durch eine nicht der DSGVO entsprechende Verarbeitung personenbezogener Daten verursacht wurden.

13.2.Soweit beide Parteien für einen Schaden verantwortlich sind, haften sie gegenüber betroffenen Personen gemäß Art. 82 Abs. 4 DSGVO als Gesamtschuldner.

Im Innenverhältnis haftet jede Partei nur für den Schaden, der ihrem jeweiligen Verantwortungsbereich und Verursachungsbeitrag entspricht.

13.3.Eine Partei haftet nicht, soweit sie nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

13.4.Etwaige Haftungsbeschränkungen dieser Vereinbarung gelten nicht bei Vorsatz, grober Fahrlässigkeit oder bei Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit.

13.5.Im Übrigen richtet sich die Haftung nach den Regelungen des zugrunde liegenden Hauptvertrages.

14.Schlussbestimmungen

14.1.Beide Parteien verpflichten sich, sämtliche ihnen im Zusammenhang mit dieser Vereinbarung bekannt gewordenen vertraulichen Informationen, Geschäftsgeheimnisse sowie Informationen über technische und organisatorische Sicherheitsmaßnahmen auch über die Beendigung dieser Vereinbarung hinaus vertraulich zu behandeln.

Dies gilt insbesondere für Inhalte dieser Vereinbarung sowie für im Rahmen von Audits oder Prüfungen bereitgestellte Unterlagen, Nachweise und Dokumentationen.

14.2.Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Dies gilt auch für Änderungen dieses Formerfordernisses.

Die Parteien sind sich einig, dass die Anforderungen des Art. 28 Abs. 9 DSGVO auch durch elektronische Vereinbarungen und Kommunikation erfüllt werden können.

14.3.Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts (CISG).

Soweit gesetzlich zulässig, ist ausschließlicher Gerichtsstand Chemnitz.

14.4.Diese Vereinbarung ersetzt sämtliche früheren Vereinbarungen zur Auftragsverarbeitung zwischen den Parteien hinsichtlich des Vertragsgegenstands dieser Vereinbarung.

ANLAGE A.1: TECHNISCHE-ORGANISATORISCHE MASSNAHMEN

Der Auftragsverarbeiter trifft technische und organisatorische Maßnahmen gemäß Art. 28 Abs. 3 lit. c sowie Art. 32 DSGVO zur angemessenen Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten.

Die Maßnahmen werden unter Berücksichtigung des Stands der Technik, der Implementierungskosten, des Umfangs und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für betroffene Personen umgesetzt.

1.Zutrittskontrolle

Maßnahmen zur Verhinderung des unbefugten Zutritts zu Datenverarbeitungsanlagen:

- Nutzung dokumentierter Hosting- und Rechenzentrumsstandorte innerhalb der EU bzw. des EWR
- physische Sicherheitsmaßnahmen der eingesetzten Rechenzentren
- kontrollierter Zugang zu Büroräumen und Arbeitsgeräten
- Einsatz angemessener Zugangs- und Berechtigungskonzepte

2.Zugriffs- und Zugangskontrolle

Maßnahmen zur Verhinderung unbefugter Systemnutzung:

- Verwendung individueller Benutzerkonten
- rollenbasierte Berechtigungskonzepte
- Verwaltung und Einschränkung von Benutzerrechten
- Verwendung angemessener Kennwort- und Authentifizierungsrichtlinien
- Absicherung administrativer Zugriffe
- Einsatz zusätzlicher Schutzmaßnahmen für administrative oder besonders schützenswerte Zugriffe soweit technisch vorgesehen

3.Zugriffsbeschränkung und Berechtigungskonzepte

Maßnahmen zur Sicherstellung, dass ausschließlich berechtigte Personen Zugriff auf personenbezogene Daten erhalten:

- rollenabhängige Zugriffsrechte
- organisatorische Trennung administrativer und regulärer Benutzerrollen
- Einschränkung von Zugriffsrechten nach dem Erforderlichkeitsprinzip
- Überprüfung bestehender Berechtigungen soweit organisatorisch vorgesehen

4.Weitergabe- und Übertragungskontrolle

Maßnahmen zum Schutz personenbezogener Daten bei Übertragung und Weitergabe:

- Verwendung angemessener Verschlüsselungsverfahren bei der Datenübertragung

- Absicherung externer Zugriffe
- kontrollierte Schnittstellen und Zugriffswege
- dokumentierte Bereitstellung personenbezogener Daten

5.Eingabe- und Protokollierungskontrolle

Maßnahmen zur Nachvollziehbarkeit von Verarbeitungsvorgängen:

- nachvollziehbare Protokollierung relevanter Zugriffe und administrativer Vorgänge
- Dokumentation sicherheitsrelevanter Tätigkeiten soweit erforderlich
- Protokollierung von Exportvorgängen soweit technisch vorgesehen
- Dokumentation von Änderungen und Konfigurationsvorgängen soweit organisatorisch vorgesehen

6.Auftragskontrolle

Maßnahmen zur Verarbeitung personenbezogener Daten ausschließlich entsprechend dokumentierter Weisungen:

- Verarbeitung personenbezogener Daten ausschließlich im Rahmen vertraglicher Vereinbarungen
- Verpflichtung von Mitarbeitenden auf Vertraulichkeit
- dokumentierte interne Datenschutz- und Sicherheitsrichtlinien
- Sensibilisierung und Schulung von Mitarbeitenden
- Auswahl und Kontrolle eingesetzter Unterauftragsverarbeiter

7.Verfügbarkeitskontrolle und Datensicherung

Maßnahmen zum Schutz vor Verlust oder Zerstörung personenbezogener Daten:

- Durchführung angemessener Datensicherungsmaßnahmen
- Verfahren zur Wiederherstellung von Daten
- Schutz vor unbeabsichtigter Löschung oder Verlust
- dokumentierte Backup- und Wiederherstellungsverfahren
- angemessene Maßnahmen zur Sicherstellung der Systemverfügbarkeit

8.Trennungskontrolle

Maßnahmen zur getrennten Verarbeitung von Daten unterschiedlicher Kunden:

- logische Trennung von Kundendaten
- mandantenbezogene Datenverarbeitung
- organisatorische oder technische Trennung von Produktiv- und Testumgebungen soweit vorgesehen
- eingeschränkte Nutzung personenbezogener Daten in Testumgebungen

9.Mobile Anwendungen und Fernzugriffe

Maßnahmen zur Absicherung mobiler Anwendungen und Remotezugriffe:

- angemessene Schutzmaßnahmen für mobile Anwendungen und mobile Datenübertragungen
- abgesicherte Fernzugriffe
- Zugriffsbeschränkungen für mobile Anwendungen
- Schutz lokaler Zugriffsdaten soweit technisch vorgesehen
- Dokumentation administrativer Fernzugriffe soweit erforderlich

10.GPS- und Standortdaten

Soweit Funktionen zur Verarbeitung von GPS- oder Standortdaten genutzt werden:

- Verarbeitung ausschließlich nach Aktivierung durch den Verantwortlichen
- zweckgebundene Verarbeitung
- Deaktivierungsmöglichkeiten innerhalb der Anwendung soweit vorgesehen
- Beschränkung der Standortverarbeitung auf den jeweils vorgesehenen Zweck und Umfang
- Beschränkung auf erforderliche Standortinformationen

11.Lösch- und Aufbewahrungskonzepte

Maßnahmen zur datenschutzgerechten Löschung personenbezogener Daten:

- dokumentierte Lösch- und Aufbewahrungsprozesse
- Löschung personenbezogener Daten nach Vertragsende gemäß vertraglicher Vereinbarungen
- Read-only-Phasen und Exportmöglichkeiten soweit vorgesehen
- Löschung oder Überschreibung von Sicherungskopien im Rahmen bestehender Backupzyklen

12. Incident- und Sicherheitsmanagement

Maßnahmen zum Umgang mit Sicherheitsvorfällen:

- dokumentierte Prozesse zum Umgang mit Datenschutz- und Sicherheitsvorfällen
- interne Melde- und Eskalationswege
- angemessene Prozesse zur Behandlung erkannter Sicherheits- und Datenschutzvorfälle
- Einspielung sicherheitsrelevanter Aktualisierungen soweit organisatorisch vorgesehen
- angemessene Überprüfung eingesetzter Systeme und Anwendungen im Hinblick auf Sicherheitsanforderungen

13.Datenschutzmanagement und Vertraulichkeit

Organisatorische Maßnahmen zur Sicherstellung datenschutzkonformer Verarbeitung:

- Verpflichtung aller Mitarbeitenden auf Vertraulichkeit
- datenschutzbezogene Sensibilisierung und Schulungen
- interne Zuständigkeiten für Datenschutz und Informationssicherheit
- Unterstützung bei datenschutzrechtlichen Anfragen und Vorfällen
- Überprüfung datenschutzrelevanter organisatorischer Maßnahmen soweit vorgesehen

ANLAGE A.2 – Unterauftragnehmer (timatra)

Der Auftragsverarbeiter setzt zur Erbringung der Leistungen für timatra folgende Unterauftragnehmer ein.

Die Einbindung erfolgt ausschließlich im erforderlichen Umfang und unter Beachtung der datenschutzrechtlichen Anforderungen gemäß Art. 28 DSGVO.

Der Auftragsverarbeiter informiert den Kunden über wesentliche Änderungen mit angemessener Vorlaufzeit.

1. Hosting und Infrastruktur

Dienstleister	Standort	Leistung	Drittlandtransfer
IONOS SE	Deutschland / EU	Webhosting, Webspace, Datenbank- und technische Hosting-Infrastruktur	Nein

Dienstleister	Standort	Leistung	Drittlandtransfer
netcup GmbH	Deutschland und Österreich / EU – Rechenzentren Nürnberg und Wien	Hosting, Root-Server, Serverinfrastruktur und Datenspeicherung	Nein
OVH GmbH (OVHcloud)	Deutschland/Frankreich	Bereitstellung eines privaten vRack-Netzwerks zur sicheren Verbindung und Isolation von Servern und Cloud-Diensten	Nein

2. E-Mail- und Kommunikationsdienste

Dienstleister	Standort	Leistung	Drittlandtransfer
SCALEWAY SAS	Frankreich / EU	Versand transaktionaler System- und Benachrichtigungs-E-Mails; SMTP- und E-Mail-Infrastruktur	Nein

3. Fernwartung und Support

Dienstleister	Standort	Leistung	Drittlandtransfer
TeamViewer Germany GmbH	Deutschland / EU	Fernwartung, Remote-Zugriff und technischer Support	ggf. ja**

** Abhängig vom Standort des verbundenen Endgeräts sowie von den eingesetzten Zusatzfunktionen und Unterauftragnehmern. Drittlandübermittlungen erfolgen nach Maßgabe der Art. 44 ff. DSGVO.

4. Textverarbeitungsdienste

Die Verarbeitung richtet sich nach den vereinbarten Zwecken und Weisungen des Kunden. Die übermittelten Daten sind auf den hierfür erforderlichen Umfang zu beschränken.

Dienstleister	Standort	Leistung	Drittlandtransfer
Melious AI GmbH, Campus Starterzentrum, Geb. A1.2, 66123 Saarbrücken, Deutschland	Deutschland / EU / EWR	API-gestützte Verarbeitung von Texteingaben und bereitgestellten Kontextdaten sowie Erstellung von Antworten zur Unterstützung interner Arbeitsabläufe. Dabei können personenbezogene Kundendaten verarbeitet werden.	Nach veröffentlichter Datenschutzerklärung Verarbeitung von Eingaben und Antworten innerhalb der EU sowie Speicherung hochgeladener Dateien innerhalb des EWR. Der veröffentlichte AV-Vertrag enthält Regelungen für Drittlandübermittlungen gemäß Ziffern 1.3 und 6.4 sowie Art. 44 ff. DSGVO.

Nach der Datenschutzerklärung von Melious vom 9. November 2026 werden die übermittelten Eingaben und Antworten nicht zu Trainingszwecken verwendet. Der veröffentlichte AV-Vertrag vom 11. November 2026 beschränkt die Verarbeitung der im Auftrag verarbeiteten Daten auf die vereinbarten Leistungen und die Weisungen des Auftraggebers. Gesetzlich vorgeschriebene Verarbeitungen bleiben vorbehalten.

Zur Erbringung der Verarbeitungsleistungen kann Melious Eingaben und Kontextdaten an weitere Unterauftragnehmer übermitteln. Der veröffentlichte AV-Vertrag beschreibt die Verteilung von Anfragen auf mehrere Anbieter einschließlich eines automatischen Wechsels bei Ausfällen. Laut Anlage 1 werden ausschließlich Betriebsmetadaten wie Zeitstempel, verwendetes Modell, Tokenumfang sowie Routing- und Fehlerinformationen protokolliert, nicht die Inhalte der Eingaben und Antworten.

Die Zusage einer Verarbeitung ohne dauerhafte Speicherung der Eingaben und Antworten („Zero Data Retention“) nach Ziffer 3.6 des veröffentlichten AV-Vertrags gilt nur auf den von Melious selbst betriebenen Servern einschließlich der in Anlage 4 entsprechend gekennzeichneten dedizierten Hardware. Für sonstige Unterauftragnehmer gilt diese Klausel ausdrücklich nicht. Ausgenommen sind außerdem aktiv genutzte Speicherfunktionen wie Batch-API, Dateien, Vektorspeicher und Vault, Betriebsmetadaten sowie gesetzlich vorgeschriebene Verarbeitungen. Eine allgemeine Zusage, dass Daten weder gespeichert noch an weitere Dienstleister übermittelt werden, ist damit nicht verbunden.

Für gespeicherte Daten regelt Ziffer 10 des veröffentlichten AV-Vertrags die Löschung oder Rückgabe auf Verlangen bzw. nach Vertragsende, vorbehaltlich gesetzlicher Aufbewahrungspflichten. Als gelöscht markierte Daten sind innerhalb von 30 Tagen endgültig zu löschen. Sicherungskopien werden turnusmäßig spätestens nach 30 Tagen gelöscht. Nachweisdokumentationen zur ordnungsgemäßen Verarbeitung sind davon ausgenommen und bis zum Ablauf des vierten Kalenderjahres nach der jeweiligen Verarbeitung aufzubewahren.

Die vorherige schriftliche Zustimmung zu Drittlandverlagerungen nach Ziffer 1.3 des veröffentlichten AV-Vertrags steht unter dem Vorbehalt von Ziffer 6.4. Danach sind Unterauftragsverarbeitungen außerhalb des EWR bei einem einschlägigen Angemessenheitsbeschluss oder wirksam vereinbarten

Standarddatenschutzklauseln zulässig. Andernfalls verlangt der Vertrag die anderweitige Erfüllung der Art. 46 bis 49 DSGVO und eine vorherige Zustimmung des Auftraggebers in Textform. Die Anforderungen der Art. 44 ff. DSGVO bleiben zu beachten. Diese Angaben beschreiben die veröffentlichten Regelungen von Melious und ersetzen nicht die Pflichten aus dieser Vereinbarung gegenüber dem Kunden.

Weitere Informationen: Datenschutzerklärung, Auftragsverarbeitungsvertrag und Unterauftragnehmer von Melious. Die Angaben zu den Zusagen von Melious beruhen auf diesen veröffentlichten Dokumenten.

5. Drittlandtransfers

Soweit Unterauftragnehmer personenbezogene Daten außerhalb der EU bzw. des EWR verarbeiten, erfolgt dies ausschließlich unter Einhaltung der Art. 44 ff. DSGVO.

Hierzu können insbesondere folgende Mechanismen eingesetzt werden:

- Angemessenheitsbeschlüsse gemäß Art. 45 DSGVO
- EU-Standardvertragsklauseln (SCCs)
- ergänzende technische und organisatorische Maßnahmen