Auftragsverarbeitungsvertrag (AVV)

Stand: 5. November 2026

Präambel

Dieser AVV ergänzt den Vertrag über die Nutzung der KI-Plattform denkk („Vertrag“) zwischen der Meetflow GmbH, Carlonestr. 15, 94137 Bayerbach („denkk“), und dem Kunden, der auf diesen AVV Bezug nimmt (gemeinsam die „Parteien“). Der AVV tritt automatisch mit dem Abschluss des Vertrags in Kraft und gilt ab demselben Zeitpunkt.

Bei der Erfüllung des Vertrags verarbeitet denkk personenbezogene Daten, die der Kunde bereitstellt. denkk verarbeitet diese Daten im Auftrag des Kunden: als Auftragsverarbeiter, wenn der Kunde Verantwortlicher ist, oder als Unterauftragsverarbeiter, wenn der Kunde selbst Auftragsverarbeiter ist. Der AVV gilt daher, wenn und soweit denkk bei der Erbringung der Leistungen personenbezogene Daten für den Kunden verarbeitet. Er ersetzt alle früheren Datenschutzvereinbarungen der Parteien zu diesen Leistungen.

1. Definitionen

1.1 „Kundendaten“ sind alle personenbezogenen Daten, die bei der Nutzung der Leistungen hochgeladen, aus verbundenen Drittsystemen abgerufen oder beim Auslösen von Aktionen in diesen Systemen im Auftrag des Kunden verarbeitet werden und die denkk bei der Erbringung der Leistungen im Auftrag des Kunden verarbeitet.

1.2 „Verantwortlicher“ ist die Person oder Gesellschaft, die über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

1.3 „Auftragsverarbeiter“ ist die Person oder Gesellschaft, die personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet.

1.4 „Datenschutzgesetze“ sind alle auf die Verarbeitung personenbezogener Daten anwendbaren Datenschutzgesetze, in der EU und im EWR insbesondere die Datenschutz-Grundverordnung (DSGVO), die Richtlinie 2002/58/EG (e-Privacy) und die nationalen Datenschutzgesetze der Mitgliedstaaten.

1.5 „EWR“ ist der Europäische Wirtschaftsraum.

1.6 „EU“ ist die Europäische Union.

1.7 „Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

1.8 „Verarbeitung“ hat die Bedeutung nach der DSGVO und umfasst jeden Vorgang im Zusammenhang mit personenbezogenen Daten, etwa Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleichen oder Verknüpfen, Einschränken und Löschen.

1.9 „Sicherheitsvorfall“ ist jede unbefugte oder unrechtmäßige Verletzung der Sicherheit, die zur versehentlichen oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung von oder zum unbefugten Zugang zu Kundendaten führt.

1.10 „Leistungen“ hat die im Vertrag festgelegte Bedeutung.

1.11 „SCC“ sind die Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer im Anhang des Durchführungsbeschlusses (EU) 2021/914 der Kommission vom 4. Juni 2021.

1.12 „Unterauftragsverarbeiter“ ist jeder Auftragsverarbeiter, den denkk zur Unterstützung bei der Erbringung der Leistungen beauftragt.

2. Gegenstand

2.1 Dieser AVV regelt die Rechte und Pflichten der Parteien bei der Verarbeitung von Kundendaten durch denkk im Zusammenhang mit der Erbringung der Leistungen.

2.2 Dazu beauftragt der Kunde denkk als Auftragsverarbeiter, wenn er selbst Verantwortlicher ist, oder als Unterauftragsverarbeiter, wenn er selbst Auftragsverarbeiter ist.

2.3 Der AVV gilt für alle Kundendaten nach Anlage 1, auf die denkk bei der Erbringung der Leistungen Zugriff hat. Dazu gehören Kundendaten, die der Kunde denkk bereitstellt, die denkk bei der Erbringung der Leistungen erzeugt oder auf die denkk auf andere Weise im Rahmen der Leistungen Zugriff erhält, etwa direkt von betroffenen Personen. Der AVV gilt nicht für Daten, die keine Kundendaten sind, einschließlich nicht personenbezogener Daten des Kunden und Daten, die nicht im Rahmen der Leistungen verarbeitet werden.

3. Verarbeitung im Auftrag des Kunden

3.1 denkk trifft geeignete technische und organisatorische Maßnahmen, damit die Verarbeitung der Kundendaten den Datenschutzgesetzen entspricht und die Rechte der betroffenen Personen gewahrt bleiben.

3.2 denkk und etwaige Unterauftragsverarbeiter verarbeiten Kundendaten grundsätzlich im EWR. Eine Übermittlung in ein Drittland außerhalb des EWR findet nur statt, wenn denkk die Einhaltung der Datenschutzgesetze sicherstellt und eine geeignete Rechtsgrundlage besteht, etwa ein Angemessenheitsbeschluss, SCC oder andere zulässige Garantien.

3.3 Im Verhältnis der Parteien ist allein der Kunde für die Rechtmäßigkeit der Verarbeitung der Kundendaten und die Wahrung der Rechte der betroffenen Personen verantwortlich. Machen Dritte wegen einer Verarbeitung von Kundendaten nach diesem AVV Ansprüche gegen denkk geltend, stellt der Kunde denkk von diesen Ansprüchen frei.

4. Weisungen des Kunden

4.1 denkk verarbeitet die Kundendaten nur auf dokumentierte Weisung des Kunden, auch im Hinblick auf Übermittlungen in ein Drittland. Ist denkk gesetzlich zu einer Verarbeitung ohne Weisung verpflichtet, teilt denkk dem Kunden diese Verpflichtung vorher mit, es sei denn, das Gesetz verbietet eine solche Mitteilung aus Gründen des öffentlichen Interesses.

4.2 Das Weisungsrecht des Kunden zu Art, Umfang und Verfahren der Verarbeitung ist auf den in diesem AVV und im Vertrag festgelegten Umfang beschränkt. Stimmt denkk einer darüber hinausgehenden Weisung zu, ersetzt der Kunde denkk die dadurch entstehenden Kosten und Aufwendungen.

4.3 Der Kunde erteilt Weisungen schriftlich, per E-Mail (Textform) oder durch die Nutzung der Funktionen der Leistungen.

4.4 denkk verwendet Kundendaten ausschließlich zur Erbringung der Leistungen. Ausgenommen sind Sicherungskopien, die für eine ordnungsgemäße Verarbeitung erforderlich sind, Daten, die zur Erfüllung gesetzlicher Aufbewahrungspflichten aufbewahrt werden, sowie anonymisierte oder aggregierte Daten, die keinen Rückschluss auf Personen zulassen und nur für interne Zwecke wie Analysen oder Verbesserungen der Leistungen genutzt werden. Kundendaten und daraus gewonnene anonymisierte oder aggregierte Daten werden nicht zum Training von KI-Modellen verwendet.

5. Unterauftragsverarbeiter

5.1 denkk setzt Unterauftragsverarbeiter nur mit vorheriger schriftlicher Zustimmung des Kunden ein. Die Zustimmung kann im Einzelfall oder allgemein erteilt werden.

5.2 Der Kunde stimmt mit Wirkung ab dem Datum dieses AVV dem Einsatz der in Anlage 2 aufgeführten Unterauftragsverarbeiter zu.

5.3 Der Kunde erteilt außerdem seine allgemeine Zustimmung zum Einsatz weiterer Unterauftragsverarbeiter. denkk informiert den Kunden mindestens 15 Tage, bevor ein neuer Unterauftragsverarbeiter erstmals Kundendaten verarbeitet, über jede geplante Änderung der Liste, also über das Hinzufügen oder Ersetzen eines Unterauftragsverarbeiters. Der Kunde kann aus berechtigten Gründen innerhalb von 15 Tagen nach der Mitteilung schriftlich widersprechen. Die Parteien arbeiten dann nach Treu und Glauben an einer Lösung.

5.4 Setzt denkk einen Unterauftragsverarbeiter für bestimmte Verarbeitungen im Auftrag des Kunden ein, erlegt denkk ihm durch Vertrag oder ein anderes nach den Datenschutzgesetzen zulässiges Rechtsinstrument dieselben Datenschutzpflichten auf, die in diesem AVV festgelegt sind. denkk stellt dabei sicher, dass der Unterauftragsverarbeiter hinreichende Garantien bietet, insbesondere für geeignete technische und organisatorische Maßnahmen nach der DSGVO und den übrigen Datenschutzgesetzen. Es genügt, wenn das Schutzniveau des Unterauftragsverarbeiters dem dieses AVV gleichwertig ist.

5.5 Unterliegt der Einsatz eines Unterauftragsverarbeiters den Art. 44 ff. DSGVO, schließt denkk, soweit erforderlich, die anwendbaren SCC ab und stellt sicher, dass der Unterauftragsverarbeiter geeignete technische und organisatorische Maßnahmen zur Einhaltung der Datenschutzgesetze trifft.

5.6 Werden die SCC unwirksam oder nicht mehr als Übermittlungsmechanismus nach der DSGVO oder anderen Datenschutzgesetzen anerkannt, darf denkk auf jede andere nach den Datenschutzgesetzen zulässige Garantie zurückgreifen, etwa verbindliche interne Datenschutzvorschriften (BCR) oder andere geeignete Garantien oder Ausnahmen nach Kapitel V DSGVO.

5.7 Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, ist denkk dem Kunden gegenüber dafür verantwortlich.

5.8 Die Beauftragung Dritter mit Nebenleistungen, etwa Telekommunikation, Wartung, Benutzerunterstützung, Reinigung, Prüfung oder Entsorgung von Datenträgern, gilt nicht als Einsatz eines Unterauftragsverarbeiters. denkk stellt aber durch geeignete Vereinbarungen und Kontrollen sicher, dass Sicherheit und Vertraulichkeit der Kundendaten auch dann geschützt sind.

5.9 Die Anbindung an Drittsysteme, die der Kunde freigegeben hat, über offene Schnittstellen (u. a. Model Context Protocol) erfolgt im Auftrag und mit den Zugangsdaten des Kunden. Der Kunde weist die Datenflüsse zwischen der Plattform und dem verbundenen Drittsystem an, einschließlich der dort ausgelösten Aktionen. Betreiber solcher Drittsysteme sind keine Unterauftragsverarbeiter von denkk, soweit der Kunde eigene Vertragsverhältnisse mit ihnen unterhält. Für die Rechtmäßigkeit der Verarbeitung in den Drittsystemen und die datenschutzrechtlichen Grundlagen des Zugriffs ist der Kunde verantwortlich.

6. Kontrollrechte des Kunden

6.1 denkk stellt dem Kunden auf schriftliche Anfrage innerhalb eines angemessenen Zeitraums die Informationen zur Verfügung, die zum Nachweis der Einhaltung dieses AVV erforderlich sind.

6.2 Der Kunde oder ein von ihm beauftragter Prüfer kann die Einhaltung dieses AVV durch denkk überprüfen. Prüfungen finden während der üblichen Geschäftszeiten statt und so, dass der Betrieb von denkk möglichst wenig gestört wird.

6.3 denkk kann die Einhaltung dieses AVV auch durch aktuelle Prüfbescheinigungen, Berichte oder Auszüge unabhängiger Stellen (etwa Wirtschaftsprüfer, Datenschutzbeauftragte, IT-

Sicherheitsabteilungen oder Datenschutzauditoren) oder durch geeignete Zertifizierungen aus anerkannten IT-Sicherheits- oder Datenschutzaudits nachweisen.

7. Vertraulichkeit

denkk stellt sicher, dass alle Personen, die zur Verarbeitung von Kundendaten nach diesem AVV befugt sind, vertraglich oder aufgrund einer gesetzlichen Verschwiegenheitspflicht zur Vertraulichkeit verpflichtet sind.

8. Technische und organisatorische Maßnahmen

8.1 Unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten der betroffenen Personen treffen der Kunde und denkk in ihrem jeweiligen Verantwortungsbereich geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf Sicherheitsvorfälle.

8.2 Die technischen und organisatorischen Maßnahmen von denkk sind in Anlage 3 aufgeführt. Der Kunde bestätigt, dass diese Maßnahmen die Anforderungen erfüllen und ein angemessenes Schutzniveau für die Verarbeitung der Kundendaten gewährleisten.

8.3 denkk darf die technischen und organisatorischen Maßnahmen jederzeit durch gleich- oder höherwertige Maßnahmen ersetzen, sofern diese den Anforderungen dieser Ziffer 8 genügen.

9. Informationspflichten von denkk

9.1 denkk informiert den Kunden unverzüglich, wenn denkk von einem Sicherheitsvorfall Kenntnis erhält.

10. Unterstützung des Kunden

10.1 denkk unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anfragen betroffener Personen zu beantworten und seine weiteren Pflichten nach den Datenschutzgesetzen zu erfüllen.

10.2 denkk informiert den Kunden unverzüglich, wenn eine Weisung des Kunden nach Auffassung von denkk gegen Datenschutzgesetze verstößt.

11. Laufzeit

11.1 Dieser AVV tritt automatisch mit dem Abschluss des Vertrags in Kraft und gilt mindestens für die Dauer des Vertrags, soweit nichts anderes bestimmt ist.

11.2 Endet der Vertrag, gleich aus welchem Grund, endet auch dieser AVV automatisch. Seine Bestimmungen gelten jedoch fort, soweit dies für einen ordnungsgemäßen Abschluss der Verarbeitung von Kundendaten nach den Datenschutzgesetzen erforderlich ist, insbesondere für die Löschung oder Rückgabe der Kundendaten. Ist diese Verarbeitung abgeschlossen, endet der AVV ohne weitere Mitteilung.

12. Löschung und Rückgabe nach Vertragsende

Nach Beendigung der Leistungen löscht denkk nach Weisung des Kunden alle Kundendaten oder gibt sie zurück. Der Kunde teilt denkk seine Wahl innerhalb von 30 Tagen nach Beendigung der Leistungen mit. Erfolgt in dieser Frist keine Mitteilung, darf denkk die Kundendaten löschen, sofern nicht das geltende Recht eine weitere Speicherung vorschreibt. Gesetzliche Aufbewahrungs- und Archivierungspflichten bleiben unberührt. Auf Anfrage des Kunden bestätigt denkk die Löschung oder Rückgabe.

13. Datenschutzbeauftragter

denkk bestellt einen Datenschutzbeauftragten, soweit die Datenschutzgesetze dies verlangen, und teilt dem Kunden in diesem Fall dessen Kontaktdaten mit.

14. Vergütung

14.1 Alle Leistungen von denkk nach diesem AVV sind mit der im Vertrag vereinbarten Vergütung vollständig abgegolten, soweit dieser AVV nicht ausdrücklich etwas anderes bestimmt.

14.2 Soweit Leistungen nach diesem AVV als vergütungspflichtig bezeichnet sind, werden sie nach Aufwand zu den im Vertrag vereinbarten Sätzen vergütet. Sind keine Sätze vereinbart, gelten die zum Zeitpunkt der Leistung gültigen Standardsätze von denkk.

15. Haftung

15.1 Die Haftungsregelungen des Vertrags gelten für diesen AVV entsprechend.

15.2 Behördliche Bußgelder oder Strafen, die unmittelbar gegen den Kunden verhängt werden, kann der Kunde nicht von denkk zurückverlangen, es sei denn, sie beruhen auf einem Verstoß von denkk gegen diesen AVV oder die Datenschutzgesetze. In diesem Fall ist die Haftung von denkk auf den Mitverschuldensanteil beschränkt, den ein zuständiges Gericht oder eine zuständige Behörde rechtskräftig feststellt, und unterliegt den Haftungsregelungen des Vertrags.

16. Schlussbestimmungen

16.1 Dieser AVV ist fester Bestandteil des Vertrags. Bei Widersprüchen zwischen Vertrag und AVV hat der AVV ausschließlich in Bezug auf die Verarbeitung von Kundendaten Vorrang.

16.2 denkk darf diesen AVV ändern, soweit dies wegen Änderungen der Datenschutzgesetze, regulatorischer Anforderungen oder verbindlicher Entscheidungen der Aufsichtsbehörden erforderlich ist. denkk informiert den Kunden mindestens 30 Tage vorher schriftlich oder in Textform, etwa per E-Mail, es sei denn, eine sofortige Änderung ist gesetzlich oder regulatorisch vorgeschrieben. Widerspricht der Kunde aus berechtigten Gründen, suchen die Parteien nach Treu und Glauben eine für beide akzeptable Lösung. Kommt innerhalb angemessener Frist keine Einigung zustande, kann der Kunde den Vertrag für die betroffenen Verarbeitungen schriftlich kündigen.

16.3 Ist eine Bestimmung dieses AVV ganz oder teilweise unwirksam oder undurchführbar oder wird sie es, bleiben die übrigen Bestimmungen wirksam. Dasselbe gilt für Regelungslücken. An die Stelle der unwirksamen Bestimmung oder zur Füllung der Lücke tritt eine angemessene Regelung, die dem wirtschaftlich Gewollten und dem Sinn und Zweck dieses AVV am nächsten kommt.

16.4 Im Übrigen gelten die Schlussbestimmungen des Vertrags entsprechend.

Anlage 1: Details der Verarbeitung

1. Kategorien betroffener Personen

- Nutzer der Leistungen
- Mitarbeitende des Kunden
- Personen, auf die sich Daten beziehen, die Nutzer eingeben, die aus verbundenen Drittsystemen abgerufen oder beim Auslösen von Aktionen im Auftrag des Kunden verarbeitet werden

2. Arten von Kundendaten

- Namen und E-Mail-Adressen von Nutzern und Mitarbeitenden des Kunden
- Daten, die Nutzer eingeben
- Personenbezogene Daten, die aus vom Kunden freigegebenen Drittsystemen abgerufen oder beim Auslösen von Aktionen in diesen Systemen im Auftrag des Kunden verarbeitet werden

3. Umfang und Art der Verarbeitung

- Inhalte der Kommunikation mit den KI-Modellen (Eingaben und Antworten)
- Dokumente und Informationen, die der Kunde auf der Plattform hochlädt und speichert
- Abruf von Daten aus vom Kunden freigegebenen Drittsystemen über offene Schnittstellen (u. a. Model Context Protocol)
- Übermittlung und Verarbeitung von Kundendaten beim Auslösen von Aktionen in verbundenen Drittsystemen im Auftrag des Kunden, im Rahmen der vom Kunden erteilten Berechtigungen

4. Zweck der Verarbeitung

- Bereitstellung der Leistungen nach den Weisungen des Kunden, einschließlich des Abrufs von Daten aus verbundenen Drittsystemen und des Auslösens von Aktionen in diesen Systemen im Auftrag des Kunden

Anlage 2: Unterauftragsverarbeiter

Hetzner Online GmbH
Anschrift: Industriestr. 25, 91710 Gunzenhausen, Deutschland
Aufgabe: Bereitstellung von Cloud-Infrastruktur für das Hosting der Plattform
Ort der Verarbeitung: Deutschland

UpCloud Oy
Anschrift: Aleksanterinkatu 15 B, 7. Etage, 00100 Helsinki, Finnland
Aufgabe: Bereitstellung der Datenbank und des Zwischenspeichers (Cache)
Ort der Verarbeitung: Deutschland

Melious AI GmbH
Anschrift: Universität des Saarlandes, Campus Starterzentrum, Geb. A1.2, 66123 Saarbrücken, Deutschland
Aufgabe: Bereitstellung der KI-Modelle zur Verarbeitung von Nutzeranfragen (Input) und Erzeugung von Modellantworten (Output)
Ort der Verarbeitung: EU/EWR

WhiteCloud Project S.R.L. (orkestr)
Anschrift: Ardealului Nr. 62, Sector 1, 013436 Bukarest, Rumänien
Aufgabe: Bereitstellung isolierter Umgebungen zur Code-Ausführung (Code-Sandbox)
Ort der Verarbeitung: EU/EWR

Brevo SAS
Anschrift: 9–17 rue Salneuve, 75017 Paris, Frankreich
Aufgabe: Versand von E-Mails der Plattform an Nutzer
Ort der Verarbeitung: EU

Stripe Payments Europe, Limited
Anschrift: 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Irland
Aufgabe: Abwicklung und Verwaltung von Zahlungsvorgängen
Ort der Verarbeitung: EU

Anlage 3: Technische und organisatorische Maßnahmen (TOMs)

gem. Art. 32 DSGVO · Meetflow GmbH · Stand: 15. Oktober 2026

Hinweis

Dieses Dokument enthält Informationen, welche Geschäftspartnern, Kunden sowie weiteren externen Stellen, die ein gesetzliches oder sonstig begründetes Einsichtsrecht haben, zur Verfügung gestellt werden. Aus Gründen der Lesbarkeit wurde im Text die männliche Form gewählt, nichtsdestoweniger beziehen sich die Angaben auf Angehörige aller Geschlechter.

Präambel

Der Verantwortliche hat geeignete Maßnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung implementiert. Der allgemeine Teil (Grundsätzliche Maßnahmen) beschreibt technische und organisatorische Maßnahmen die unabhängig von den jeweiligen Dienstleistungen und Services, Standorten und Kunden gelten. In den darauf folgenden Abschnitten sind Maßnahmen beschrieben, die über die im allgemeinen Teil dokumentierten Maßnahmen hinaus gelten.

1. Grundsätzliche Maßnahmen

Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:

- Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung systematisch überwacht sowie anlassbezogen und mindestens jährlich evaluiert wird.
- Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet. Es umfasst Formulare, Anleitungen und alle notwendigen Umsetzungsverfahren.
- Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe und Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren.
- Die an Mitarbeiter, im Hinblick auf die Verarbeitung personenbezogener Daten erteilten Berechtigungen, sowie ausgegebenen Schlüssel, Zugangskarten oder Codes jeglicher Art, werden nach deren Ausscheiden aus dem Unternehmen, bzw. Wechsel der Zuständigkeiten, gemäß eines Berechtigungskonzeptes, eingezogen, bzw. entzogen.
- Bei Dienstleistern, die personenbezogene Daten im Auftrag verarbeiten, wird der Schutz von personenbezogenen Daten und die Sicherung der Rechte und Pflichten von Auftraggebern/Auftragnehmern einer Auftragsverarbeitung gewährleistet. Dies gilt auch für vergleichbare Situationen mit einem Datentransfer in sogenannte Drittstaaten.
- Mitarbeiter werden im Hinblick auf den Datenschutz geschult, belehrt und instruiert, auf Verschwiegenheit verpflichtet, wie auch auf mögliche Haftungsfolgen hingewiesen. Für die Verarbeitung personenbezogener Daten werden vom Unternehmen bereitgestellte Endgeräte genutzt.
- Der Schutz von personenbezogenen Daten wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt (Art. 25 DSGVO).
- Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virenscanner und Firewalls.

- Einsatz eines auf technische Fehler- und Performanceinformationen beschränkten Monitorings ohne Erfassung von Prompts, Modellantworten, Dokumentinhalten und sonstigen Kundendaten.
- Prüfung von Änderungen in einer vom Produktivbetrieb getrennten Testumgebung vor der Produktivsetzung sowie regelmäßig ausgeführte Schwachstellentests.

2. Zutrittskontrolle

Alle Maßnahmen, die dazu geeignet sind, den Zutritt für Unbefugte zu den Datenverarbeitungsanlagen zu verhindern.

Umgesetzte Maßnahmen:

- Hosting der Anwendung und der Kundendaten in ISO/IEC 27001-zertifizierten Rechenzentren; die physische Zutrittskontrolle der Rechenzentren wird durch die Hosting-Anbieter gewährleistet
- Manuelles Schließsystem
- Türen mit Knauf Außenseite
- Besucher halten sich nicht unbeaufsichtigt in Räumen auf, in denen personenbezogene Daten verarbeitet werden
- Besucher werden ausschließlich in Besprechungs- oder Empfangsräumen empfangen, nicht in Büroräumen
- Besucher werden an der Tür bzw. am Empfang in Empfang genommen und gelangen nicht ohne Begleitung in weitere Räume
- Während der Anwesenheit von Besuchern ist durchgehend Personal in den Räumen anwesend

3. Zugangskontrolle / Zugriffskontrolle

Alle Maßnahmen, die geeignet sind, die Nutzung der Datenverarbeitungssysteme durch Unbefugte zu verhindern sowie alle Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Umgesetzte Maßnahmen:

- Login mit Benutzername + Passwort
- Multi-Faktor-Authentifizierung, insbesondere für privilegierte und sicherheitsrelevante Zugänge
- Passwortmanager zur Erzeugung und sicheren Speicherung eindeutiger Zugangsdaten
- stets aktueller Virenschutz
- stets aktuelle Softwareversionen
- Verschlüsselter Datentransfer über https/TLS oder vergleichbare Schutzsysteme
- Administrativer Zugriff auf die Hosting-Infrastruktur ausschließlich über verschlüsselte und zugangsgeschützte Verbindungen
- Verschlüsselung von Datenträgern
- Verschlüsselung von Notebooks / Tablet
- Verschlüsselung der Kundendaten in der Datenbank (AES-256)
- Automatische Desktopsperre
- Richtlinie „Sicheres Passwort“
- Allg. Richtlinie Datenschutz und / oder Sicherheit
- Mobile Device Policy
- Einsatz Berechtigungskonzepte
- Minimale Anzahl an Administratoren
- Verwaltung Benutzerrechte durch Administratoren

4. Weitergabekontrolle

Alle Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Umgesetzte Maßnahmen:

- Daten werden nur an autorisierte Dritte weitergegeben
- Verschlüsselung von Datenträgern und Verbindungen
- Bereitstellung über verschlüsselte Verbindungen wie sftp, https

5. Eingabekontrolle

Alle Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Umgesetzte Maßnahmen:

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Protokollierung von Aktionen in der Anwendung in einem für den Kunden einsehbaren Audit-Log
- Gesonderte Protokollierung sicherheitsrelevanter Datenbankzugriffe
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Klare Zuständigkeiten für Löschungen

6. Auftragskontrolle

Alle Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Umgesetzte Maßnahmen:

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
- Schriftliche Weisungen an den Auftragnehmer
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- Regelung zum Einsatz weiterer Subunternehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

7. Verfügbarkeitskontrolle / Integrität

Alle Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Umgesetzte Maßnahmen:

- Backup & Recovery-Konzept (ausformuliert)
- Ständig kontrolliertes Backup- und Recoverykonzept
- Tägliche Sicherung der Datenbank sowie fortlaufende Sicherung der Transaktionen zur zeitpunktgenauen Wiederherstellung (Point-in-Time-Recovery)
- Speicherung aller Daten und Sicherungen innerhalb der Europäischen Union

- Technischer Schutz vor Datenverlust und unbefugten Zugriffen durch Virenschutz, Anti-Spyware und Spamfilter
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Physische Schutz- und Redundanzmaßnahmen der Rechenzentrumsbetreiber, insbesondere für Stromversorgung, Klimatisierung, Brandschutz und Speichersysteme

8. Gewährleistung des Zweckbindungs-/Trennungsgebotes

Alle Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Umgesetzte Maßnahmen:

- Trennung von Produktiv- und Testumgebung
- Logische Mandantentrennung in der Datenbank durch Row-Level Security
- Steuerung über Berechtigungskonzept
- Festlegung von Datenbankrechten
- Installation eines mandantenfähigen Systems