Diese Vereinbarung zur Auftragsverarbeitung („**AVV**“) spezifiziert die Datenschutzpflichten und -rechte der Parteien im Zusammenhang mit der Verarbeitung der von TTE Strategy (nachfolgend „**Auftragnehmer**“) für den Kunden (nachfolgend „**Auftraggeber**“) verarbeiteten personenbezogenen Daten unter dem zwischen den Parteien geschlossenen Vertrag über die Bereitstellung der Plattform (nachfolgend „**Hauptvertrag**“).

1 Anwendungsbereich

Bei der Erbringung der Leistungen gemäß dem Hauptvertrag verarbeitet der Auftragnehmer personenbezogene Daten, die der Auftraggeber zur Erbringung der Leistungen zur Verfügung gestellt hat und bezüglich derer der Auftraggeber als Verantwortlicher im datenschutzrechtlichen Sinn fungiert („**Auftraggeber-Daten**“). Im Falle von Widersprüchen zwischen dieser AVV und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus dieser AVV vor.

2 Gegenstand und Umfang der Beauftragung / Weisungsbefugnisse des Auftraggebers

2.1 Der Auftragnehmer wird die Auftraggeber-Daten ausschließlich im Auftrag und gemäß den Weisungen des Auftraggebers verarbeiten, sofern der Auftragnehmer nicht durch das Recht der Europäischen Union oder eines Mitgliedsstaates gesetzlich zur 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.

2.2 Die Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer erfolgt ausschließlich in der Art, dem Umfang und zu dem Zweck wie in **Anhang 1** zu dieser AVV spezifiziert; die Verarbeitung betrifft ausschließlich die darin bezeichneten Arten personenbezogener Daten und Kategorien betroffener Personen.

2.3 Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrags.

2.4 Es ist dem Auftragnehmer gestattet, Auftraggeber-Daten außerhalb des Europäischen Wirtschaftsraums („**EWR**“) zu verarbeiten oder durch weitere Auftragsverarbeiter gemäß Ziffer 5 verarbeiten zu lassen, wenn die Voraussetzungen der Art. 44 bis 48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt und insbesondere der Auftragnehmer besondere Anforderungen zum Schutz der Auftraggeber-Daten getroffen hat.

2.5 Die Weisungen ergeben sich aus dem Hauptvertrag.

Der Auftraggeber ist zur Erteilung von weiteren Weisungen über Art, Umfang, Zwecke und Mittel der Verarbeitung von Auftraggeber-Daten nur berechtigt, wenn solche Weisungen nach dem Recht der Europäischen Union oder eines Mitgliedstaates oder aufgrund gerichtlicher oder behördlicher Anordnung erforderlich sind. In allen übrigen Fällen, in denen der Auftraggeber Weisungen erteilt, die über die Vereinbarungen im Hauptvertrag oder dieser AVV hinausgehen, trägt der Auftraggeber die Kosten und Aufwendungen für die Ausführung solcher

Weisungen. Bevor er solche Weisungen ausführt, wird der Auftragnehmer den Auftraggeber über die zu erwartenden Kosten und Aufwendungen informieren und dessen Bestätigung abwarten. Letzteres gilt nicht für Weisungen zur Einstellung der Datenverarbeitung als Ganzes oder zur Löschung einzelner oder aller Auftraggeber-Daten.

2.6 Weisungen sollen in Schrift- oder Textform erfolgen. Mündliche Weisungen wird der Auftraggeber schriftlich oder per E-Mail bestätigen.

2.7 Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen diese AVV, die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt, wird er den Auftraggeber hierüber unverzüglich in Schrift- oder Textform informieren. Der Auftragnehmer ist berechtigt, die Ausführung einer solchen Weisung solange auszusetzen, bis der Auftraggeber sie in Schrift- oder Textform bestätigt. Besteht der Auftraggeber trotz der vom Auftragnehmer vorgebrachten Bedenken auf die Durchführung einer Weisung, stellt der Auftraggeber den Auftragnehmer von sämtlichen Schäden und Kosten frei, die dem Auftragnehmer durch die Ausführung der Weisung des Auftraggebers entstehen. Der Auftragnehmer wird den Auftraggeber über gegen den Auftragnehmer geltend gemachte Schäden und ihm entstehende Kosten informieren und Ansprüche Dritter nicht ohne Zustimmung des Auftraggebers anerkennen und die Verteidigung, nach Wahl des Auftragnehmers, in Koordination mit dem Auftraggeber vornehmen oder diesem überlassen.

3 Anforderungen an Personal

3.1 Der Auftragnehmer hat alle Personen, die Auftraggeber-Daten verarbeiten, zur Vertraulichkeit zu verpflichten, soweit diese nicht einer angemessenen gesetzlichen Verschwiegenheit unterliegen.

3.2 Der Auftragnehmer stellt sicher, dass ihm unterstellte Personen, die Zugang zu Auftraggeber-Daten haben, diese nur nach Maßgabe dieser AVV sowie nach Weisungen des Auftraggebers verarbeiten, es sei denn, sie sind nach dem Recht der Europäischen Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

4 Sicherheit der Verarbeitung

4.1 Der Auftragnehmer ergreift alle geeigneten technischen und organisatorischen Maßnahmen, die unter Berücksichtigung des Stands der Technik, der Implementierungskosten und – soweit dem Auftragnehmer bekannt – der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen erforderlich sind, um ein dem Risiko angemessenes Schutzniveau für die Auftraggeber-Daten zu gewährleisten.

4.2 Der Auftragnehmer hat vor dem Beginn der Verarbeitung der Auftraggeber-Daten insbesondere die in **Anhang 2** zu dieser AVV spezifizierten technischen und organisatorischen Maßnahmen zu ergreifen und während der Dauer des Hauptvertrags aufrechtzuerhalten sowie sicherzustellen, dass die Verarbeitung von Auftraggeber-Daten im Einklang mit diesen Maßnahmen durchgeführt wird.

4.3 Es obliegt dem Auftraggeber, die von dem Auftragnehmer ergriffenen technischen und organisatorischen Maßnahmen zu überprüfen, insbesondere ob diese auch im Hinblick auf Umstände der Datenverarbeitung ausreichend sind, die dem Auftragnehmer nicht bekannt sind.

4.4 Da die technischen und organisatorischen Maßnahmen dem technischen Fortschritt unterliegen, ist der Auftragnehmer berechtigt und verpflichtet, alternative, adäquate Maßnahmen umzusetzen, um das Sicherheitsniveau der in **Anhang 2** festgelegten Maßnahmen nicht zu unterschreiten. Nimmt der Auftragnehmer wesentliche Änderungen an den in **Anhang 2** festgelegten Maßnahmen vor, wird er den Auftraggeber hierüber vorab informieren.

5 Inanspruchnahme weiterer Auftragsverarbeiter

5.1 Der Auftragnehmer setzt bei der Verarbeitung der Auftraggeber-Daten die in **Anhang 3** aufgelisteten weiteren Auftragsverarbeiter ein. Diese gelten mit Abschluss der AVV als genehmigt.

5.2 Der Auftragnehmer darf zur Verarbeitung von Auftraggeber-Daten weitere Auftragsverarbeiter unter folgender Maßgabe in Anspruch nehmen:

Der Auftragnehmer informiert den Auftraggeber mindestens dreißig (30) Tage vor der Inanspruchnahme des weiteren Auftragsverarbeiters in Text- oder Schriftform an eine vom Auftraggeber für diese Zwecke benannte Adresse. Soweit der Auftraggeber nicht innerhalb von vierzehn (14) Tagen Widerspruch erhebt, gilt die Inanspruchnahme als genehmigt.

5.3 Wenn der Auftraggeber gemäß Ziffer 5.2 Widerspruch erhebt, ist der Auftragnehmer berechtigt, nach seiner Wahl entweder seine Leistungen aus dem Hauptvertrag ohne den Einsatz des abgelehnten weiteren Auftragsverarbeiters zu erbringen oder den Hauptvertrag und diese AVV zu kündigen.

5.4 Der Auftragnehmer hat jedem weiteren Auftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten aufzuerlegen, die gemäß dieser AVV für den Auftragnehmer gelten.

5.5 Der Auftragnehmer ist verpflichtet, nur solche weiteren Auftragsverarbeiter auszuwählen und in Anspruch zu nehmen, die hinreichende Garantien dafür bieten, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung der Auftraggeber-Daten entsprechend den Anforderungen der DSGVO, dieser AVV und eventueller zusätzlicher Vertraulichkeitsverpflichtungen erfolgt.

6 Rechte der betroffenen Personen

6.1 Der Auftragnehmer wird alle zumutbaren technischen und organisatorischen Maßnahmen treffen, um den Auftraggeber dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen betroffener Personen auf Wahrnehmung der ihnen zustehenden Rechte nachzukommen.

6.2 Der Auftragnehmer wird insbesondere, im Rahmen seiner Möglichkeiten:

- den Auftraggeber unverzüglich informieren, falls sich eine betroffene Person mit einem Antrag auf Wahrnehmung ihrer Rechte in Bezug auf Auftraggeber-Daten unmittelbar an den Auftragnehmer wenden sollte;
- dem Auftraggeber auf dessen Anfrage alle bei ihm vorhandenen Informationen über die Verarbeitung von Auftraggeber-Daten geben, die der Auftraggeber zur Beantwortung des Antrags einer betroffenen Person benötigt und über die der Auftraggeber nicht selbst verfügt;
- Auftraggeber-Daten auf Weisung des Auftraggebers unverzüglich berichtigen, löschen oder in der Verarbeitung einschränken, soweit der Auftraggeber dies nicht selbst vornehmen kann und dies dem Auftragnehmer technisch möglich ist;
- den Auftraggeber soweit erforderlich unterstützen, die im Verantwortungsbereich des Auftragnehmers verarbeiteten Auftraggeber-Daten – soweit dies dem Auftragnehmer technisch möglich ist – in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, soweit der betroffenen Person gegenüber dem Auftraggeber ein Recht auf Datenübertragbarkeit bezüglich der Auftraggeber-Daten zusteht.

7 Sonstige Unterstützungspflichten des Auftragnehmers

7.1 Der Auftragnehmer meldet dem Auftraggeber, unverzüglich nachdem ihm eine solche bekannt geworden ist, jede Verletzung des Schutzes von Auftraggeber-Daten, insbesondere Vorkommnisse, die zur tatsächlichen Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu Auftraggeber-Daten führen. Die Meldung enthält nach Möglichkeit eine Beschreibung:

a) der Art der Verletzung des Schutzes der Auftraggeber-Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen;

b) der wahrscheinlichen Folgen der Verletzung des Schutzes der Auftraggeber-Daten;

c) der von dem Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes der Auftraggeber-Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7.2 Der Auftragnehmer ist verpflichtet, bei allen Verletzungen des Schutzes von Auftraggeber-Daten unverzüglich sämtliche erforderlichen und zumutbaren Maßnahmen zur Behebung der Verletzung des Schutzes der Auftraggeber-Daten und gegebenenfalls zur Abmilderung ihrer möglichen nachteiligen Auswirkungen zu ergreifen.

7.3 Ist der Auftraggeber gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeber-Daten zu erteilen oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftragnehmer verpflichtet, den Auftraggeber bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit im Rahmen seiner Möglichkeiten zu unterstützen.

7.4 Der Auftragnehmer wird den Auftraggeber bei der Einhaltung der in Art. 32 DSGVO genannten Pflichten unterstützen, soweit ihm dies unter Berücksichtigung der ihm zur Verfügung stehenden Informationen über die konkrete Nutzung der Leistungen des Auftraggebers möglich ist.

7.5 Für den Fall, dass der Auftraggeber verpflichtet ist, die Aufsichtsbehörden und/oder betroffene Personen nach Art. 33, 34 DSGVO zu informieren, wird der Auftragnehmer im Rahmen des Möglichen den Auftraggeber auf dessen Anfrage unterstützen, diese Pflichten einzuhalten. Der Auftragnehmer ist insbesondere verpflichtet, sämtliche Verletzungen des Schutzes von Auftraggeber-Daten einschließlich aller damit im Zusammenhang stehenden Fakten in einer Weise zu dokumentieren, die dem Auftraggeber den Nachweis der Einhaltung etwa einschlägiger gesetzlicher Meldepflichten ermöglicht.

7.6 Der Auftragnehmer wird den Auftraggeber mit den ihm zur Verfügung stehenden Informationen und im Rahmen des Zumutbaren bei etwaig von ihm durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

8 Datenlöschung und -zurückgabe

8.1 Der Auftragnehmer wird nach Wahl des Auftraggebers mit Beendigung des Hauptvertrages alle Auftraggeber-Daten entweder vollständig löschen oder an den Auftraggeber zurückgeben und bestehende Kopien löschen, sofern nicht nach dem Recht der Europäischen Union oder eines Mitgliedsstaates eine Verpflichtung des Auftragnehmers zur weiteren Speicherung der Auftraggeber-Daten besteht.

8.2 Der Auftragnehmer ist jedoch berechtigt, für einen Zeitraum von dreißig (30) Tagen Sicherungskopien der Auftraggeber-Daten aufzubewahren, soweit eine Löschung der Auftraggeber-Daten aus diesen Sicherungskopien technisch oder im Hinblick auf Art. 32 DSGVO nicht geboten ist. Für diesen Zeitraum gelten die Rechte und Pflichten der Parteien aus dieser AVV in Bezug auf die Sicherungskopien abweichend von Ziffer 2.3 fort.

8.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung der Auftraggeber-Daten dienen, sind durch den Auftragnehmer entsprechend der gesetzlichen Aufbewahrungsfristen über das Vertragsende dieser AVV hinaus aufzubewahren.

9 Nachweise und Überprüfungen

9.1 Der Auftragnehmer hat sicherzustellen und regelmäßig zu kontrollieren, dass die Verarbeitung der Auftraggeber-Daten mit dieser AVV, dem Hauptvertrag sowie den Weisungen des Auftraggebers in Einklang steht.

9.2 Der Auftragnehmer wird die Umsetzung der Pflichten nach dieser AVV in geeigneter Weise dokumentieren und dem Auftraggeber alle erforderlichen Nachweise über die Einhaltung der Pflichten des Auftragnehmers nach der DSGVO und dieser AVV auf dessen Anfrage vorlegen.

9.3 Der Auftraggeber ist berechtigt, den Auftragnehmer regelmäßig während der Laufzeit des Hauptvertrags bezüglich der Einhaltung der Regelungen dieser AVV, insbesondere der Umsetzung der technischen und organisatorischen Maßnahmen gemäß **Anhang 2** selbst oder durch einen qualifizierten und zur Verschwiegenheit verpflichteten Prüfer zu überprüfen; einschließlich durch Inspektionen. Der Auftragnehmer ermöglicht solche Überprüfungen und trägt durch alle zweckmäßigen und zumutbaren Maßnahmen zu solchen Überprüfungen bei; unter anderem durch die Gewährung der notwendigen Zugangs- und Zugriffsrechte und die Bereitstellung aller notwendigen Informationen.

9.4 Die Überprüfungen und Inspektionen sollen den Auftragnehmer in seinem normalen Geschäftsbetrieb nach Möglichkeit nicht behindern und diesen nicht über Gebühr belasten. Insbesondere sollen Inspektionen bei dem Auftragnehmer ohne konkreten Anlass nicht mehr als einmal im Kalenderjahr und nur während der üblichen Geschäftszeiten des Auftragnehmers stattfinden. Der Auftraggeber hat dem Auftragnehmer Inspektionen rechtzeitig vorab in Schrift- oder Textform anzukündigen.

9.5 Gemäß den Bestimmungen der DSGVO unterliegen der Auftraggeber und der Auftragnehmer öffentlichen Kontrollen durch die zuständige Aufsichtsbehörde. Auf Anforderung durch den Auftraggeber wird der Auftragnehmer die gewünschten Informationen an die Aufsichtsbehörde liefern und dieser die Möglichkeit zur Prüfung einräumen; davon umfasst sind Inspektionen beim Auftragnehmer durch die Aufsichtsbehörde oder die von ihr benannten Personen. Der Auftragnehmer gewährt der zuständigen Aufsichtsbehörde in diesem Rahmen die erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte.

10 Haftung

Die im Hauptvertrag vereinbarten Haftungsbeschränkungen gelten entsprechend.

11 Sonstiges

11.1 Änderungen und Nebenabreden zu dieser AVV bedürfen der Schriftform. Dies gilt auch für diese Schriftformklausel.

11.2 Rechtswahl- und Gerichtsstandsvereinbarungen aus dem Hauptvertrag gelten für diese AVV entsprechend.

Anhang 1 - Zweck, Art und Umfang der Datenverarbeitung, Art der Daten und Kreis der betroffenen Personen

Zweck der Datenverarbeitung	Bereitstellung der KI-gestützten Plattform wie im Hauptvertrag vereinbart.
Art und Umfang der Datenverarbeitung	Containerisierte Webanwendung (SvelteKit/Node.js), PostgreSQL-Datenbank, privater Object Storage für Uploads, E-Mail-Dienst für Login und Zwei-Faktor-Authentifizierung sowie automatisierte Backups. Mandantentrennung über Row Level Security. Über die Speicherung hinaus werden Nutzereingaben, Case-Daten und hochgeladene Dokumente (TXT, CSV, JSON, PDF, DOCX) per Textextraktion aufbereitet und zur Analyse, Empfehlung und Konsistenzprüfung an die eingesetzten KI-Modelle übergeben. Die Verarbeitung erfolgt serverseitig. Die Verarbeitung erfolgt überwiegend automatisiert. Hosting auf Microsoft Azure in einer EU-Region. KI-Anfragen laufen über den EU-Endpunkt von Requesty.ai an EU-Modelle und bei Websearch Aktivitäten an globale Modelle.
Art der Daten	Namen, Kontaktdaten, E-Mail-Adressen
Kreis der betroffenen Personen	Kunden, Arbeitnehmer der Kunden, sonstige Dritte (z.B. Geschäftspartner)

Anhang 2 – Technische und organisatorische Maßnahmen

1 Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO) und Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO)

Um die Vertraulichkeit personenbezogener Daten sicherzustellen, sind Zutritt, Zugriff und Zugang zu Systemen, die personenbezogene Daten speichern, verarbeiten oder weitergeben streng geregelt und werden regelmäßig überprüft. Außerdem sind jeweils angemessene Verfahren zur getrennten Verarbeitung der Daten im Einsatz, um die Vertraulichkeit der Daten und Systeme im angemessenen Umfang zu sichern.

1.1 Zutrittskontrolle

Ziel der Zutrittskontrolle ist es, Unbefugten den räumlichen Zutritt zu solchen Datenverarbeitungsanlagen zu verwehren, in denen personenbezogene Daten verarbeitet werden.

Es existiert ein klar definiertes Zutrittsberechtigungskonzept zu unseren Räumlichkeiten.

- Die Anwesenheitszeiten der Mitarbeiter werden dokumentiert (Zeiterfassungseinrichtungen).
- Besucher/Externe werden begleitet/abgeholt und stets beaufsichtigt.
- Der Zutritt ist durch magnetische oder Chipkarten / Schlüssel möglich.
- Ein Alarmsystem ist vorhanden.
- Einzelne IT-Systeme werden in externen Rechenzentren (Hosting) und bei externen Diensten betrieben (Software-as-a-service). Dort gewährleistet der jeweilige Anbieter die Zutrittskontrolle.
- Dokumentation von Vorfällen und unbefugten Zutrittsversuchen.

1.2 Zugangskontrolle/Verschlüsselung

Ziel der Zugangskontrolle ist es, Unbefugten die Nutzung solcher Datenverarbeitungssysteme zu verwehren, mit denen die personenbezogenen Daten verarbeitet werden.

Der Zugang zu PCs, Servern und Netzkomponenten erfolgt durch Berechtigungsvergabe und Authentifizierung. Die Zugangsregelungen umfassen folgende Maßnahmen:

- Der Zugang zu extern gehosteten/betriebenen IT-Systemen ist besonders gesichert (Verschlüsselung, Start-PIN).
- Das Netzwerk ist gegen ungewollte Zugriffe von außen abgeschottet (Firewall, Intrusion Detection System).
- Der Zugang zu IT-Systemen ist nur mit Benutzerkennung und individuellem Passwort möglich.
- IT-Systeme werden bei wiederholt erfolglosen Anmeldeversuchen gesperrt.
- Einzelne Endgeräte werden funktional zugeordnet und die Systemnutzung protokolliert.
- Mobile Datenträger sind verschlüsselt (Hardwareverschlüsselung).
- Es gibt eine Bildschirmsperre mit automatischer Sperrung bei längerer Abwesenheit an Arbeitsstationen.
- Eine Zwei-Faktor-Authentifizierung wird genutzt.
- Nutzung von sicheren Passwörtern mit Mindestlänge und Komplexitätsvorgaben.
- Verwendung des Passwortmanagers

1.3 Zugriffskontrolle

Ziel der Zugriffskontrolle ist es, unerlaubte Tätigkeiten in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen zu verhindern.

- Individuelle Zugriffsrechte für jeden einzelnen Benutzer sind vorhanden.
- Die Verwaltung und Steuerung des Berechtigungskonzeptes erfolgen zentral.
- Zugriffsberechtigungen werden aufgabenbezogen und nach dem Need-to-know-Prinzip erteilt.
- Die Zugriffsberechtigungen werden regelmäßig überprüft. Nicht mehr erforderliche Berechtigungen werden unverzüglich entzogen.
- Es ist organisatorisch geregelt, dass Daten auf lokale IT-Systeme kopiert werden.
- Daten auf mobilen IT-Systemen sind verschlüsselt (komplettes System, Hardwareverschlüsselung).
- Regelmäßige Sicherheitsüberprüfung und Audits der Zugriffskontrollen.

1.4 Trennungskontrolle/Zweckbindungskontrolle

Ziel der Trennungskontrolle und Zweckbindungskontrolle ist die Gewährleistung getrennter Verarbeitung von zu unterschiedlichen Zwecken erhobenen Daten.

- Es existiert eine softwareseitige Mandantentrennung.
- Logische Trennung von sensiblen und allgemeinen Daten.

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

Zur Sicherstellung der Integrität der personenbezogenen Daten insbesondere Systeme kontrolliert, auf denen personenbezogene Daten eingegeben und von denen diese Daten transferiert bzw. weitergegeben werden.

2.1 Weitergabekontrolle

Ziel der Weitergabekontrolle ist es, das unbefugte Lesen, Kopieren, Verändern oder Entfernen personenbezogener Daten während ihrer elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger zu verhindern und die Überprüfung und Feststellung, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen sind.

- Übermittlungen personenbezogener Daten sind im Verzeichnis von Verarbeitungstätigkeiten dokumentiert.
- Die Datenspeicherung und -verarbeitung erfolgt auf IT-Systemen im Rechenzentrum. Die Verbindung zwischen Clients und Server ist besonders gesichert (Verschlüsselung).
- Datenträger werden kontrolliert vernichtet (physische Vernichtung).

- Besucher haben keinen Zugriff auf betriebliches LAN/WLAN.

2.2 Eingabekontrolle

Ziel der Eingabekontrolle ist es, die nachträgliche Überprüfung und Feststellung der näheren Umstände der Dateneingabe, Datenveränderung und Datenlöschung zu ermöglichen.

- Gescheiterte Zugriffsversuche werden protokolliert.
- Aktivitäten des Systemverwalters und sämtlicher Benutzer werden protokolliert.
- Die Protokolldaten werden gegen Verlust und Veränderung gesichert.

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

Um die personenbezogenen Daten vor Verlust und Zerstörungen zu schützen, gibt es ein Sicherheitskonzept und Pläne zur Wiederherstellung.

3.1 Verfügbarkeitskontrolle

Ziel der Verfügbarkeitskontrolle ist es, personenbezogene Daten vor zufälliger oder mutwilliger Zerstörung oder Verlust zu schützen (die Angaben beziehen sich auf eigene IT-Systeme des Auftragnehmers).

- Es existiert ein Datensicherheitskonzept.
- Schadsoftwareschutz ist vorhanden.
- Sicherheitsrelevante Updates und Patches werden regelmäßig und zeitnah eingespielt.
- Eine unterbrechungsfreie Stromversorgung ist gewährleistet.

3.2 Rasche Wiederherstellbarkeit

Sollte trotzdem ein Verlust personenbezogener Daten eintreten, ist es das Ziel, diese schnellstmöglich wiederherzustellen.

- Es werden täglich/wöchentlich versionierte Daten- und Systembackups nach einem Backup-Plan erstellt.
- Es werden Festplattenspiegelungen hergestellt (RAID). Es gibt ein Backup-Rechenzentrum.
- Für den Fall des Datenverlusts gibt es ein Berichtsverfahren und einen Notfallplan. Die Funktionsfähigkeit dieser Pläne wird in regelmäßigen Abständen getestet.

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d), 25 Abs. 1 DSGVO)

Zur Sicherstellung einer ordnungsgemäßen und rechtmäßigen Datenverarbeitung sind spezifische Abläufe implementiert.

4.1 Auftragskontrolle

Ziel der Auftragskontrolle ist es, sicherzustellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Die Auftragnehmer werden sorgfältig ausgesucht.
- Weisungen werden grundsätzlich schriftlich erteilt.
- Der Auftragnehmer wird durch die Geschäftsführung oder den Datenschutzbeauftragten kontrolliert.

4.2 Interne Datenschutz-Kontrollen

Ziel der internen Datenschutz-Kontrollen ist es, die Aktualität der dokumentierten Maßnahmen zu überprüfen und mögliche Schwachstellen und Umsetzungsdefizite auszudecken.

- Jährlicher Soll-/Ist-Abgleich der dokumentierten Maßnahmen durch den Datenschutzbeauftragten
- Regelmäßige Schwachstellen-Analyse der IT-Systeme durch die IT-Abteilung

4.3 Datenschutz-Management

Ziel des Datenschutzmanagements ist es, die Steuerung der Datenschutzprozesse zu ermöglichen und die Einhaltung der datenschutzrechtlichen Vorgaben nachweisbar sicherzustellen.

- Es wurde eine fachkundige Person zum Datenschutzbeauftragten benannt.
- Beschäftigte werden regelmäßig im Datenschutz geschult und sensibilisiert und sind über die Vertraulichkeit von Daten belehrt.

Anhang 3 – Weitere Auftragsverarbeiter

Name	Art der Daten	Zweck	Ort der Verarbeitung / Garantien
Microsoft Inc.	Namen, Kontaktdaten, Authentifizierungsdaten, Nutzers IDs	Cloud-Hosting	EU/EWR
Requesty Ltd.	Nutzer IDs, Namen, in Prompts enthaltene personenbezogene Daten	Bereitstellung von KI-Funktionen	EU/EWR / Global