# Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO

zwischen der

**[Name/Firma]**
[Straße, Hausnummer]
[PLZ Ort]

**-Auftraggeber-**

und der

**H24 GmbH**
Ledererzeile 48
83512 Wasserburg am Inn

**-Auftragnehmer-**

## 1 Allgemeines

(1) Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers i.S.d. Art. 4 Nr. 8 und Art. 28 der DSGVO.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

## 2 Gegenstand und Dauer der Vereinbarung

(1) Der Gegenstand der Auftragsverarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in der **Anlage 1** zu diesem Vertrag festgelegt.

(2) Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages.

(3) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(4) Die Dauer der Auftragsverarbeitung ergibt sich aus dem Hauptvertrag.

Copyright actago GmbH, 2026

(5) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schwerwiegenden Verstoß dar.

# 3 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 1 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte im Zusammenhang mit dieser Verarbeitung von Daten im Auftrag gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen müssen in Textform (z.B. E-Mail) erfolgen, zwischen den Vertragsparteien einvernehmlich abgestimmt sein und protokolliert werden. Das Protokoll umfasst zumindest den Inhalt der Weisung, das Datum, optional die Uhrzeit und die involvierten Ansprechpartner beider Parteien.

(4) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

(5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 2** benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

# 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. 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. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem AVV und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes

Copyright actago GmbH, 2026 

vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Vertraulichkeit verpflichtet (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer führt in regelmäßigen Abständen Maßnahmen zur Mitarbeitersensibilisierungen zum Datenschutz durch und überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

(3) Die Verarbeitung von Daten ist nur eigener Hardware des Auftragnehmers gestattet (Privatcomputer von Mitarbeitern des Auftragnehmers dürfen nicht verwendet werden). Für den Fall, dass Mitarbeiter des Auftragnehmers in privaten oder öffentlichen Räumen arbeiten, habe die technischen und organisatorischen Maßnahmen dem Stand der **Anlage 3** dieses Vertrages zu entsprechen. Diese Mitarbeiter sind speziell zu unterweisen. Die Unterweisungen sind zu protokollieren.

(4) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. e und f DSGVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an den Auftraggeber weiterzuleiten.

(5) Der Auftragnehmer sichert zu, den Auftraggeber bei seinen Pflichten nach Art. 32 bis 36 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gemäß Ziff. 4 dieses Vertrages durchführen. Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO.

(6) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 UAbs. 1 Satz 2 lit. h DSGVO). Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Vereinbarungen zu Kontroll- und Prüfungsunterlagen sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

(7) Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Er verpflichtet sich, auch für diesen Auftrag relevante Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen. Der Auftragnehmer verpflichtet sich bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Dies besteht auch nach Beendigung des Vertrages fort.

(8) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird.

# 5 Datenschutzbeauftragter des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt

hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt. Der Datenschutzbeauftragte der H24 GmbH kann wie folgt kontaktiert werden:

actago GmbH
Weidenstraße 66
94405 Landau an der Isar
Tel.: 09951 99990-508
E-Mail: schmerbeck@actago.de

(2) Die Pflicht zur Benennung eines Datenschutzbeauftragten nach Absatz 1 kann im Ermessen des Auftraggebers entfallen, wenn der Auftragnehmer nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen und der Auftragnehmer nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der gesetzlichen Vorschriften, der Regelungen dieses AVVs sowie etwaiger weiterer Weisungen des Auftraggebers gewährleisten.

# 6 Unterauftragsverhältnisse

(1) Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern befugt, soweit der Auftraggeber nicht ausdrücklich innerhalb einer Frist von zwei Wochen nach Mitteilung der geplanten Beauftragung widerspricht. Er setzt den Auftraggeber hiervon unverzüglich in Kenntnis. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der **Anlage 2** zu dieser Vereinbarung angeben. Sofern der Auftraggeber der Beauftragung eines Subunternehmers widerspricht, darf dieser vom Auftragnehmer für die Erfüllung seiner vertraglichen Pflichten nicht beauftragt werden.

(2) Der Auftragnehmer hat dafür Sorge zu tragen, dass er den Unterauftragnehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt (Art. 28 Abs. 4 S. 1 DSGVO). Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

(3) Eine Beauftragung von Unterauftragnehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(4) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Unterauftragnehmern gelten (Art. 28 Abs. 4 S. 1 DSGVO). In dem Vertrag mit dem Unterauftragnehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Unterauftragnehmers deutlich voneinander abgegrenzt werden. Werden mehrere Unterauftragnehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Unterauftragnehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Unterauftragnehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

(5) Der Vertrag mit dem Unterauftragnehmern muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 9 DSGVO).

(6) Die Weiterleitung von Daten an den Unterauftragnehmer ist erst zulässig, wenn der Unterauftragnehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

(7) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Unterauftragnehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden (Art. 28 Abs. 4 S. 2 DSGVO).

Copyright actago GmbH, 2026

(8) Etwaige Regelungen zu einer Vergütung von Leistungen sind zwischen den Parteien gesondert zu vereinbaren.

# 7 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 3** zu diesem Vertrag beigefügt. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann einmal jährlich oder bei begründeten Anlässen eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

# 8 Vertraulichkeits- und Geheimhaltungspflichten

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

(4) Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

(5) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

(6) Die besonderen Anforderungen und ergänzenden Schutzmaßnahmen für Berufsgeheimnisträger sind in **Anlage 4** zu diesem Vertrag geregelt und sind sofern erforderlich gesondert zu unterzeichnen.

Copyright actago GmbH, 2026

# 9 Löschung und Rückgabe von Daten

(1) Nach Beendigung des AVV, auf Verlangen des Auftraggebers oder nach vollständiger Erbringung der geschuldeten Leistung hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 (bei Papierdokumenten mindestens die Sicherheitsstufe 4) der DIN 66399 einzuhalten ist; die Vernichtung ist dem Auftraggeber unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den Auftraggeber angekündigt werden.

(3) Der Auftragnehmer darf personenbezogene Daten, die im Zusammenhang mit dem Auftrag verarbeitet worden sind, über die Beendigung des Vertrages hinaus speichern, wenn und soweit den Auftragnehmer eine gesetzliche Pflicht zur Aufbewahrung trifft. In diesen Fällen dürfen die Daten nur für Zwecke der Umsetzung der jeweiligen gesetzlichen Aufbewahrungspflichten verarbeitet werden. Nach Ablauf der Aufbewahrungspflicht sind die Daten unverzüglich zu löschen.

# 10 Haftung

Es gelten die Bestimmungen der Haftung und das Recht auf Schadenersatz nach Art 82 der DSGVO.

# 11 Schlussbestimmungen

(1) Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

(2) Sollten einzelne Regelungen dieser Vereinbarung unwirksam oder undurchführbar sein, wird davon die Wirksamkeit der übrigen Regelungen nicht berührt. An die Stelle der unwirksamen oder undurchführbaren Regelung tritt diejenige wirksame und durchführbare Regelung, deren Wirkungen der Zielsetzung am nächsten kommt, die die Vertragsparteien mit der unwirksamen oder undurchführbaren Bestimmung verfolgt haben.

(3) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i.S.d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

Copyright actago GmbH, 2026

**Auftragnehmer:**

| | |
|---|---|
| Ort, Datum | Unterschrift (Vor- und Nachname) |

**Auftraggeber:**

| | |
|---|---|
| Ort, Datum | Unterschrift (Vor- und Nachname) |

Anlage 1: Konkretisierung des Auftragsinhalts

Anlage 2: Unterauftragnehmer

Anlage 3: Technische und organisatorische Maßnahmen

Anlage 4: Zusatz für Berufsgeheimnisträger zur Auftragsverarbeitung

Copyright actago GmbH, 2026

# A.1 Anlage 1 – Konkretisierung des Auftragsinhalts

**1. Gegenstand und Zweck der Verarbeitung**

Der Auftragnehmer ist vom Auftraggeber damit beauftragt, eine browserbasierte LLM-Plattform für die Verarbeitung von Inhalten bereitzustellen. Der Auftragnehmer übernimmt die technische Bereitstellung und den Betrieb der Plattform, einschließlich der Integration und Wartung der genutzten Sprachmodelle. Die Bereitstellung erfolgt durch den Auftragnehmer. Der Betrieb der LLM-Plattform wird über die komplette Vertragslaufzeit vom Auftragnehmer gewährleistet.

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich zur Erbringung der vertraglich vereinbarten Dienstleistungen im Rahmen der browserbasierten LLM-Plattform. Dies umfasst insbesondere die Verarbeitung von Inhalten zur Generierung und Analyse von Texten und Bildern die durch die Nutzer der Plattform eingegeben oder hochgeladen werden.

Der Auftragnehmer stellt im Rahmen der LLM-Plattform eine Funktion zur automatisierten Generierung von Antwortvorschlägen für E-Mails als Add-in in der jeweiligen E-Mail-Plattform bereit. Hierbei werden Inhalte aus eingehenden oder zu beantwortenden E-Mails verarbeitet, um auf Basis der bereitgestellten Informationen kontextbezogene Textvorschläge zu erzeugen. Die Nutzung dieser Funktion erfolgt ausschließlich auf Weisung und unter Kontrolle des Auftraggebers. Eine automatisierte Versendung von E-Mails durch den Auftragnehmer findet nicht statt. Die generierten Vorschläge dienen lediglich der Unterstützung der Nutzer und bedürfen vor einer Verwendung der Prüfung und Freigabe durch den jeweiligen Nutzer.

**2. Art(en) der personenbezogenen Daten**

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

a) Inhaltsdaten (Textdaten), die vom Auftraggeber oder dessen Nutzern eingegeben, hochgeladen oder anderweitig zur Verfügung gestellt werden, insbesondere Texteingaben (Prompts), hochgeladene Dokumente, Chatverläufe sowie die durch die Plattform erzeugten Ausgaben. Hierzu können auch Inhalte aus E-Mail-Kommunikation gehören, sofern die Funktion zur Generierung von Antwortvorschlägen genutzt wird.

b) Account- und Stammdaten der Nutzer (Bestandsdaten) Daten, die zur Einrichtung, Verwaltung und Nutzung von Nutzerkonten erforderlich sind, insbesondere:

- E-Mail-Adressen
- Name bzw. Anzeigenname, soweit dieser vom Auftraggeber bereitgestellt oder vom Nutzer im Nutzerprofil hinterlegt wird
- Organisations- oder Mandantenzugehörigkeit (z. B. Behörde, Unternehmen, Domain, Tenant-ID),
- Rollen- und Berechtigungsinformationen,
- Account-Status (z. B. aktiv, gesperrt)

c) Authentifizierungs- und Sicherheitsdaten Daten, die zur sicheren Authentifizierung und Autorisierung erforderlich sind. -Identitäts- und Authentifizierungsinformationen aus einem angebundenen Identity-Provider (Single-Sign-On-Claims)

- Sitzungs- und Token-Daten (Session-IDs)

Sofern eine lokale Authentifizierung vorgesehen ist, werden Passwörter ausschließlich in Form kryptographisch sicherer Hashwerte verarbeitet, eine Speicherung von Passwörtern im Klartext erfolgt nicht. Erfolgt die Authentifizierung ausschließlich über Single Sign-On, werden durch den Auftragnehmer keine Passwörter verarbeitet.

Copyright actago GmbH, 2026

d) Technische Nutzungs- und Betriebsdaten (Metadaten) Technische Metadaten, die für den Betrieb, die Stabilität, die Sicherheit und die Optimierung der Plattform erforderlich sind, insbesondere Nutzungs- und Interaktionsdaten, System- und Performance-Metriken sowie Fehler- und Protokolldaten, jeweils beschränkt auf das erforderliche Maß.

**3. Kategorien betroffener Person**

Kreis der von der Datenverarbeitung betroffenen Personen:

- Nutzer der LLM-Plattform, die Texte, Bilddateien und Tonaufnahmen zur Verarbeitung eingeben;
- Mitarbeiter des Auftraggebers, die die Plattform für geschäftliche Zwecke nutzen.

**4. Weisungsberechtigte Personen des Auftraggebers**

Als weisungsberechtigte Personen beim Auftraggeber sind benannt:
Hier ggf. Personen benennen oder Passage streichen.

# A.2 Anlage 2 –Unterauftragnehmer

Die vertraglich vereinbarten Leistungen werden unter Einschaltung von folgenden Unterauftragnehmern durchgeführt, die in diese Verarbeitung mit einbezogen sind (Angabe Name, Rechtsform, Kontaktdaten und ladungsfähige Anschrift der Unterauftragnehmer):

| Name, Anschrift, Kontaktdaten | Auftragsinhalt |
|---|---|
| SCHIFFL group Holding GmbH & Co. KG<br>Leverkusenstraße 54<br>22761 Hamburg | Bereitstellung C5 Testat Anforderungen Infrastruktur KI-Dienste |
| Hetzner Online GmbH<br>Industriestraße 25<br>91710 Gunzenhausen | Bereitstellung Server |
| Microsoft Deutschland GmbH<br>Walter-Gropius-Straße 5<br>80807 München | Bereitstellung Infrastruktur KI-Dienste |
| Strato AG<br>Otto-Ostrowski-Straße 7<br>10249 Berlin | E-Mail und Webspace Hosting |
| Google Ireland Limited<br>Gordon House, Barrow Street<br>Dublin 4, Irland | LLM Sprachmodell |
| Microsoft Deutschland GmbH<br>Walter-Gropius-Straße 5<br>80807 München | LLM Sprachmodell |
| Mistral AI<br>15 Rue del Halles<br>75001 Paris, Frankreich | LLM Sprachmodell |

Hetzner Online-GmbH, Microsoft Deutschland GmbH und Strato AG sind Dienstanbieter im Sinne von § 5 DDG. Die eingegebenen Daten werden nicht zu Trainingszwecken des LLM verwendet.

Copyright actago GmbH, 2026

# A.3 Anlage 3 – Technische und organisatorische Maßnahmen

Im Folgenden werden die auftragsbezogenen technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

# 1.Vertraulichkeit

## 11.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen zu verwehren. Nachfolgende Maßnahmen werden von uns umgesetzt, um diese Vorgabe zu erfüllen:

| Technische Maßnahmen | Anmerkungen |
|---|---|
| ☐ Alarmanlage zum Schutz der Außenhülle | |
| ☐ Chipkarten- / Transpondersysteme | |
| ☒ Manuelles Schließsystem | Schlüsselkarte |
| ☒ Sicherheitsschlösser | |
| ☐ Schließsystem mit Codesperre | |
| ☐ Absicherung der Gebäudeschächte | |
| ☐ Türen mit Knauf an der Außenseite | |
| ☐ Sicherheitsglas in allen Fenstern, die einen einfachen Zutritt von außen ermöglichen | |
| ☐ Verwendung von Fensterschlössern | |

| Organisatorische Maßnahmen | Anmerkungen |
|---|---|
| ☒ Schlüsselregelung / Liste | |
| ☒ Besucher in Begleitung der Mitarbeiter | |
| ☒ Besucherbuch / Protokoll der Besucher | Zutrittsprotokollierung im Rechenzentrum |
| ☒ Sorgfalt bei Auswahl der Reinigungsdienste | |
| ☐ Zentrales Schließsystem | |
| ☒ Umgehende Meldung von Schlüsselverlusten | |
| ☒ Umgehende Sperrung von Schlüsseln oder Austausch von Schlössern im Verlustfall | |
| ☒ Umgehende Meldung von Einbrüchen an die Geschäftsleitung und/oder die Polizei | |
| ☒ Jährliche Neubewertung und ggf. Anpassung des Konzeptes und der Maßnahmen zur Zutrittskontrolle | |
| ☒ Räume und Schränke inkl. Fenster mit personenbezogenen Daten sind bei Abwesenheit der Mitarbeiter grundsätzlich verschlossen | |

## 11.2 Zugangskontrolle

Die Nutzung der Datenverarbeitungsanlagen (Computer-Arbeitsplätze, mobile IT-Systeme, Spezialanwendungen) durch Unbefugte ist zu verhindern. Nachfolgende Maßnahmen werden von uns umgesetzt, um diese Vorgabe zu erfüllen:

| Technische Maßnahmen | Anmerkungen |
|---|---|
| ☒ Login mit Benutzername + Passwort | |
| ☒ Anti-Virensoftware auf Servern | Regelmäßige Aktualisierung und Überprüfung |
| ☒ Anti-Virensoftware auf Clients | Regelmäßige Aktualisierung und Überprüfung |
| ☒ Anti-Viren-Software auf mobilen Geräten | |
| ☒ Firewall | |
| ☒ Mobile Device Management (MDM) | |
| ☒ VPN-Einwahl bei Remote-Zugriffen | |
| ☒ Verschlüsselung von Datenträgern | |
| ☒ Verschlüsselung Chat-Historien und hochgeladenen Dokumenten im Ruhezustand | |
| ☒ Verschlüsselung von Laptops | |
| ☒ Verschlüsselung von Smartphones | |
| ☐ Gehäuseverriegelung | |
| ☒ BIOS-Passwort | |
| ☐ Sperre externer Schnittstellen (USB) | |
| ☒ Automatische Desktopsperre mit Passwortabfrage | |

| Organisatorische Maßnahmen | Anmerkungen |
|---|---|
| ☒ Verwaltung von Benutzerberechtigungen | Rollenbasierte Zugriffssteuerung |
| ☒ Erstellen von Benutzerprofilen | |
| ☐ Zentrale Passwortvergabe | |
| ☒ IT-Dienstanweisung | |
| ☐ Datenschutzgeschäftsordnung | |
| ☒ Anleitung „Manuelle Desktopsperre“ | |
| ☒ Umsetzung einer Passwortrichtlinie<br>☒ Länge = mindestens 12 Zeichen<br>☒Komplexität (Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen) | nach BSI-Standards mit regelmäßigen Änderungen und Mindestanforderungen |
| ☒ Kleiner Personenkreis mit Administratorrechten | |
| ☒Einsatz eines Passwort-Managers (z.B. KeePass) | |
| ☒ Zweifaktor-Authentifizierung | für alle administrativen und sensiblen Zugänge |

Copyright actago GmbH, 2026

## 11.3 Zugriffskontrolle

Es ist sicherzustellen, dass jeder Beschäftigte nur Zugriff auf die personenbezogenen Daten hat, zu dem er aufgrund seines konkreten Aufgabenbereiches berechtigt ist. Nachfolgende Maßnahmen werden von uns umgesetzt, um diese Vorgabe zu erfüllen:

| Technische Maßnahmen | Anmerkungen |
|---|---|
| ☒ Aktenshredder (mind. Stufe P4 – Crosscut) | |
| ☐ Externer Aktenvernichtungsdienstleister ( Stufe P4 nach DIN 66399 zertifiziert) | |
| ☒ Physische Löschung / mechanische Vernichtung von Datenträgern | |
| ☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten | |
| ☒ Zugriff auf Netzwerk des Verantwortlichen im Home-Office nur über VPN-Verbindung | |

| Organisatorische Maßnahmen | Anmerkungen |
|---|---|
| ☒ Einsatz von Berechtigungskonzepten | |
| ☒ Minimale Anzahl an Administratoren | |
| ☐ Datenschutztresor | |
| ☒ Verwaltung der Benutzerrechte durch Administratoren | |
| ☒ Home-Office Richtlinie oder Home-Office Vereinbarung | |
| ☒ Regelmäßige Prüfung der Berechtigungen auf Aktualität | |
| ☒ Sofortige Sperrung von Konten, wenn ein Mitarbeiter ausscheidet | |

## 11.4 Trennungskontrolle

Es ist sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann durch logische und physikalische Trennung der Daten gewährleistet werden. Nachfolgende Maßnahmen werden von uns umgesetzt, um diese Vorgabe zu erfüllen:

| Technische Maßnahmen | Anmerkungen |
|---|---|
| ☒ Physikalische Trennung (Systeme / Datenbanken / Datenträger) | |
| ☐ Mandantenfähigkeit relevanter Anwendungen | |
| ☒ Trennung von Produktiv- und Testumgebung | |

| Organisatorische Maßnahmen | Anmerkungen |
|---|---|
| ☒ Steuerung über Berechtigungskonzept | |
| ☒ Festlegung von Datenbankrechten | |
| ☒ Datensätze sind mit Zweckattributen versehen | |

## 11.5 Pseudonymisierung

Die Verarbeitung von personenbezogenen Daten soll in einer Weise erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden. Nachfolgende Maßnahmen werden von uns umgesetzt, um diese Vorgabe zu erfüllen:

| Technische Maßnahmen | Anmerkungen |
|---|---|
| ☒ Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesichertem System (möglichst verschlüsselt) | |

| Organisatorische Maßnahmen | Anmerkungen |
|---|---|
| ☒ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu pseudonymisieren oder anonymisieren. | automatisierter Prozess |
| ☒ Verwendung von Kennziffern für Kunden oder Personal anstelle der Namen | |

# 12 Integrität

## 12.1 Weitergabekontrolle

Es ist sicherzustellen, 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. Zudem muss überprüft und festgestellt werden können, an welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Nachfolgende Maßnahmen werden von uns umgesetzt, um diese Vorgabe zu erfüllen:

| Technische Maßnahmen | Anmerkungen |
|---|---|
| ☐ Nutzung von Signal oder Threema als Messengerdienst (kein WhatsApp) | |
| ☐ E-Mail-Verschlüsselung<br>☒ VPN-Übertragung | |
| ☒ Protokollierung von Zugriffen und Abrufen | |
| ☐ Sichere Transportbehälter (verschließbar) und Diebstahlschutz bei Fahrzeugen | |
| ☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https | End-to-End-Verschlüsselung für sensible Daten |
| ☐ Nutzung von Signaturverfahren | |

| Organisatorische Maßnahmen | Anmerkungen |
|---|---|
| ☒ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen | |
| ☐ Übersicht regelmäßiger Abruf- und Übermittlungsvorgänge | |
| ☒ Weitergabe in anonymisierter oder pseudonymisierter Form | |

| | |
|---|---|
| ☐ Sorgfalt bei Auswahl von Transportpersonal und Fahrzeugen | |
| ☐ Schriftliche Regelung, über welche Medien welche Daten in welcher Form übermittelt werden | |
| ☒ Persönliche Übergabe mit Protokoll | |
| ☒ Überwachung von Fernwartung | |

## 12.2 Eingabekontrolle

Es muss nachträglich geprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Nachfolgende Maßnahmen werden von uns umgesetzt, um diese Vorgabe zu erfüllen:

| Technische Maßnahmen | Anmerkungen |
|---|---|
| ☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten | |
| ☐ Manuelle oder automatisierte Kontrolle der Protokolle | |

| Organisatorische Maßnahmen | Anmerkungen |
|---|---|
| ☒ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können. | |
| ☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen | |
| ☒ Vergabe von Rechten zur Eingabe, Änderungen und Löschung von Daten als Bestandteil eines Berechtigungskonzeptes | |
| ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen werden | |
| ☒ Klare Zuständigkeiten für Löschungen | |

# 13 Verfügbarkeit und Belastbarkeit

## 13.1 Verfügbarkeitskontrolle

Es ist sicherzustellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Nachfolgende Maßnahmen werden von uns umgesetzt, um diese Vorgabe zu erfüllen:

| Technische Maßnahmen | Anmerkungen |
|---|---|
| ☒ Feuer- und Rauchmeldeanlagen | |
| ☐ $CO_2$-Feuerlöscher im Serverraum | |
| ☒ Schaum-Feuerlöscher in Registratur / Archiv | |
| ☒ Keine oder durch Vergitterung (bzw. gleichwertigen Mechanismus) geschützte Fenster in Registratur / Archiv | |
| ☒ Überwachung von Feuchtigkeit in Registratur / | |

| | |
|---|---|
| Archiv | |
| ☐ Überwachung von Temperatur und Feuchtigkeit im Serverraum | |
| ☒ Klimatisierung des Serveraums | |
| ☒ Einsatz einer USV (Unterbrechungsfreie Stromversorgung) | |
| ☒ Regelmäßiger Test der USV | |
| ☒ Schutzsteckdosenleisten im Serverraum | |
| ☒ Eigener Stromkreis für den Serverraum | |
| ☐ Serverraum ohne Fenster oder Fenster vergittert mit UV-Folie | |
| ☒ Brandschutztür und Brandabschottung im Serverraum | |
| ☐ Datenschutztresor | |
| ☒ Raid System (Mind. Raid 5 oder Raid 6) | |
| ☐ Videoüberwachung Serverraum | |
| ☒ Regelmäßige Software-Updates<br>☐ Manuell<br>☒ Automatisch | |
| ☒ System-Monitoring | |

| **Organisatorische Maßnahmen** | **Anmerkungen** |
|---|---|
| ☒ Backup & Recovery Konzept (ausformuliert) | Regelmäßige Datensicherung und Verschlüsselung der Backup-Daten, redundanter Betreib und automatisierte Failover-Mechanismen, Mehrstufiges Go-Live-Konzept, Mechanismen zur Erkennung und Verhinderung von Datenmanipulationen, Implementierung von Disaster-Recovery-Strategien |
| ☒ Kontrolle der Datensicherungen | |
| ☒ Regelmäßige (halbjährliche) Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse | |
| ☐ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums | |
| ☐ Keine Aufbewahrung von Brandlasten (Papier, Kartonagen, Holzmöbel) im Serverraum | |
| ☐ Keine oder inaktivierte sanitären Anschlüsse im oder oberhalb des Serverraums | |
| ☒ IT-Notfallplan und IT-Sicherheitskonzept | |
| ☒ Getrennte Partitionen für Betriebssysteme und Daten | |
| ☐ Standorttrennung | |
| ☐ Monitoring und Reporting der Backups | |
| ☒ Zutritt zum Serverraum nur für kleinen Personenkreis (GL, IT, Technik) | |

# 14 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

## 14.1 Datenschutzmaßnahmen

| Technische Maßnahmen | Anmerkungen |
|---|---|
| ☐ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf (z.B. Wiki, Intranet, …) | |
| ☐ Etabliertes ISMS | |
| ☒ Jährliche Überprüfung der Wirksamkeit der technischen Maßnahmen | |

| Organisatorische Maßnahmen | Anmerkungen |
|---|---|
| ☒ Externer Datenschutzbeauftragter | |
| ☒ Mitarbeiter sind sensibilisiert und schriftlich auf Vertraulichkeit verpflichtet | |
| ☒ Regelmäßige Sensibilisierung der Mitarbeiter mindestens jährlich | |
| ☒ Interner / externer Informationssicherheitsbeauftragter | |
| ☒ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt | |
| ☒ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach | |
| ☒ Formaler Prozess zur Bearbeitung von Auskunftsanfragen oder Datenschutzbeschwerden seitens Betroffener ist vorhanden | |

## 14.2 Reaktion auf Sicherheitsverletzungen

| Technische Maßnahmen | Anmerkungen |
|---|---|
| ☒ Einsatz von Firewall mit regelmäßiger Aktualisierung (Server, Client) | |
| ☒ Einsatz von Spamfilter und regelmäßige Aktualisierung | |
| ☒ Einsatz von Virenscannern und regelmäßige Aktualisierung (Server, Client) | |

| Organisatorische Maßnahmen | Anmerkungen |
|---|---|
| ☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber der Aufsichtsbehörde) | |
| ☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen | |
| ☒ Einbindung von ☒ DSB und ☐ ISB in Sicherheitsvorfälle und Datenpannen | |

Copyright actago GmbH, 2026

| | |
|---|---|
| ☒ Dokumentation von Sicherheitsvorfällen und Datenpannen | |
| ☒ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen | |

## 14.3 Datenschutzfreundliche Voreinstellungen (Privacy by design / Privacy by default)

| Technische Maßnahmen | Anmerkungen |
|---|---|
| ☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweckerforderlich sind | |
| ☐ Einfache Ausübung des Widerrufs- und Widerspruchsrechts des Betroffenen durch technische Maßnahmen | |

| Organisatorische Maßnahmen | Anmerkungen |
|---|---|
| ☒ Datenschutzfreundliche Voreinstellungen in den Datenverarbeitungssystemen von Dienstleistern werden entsprechend umgesetzt und beibehalten | |
| ☒ Datenschutzfreundliche Voreinstellungen in eigenen Datenverarbeitungssystemen werden entsprechend umgesetzt und beibehalten | |

## 14.4 Auftragskontrolle

Es ist sicherzustellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Aufraggebers verarbeitet werden können.

| Organisatorische Maßnahmen | Anmerkungen |
|---|---|
| ☐ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation | |
| ☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten in Bezug auf Datenschutz und Datensicherheit | |
| ☒ Abschluss der notwendigen Vereinbarungen zur Auftragsvereinbarung (AVV) mit<br>☒ IT-Dienstleistern<br>☒ Softwareanbietern<br>☒ Webhostern<br>☐ ggf. Entsorgungsunternehmen | Einbindung des DSB |
| ☒ Schriftliche Weisungen an den Auftragnehmer | |
| ☒Benennung eines Datenschutzbeauftragten durch den Auftragnehmer, sofern dieser einer Benennungspflicht unterliegt | |
| ☒ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer | |

| | |
|---|---|
| ☒ Regelung zum Einsatz weiterer Subunternehmer | |
| ☒ Sicherstellung der Vernichtung oder Rückgabe von Daten und Datenträgern nach Beendigung des Auftrags | |
| ☐ Bei längerer Zusammenarbeit:<br>Regelmäßige Überprüfung des Auftragnehmers und seines Schutzniveaus (mind. jährlich) | |

# A.4 Zusatz für Berufsgeheimnisträger

zwischen der

**[Name]**
[Straße, Hausnummer]
[PLZ Ort]

**-Auftraggeber-**

und der

**H24 GmbH**
Ledererzeile 48
83512 Wasserburg am Inn

**-Auftragnehmer-**

## 1 Zweck und Geltungsbereich

(1) Dieser Zusatz gilt ergänzend zum Auftragsverarbeitungsvertrag (AVV) und regelt die besonderen Anforderungen an die Datenverarbeitung für Berufsgeheimnisträger im Sinne von § 203 StGB (z.B. Rechtsanwälte, Ärzte, Steuerberater) sowie vergleichbare Berufsgruppen, die der beruflichen Verschwiegenheitspflicht unterliegen.

(2) Der Zusatz stellt sicher, dass die besonderen Anforderungen an die Vertraulichkeit, den Schutz und die Integrität von Berufsgeheimnissen im Rahmen der Nutzung der browserbasierten LLM-Plattform des Auftragnehmers eingehalten werden.

## 2 Vertraulichkeit und Datenzugriff

(1) Der Auftragnehmer verpflichtet sich, die ihm anvertrauten Berufsgeheimnisse streng vertraulich zu behandeln. Dies umfasst alle Daten und Informationen, die der Auftraggeber oder dessen Mitarbeiter in Ausübung ihres Berufs oder Mandats an den Auftragnehmer übermitteln.

(2) Der Auftragnehmer stellt sicher, dass alle mit der Verarbeitung von dem Berufsgeheimnis unterliegenden Daten des Auftraggebers befassten Beschäftigten, die damit befasst sind, sich in Textform dazu verpflichtet haben, die ihnen bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenen Berufsgeheimnisse nicht unbefugt zu offenbaren und sie über die mögliche Strafbarkeit nach § 203 Abs. 4 StGB belehrt wurden. Die Pflicht zur Verschwiegenheit erstreckt sich nicht nur auf fremde Geheimnisse, sondern auf alle Tatsachen, die Ihren Mitarbeitern in Ausübung oder aus Anlass ihrer Tätigkeit anvertraut oder bekannt werden.

(3) Die Pflicht zur Verschwiegenheit besteht gegenüber jedermann, so auch gegenüber Familienangehörigen, gegenüber Arbeitskollegen, soweit eine Offenbarung nicht aus dienstlichen Gründen erforderlich ist, sowie auch gegenüber demjenigen, der von der betreffenden Tatsache bereits Kenntnis erlangt hat.

(4) Die Pflicht zur Verschwiegenheit besteht auch nach Beendigung der Beauftragung uneingeschränkt und zeitlich unbefristet fort.

(5) Der Auftragnehmer stellt durch technische und organisatorische Maßnahmen sicher, dass die verarbeiteten Daten nicht unbefugt eingesehen, geändert oder an Dritte weitergegeben werden.

Copyright actago GmbH, 2026

# 3 Verbot der Weiterverarbeitung

(1) Der Auftragnehmer sichert zu, dass die im Rahmen dieses Vertrags verarbeiteten Berufsgeheimnisse nicht zu eigenen Zwecken oder zu Zwecken Dritter verarbeitet werden.

(2) Eine Nutzung der Daten zu Forschungszwecken oder zur Verbesserung der zugrunde liegenden Sprachmodelle ist ausdrücklich ausgeschlossen.

# 4 Kontrolle und Nachweis

(1) Der Auftragnehmer ermöglicht dem Auftraggeber jederzeit, die Einhaltung der Verpflichtungen aus diesem Zusatz zu kontrollieren. Hierzu gehören insbesondere Audits und Einsichtnahmen in die entsprechenden Dokumentationen.

(2) Der Auftragnehmer dokumentiert alle Maßnahmen, die zur Einhaltung dieses Zusatzes getroffen wurden, und stellt diese dem Auftraggeber auf Anfrage zur Verfügung.

# 5 Haftung und Schadensersatz

(1) Der Auftragnehmer haftet für alle Schäden, die dem Auftraggeber durch eine Verletzung der Vertraulichkeit oder durch einen Verstoß gegen die besonderen Verpflichtungen dieses Zusatzes entstehen.

(2) Der Auftragnehmer stellt den Auftraggeber von allen Ansprüchen frei, die durch eine Verletzung der Verschwiegenheitspflichten des Auftragnehmers oder seiner Mitarbeiter entstehen.

# 6 Schlussbestimmungen

(1) Dieser Zusatz bildet einen integralen Bestandteil des Auftragsverarbeitungsvertrags und ergänzt diesen.

(2) Änderungen dieses Zusatzes bedürfen der Schriftform.

(3) Sollten einzelne Bestimmungen dieses Zusatzes unwirksam sein, berührt dies die Wirksamkeit des übrigen Zusatzes nicht.

**Auftragnehmer:**

| | |
|---|---|
| Ort, Datum | Unterschrift (Vor- und Nachname) |

**Auftraggeber:**

| | |
|---|---|
| Ort, Datum | Unterschrift (Vor- und Nachname) |

Copyright actago GmbH, 2026