Auftragsverarbeitungsvertrag – Thax Software GmbH

(Fassung vom 26.10.2026)

Diese Auftragsverarbeitungsbedingungen gelten zwischen unseren Kunden
– Verantwortlicher bzw. Auftraggeber –

und uns, der Thax Software GmbH
– Auftragsverarbeiter bzw. Auftragnehmer –,

so weit von uns personenbezogene Daten im Auftrag des Kunden verarbeitet werden.

Präambel

Die Vertragsparteien sind ein Vertragsverhältnis über die Lieferung, Konfiguration und Wartung von EDV-Systemen, Lizenzen, Soft- und Hardware sowie Support und Schulungen dafür eingegangen. Soweit in diesem Rahmen personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet werden, wird für die Auftragsverarbeitung ergänzend nach Art. 28 Datenschutzgrundverordnung (DSGVO) wie folgt geregelt:

1. Umfang und Gegenstand der Beauftragung und Verarbeitung

a) Der Auftragsverarbeiter ist von dem Verantwortlichen mit der Erstellung und Lieferung von Büromanagementsystemen (Soft- und Hardware für den Einsatz im Büro, z. B. für das Kunden-, Dokumenten-, Diktat- oder Inventarmanagement und für Spracherkennung und/oder KI-Dokumentationslösungen) sowie ggf. deren Wartung und Support beauftragt.
Zudem ist der Auftragsverarbeiter ggf. von dem Verantwortlichen mit der Lieferung und Wartung von Spracherkennungssoftware und/oder LLM-gestützter KI-Dokumentationslösungen als „Soft-ware as a Service“ (SaaS) oder Lizenzen hierfür beauftragt.

b) Der Auftragnehmer verarbeitet die Auftraggeber-Daten im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 28 DSGVO (Auftragsverarbeitung). Der Auftraggeber bleibt Verantwortlicher im datenschutzrechtlichen Sinn.

c) Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer findet grundsätzlich innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Es ist dem Auftragnehmer gleichwohl gestattet, Auftraggeber-Daten unter Einhaltung der Bestimmungen dieses Vertrags auch außerhalb des EWR zu verarbeiten, wenn die Voraussetzungen der Art. 44-48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt.

2. Kategorien betroffener Personen

a) Anwender der vom Auftragsverarbeiter gelieferten und/oder betreuten Systeme, die für den Verantwortlichen tätig sind (z. B. Mitarbeiter) – folgend Anwender genannt –

b) EDV-/IT-Betreuer, Lieferanten oder sonstige Dienstleister des Verantwortlichen, mit denen seitens des Auftragsverarbeiters zur Vertragserfüllung eine Zusammenarbeit notwendig ist – folgend IT-Dienstleister genannt –

c) Personen, deren personenbezogenen Daten von dem Auftragsverarbeiter für den Verantwortlichen verarbeitet werden, beispielsweise Kunden, Mandanten, Patienten, Beteiligte, sonstige Lieferanten, sonstige Dienstleister, Verfahrensgegner sowie von den Vorgenannten deren Vertreter – folgend zusammen Dritte genannt –

– folgend zusammen betroffene Personen genannt –.

3. Art, Zweck und Umfang der Datenverarbeitung

a) Insbesondere im Rahmen des Supports, zum Zwecke der Installation von Programmen und Up-dates dafür und zum Zwecke der Software- und Hardwarekonfiguration erhält der Auftragsverarbeiter Zugang zu den Computersystemen des Verantwortlichen, ggf. auch über einen Fernzugriff via Internet. Für eine Fehleranalyse können Fernwartungssitzungen aufgezeichnet werden. Hierin können personenbezogene Daten betroffener Personen enthalten sein.

b) Zum Zwecke einer Fehleranalyse, einer Datenrettung oder zur Anpassung von Spracherkennungsprofilen kann der Auftragsverarbeiter digitale Dokumente und Diktate erhalten, welche personenbezogene Daten betroffener Personen enthalten.

c) Zum Zwecke der Fehleranalyse kann der Auftragsverarbeiter Log-Dateien erhalten, in welchen personenbezogene Daten von Anwendern enthalten sind, beispielsweise Benutzernamen.

d) Zum Zwecke der Konfiguration und Personalisierung von Geräten oder ID-Karten kann der Auftragsverarbeiter Namen von Anwendern erhalten.

e) Zum Zwecke der Erstellung von Angeboten, Planung von Installationen und Schulungen, Vertragsausführung, Nachvollziehbarkeit

   i. kann der Auftragsverarbeiter Namen und geschäftliche Kontaktdaten von Anwendern und IT-Dienstleistern erhalten

   ii. dokumentiert der Auftragsverarbeiter als Kundenhistorie seine Tätigkeiten in seiner elektro-nischen oder physischen Kundenakte. Hierbei werden i.d.R. auch der Name und ggf. geschäftliche Kontaktdaten / Kommunikationsdaten (z. B. Telefon, E-Mail) des Anwenders, für den die Dienstleistung (z. B. Support) erbracht worden ist, und ggf. des IT-Dienstleisters notiert.

   iii. dokumentiert der Auftragsverarbeiter Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

   iv. dokumentiert der Auftragsverarbeiter Vertragsabrechnungs- und Zahlungsdaten.

f) Im Falle der Lieferung von KI-Spracherkennung bzw. KI-Dokumentationslösungen als SaaS: Der Unterauftragnehmer des Auftragnehmers betreibt, trainiert und wartet für den Auftraggeber eine Software-as-a-Service-Anwendung, die insbesondere:

   i. (Umgebungs-)Unterhaltungen erfasst und transkribiert;

   ii. Echtzeitdiktate, u. a. von Memos oder Vorlageninhalten, geschäftlichem, auch juristischem Inhalt, medizinischen Befunden, mithilfe von Sprache-zu-Text erstellt;

   iii. Entwurfsdokumente erstellt, so z. B. im Falle von medizinischer KI-Dokumentation klinische Befunde oder Überweisungsschreiben;

   iv. LLM-gestützte Zusammenfassung eines Textes; im Falle von medizinischer KI-Dokumentation auch eines umfangreichen Befunds in eine prägnante Nachsorgezusammenfassung, erstellt;

   v. im Falle von medizinischer KI-Dokumentation Empfehlungen erstellt, so z. B. für einzelne Anordnungen, Erkrankungen und andere klinische Daten wie Flussdiagramme, narrative Notizen und Notizen zu Zwischenfällen und

   vi. Informationsleitfäden erstellt, so z. B. zusammengefasste, kontextbezogene, klinisch relevante Informationen aus vertrauenswürdigen internen und glaubwürdigen externen Quellen innerhalb des Dokumentationsprozesses.

g) Im Falle der Lieferung von KI-Spracherkennung bzw. KI-Dokumentationslösungen als SaaS: Personenbezogene Daten werden im Rahmen des Betriebs der Anwendung vom Unterauftragnehmer des Auftragnehmers verarbeitet, so z. B.

   i. zum Erfassen und Transkribieren von Gesprächen (im Falle von medizinischer KI-Dokumentation auch Arzt/Patienten-Gespräche) oder Diktaten;

   ii. zum Zusammenfassen und/oder Aufbereiten von Informationen und Unterlagen aus der Dokumentation;

   iii. im Falle von medizinischer KI-Dokumentation: zum Erstellen von Befunden und Empfehlungen und

   iv. zur Recherche und Auswertungen von Informationen.

h) Insbesondere, aber nicht ausschließlich, im Falle der Lieferung von Spracherkennungssoftware und KI-Dokumentationslösungen als SaaS findet die Verarbeitung von Daten auch auf Servern eines Unter-Auftragsverarbeiters statt. Nr. 1c gilt entsprechend.

i) In einer Anlage – mit Angaben zu Zweck, Art und Umfang – können weitere Verarbeitungen von Auf-traggeber-Daten nach diesem Vertrag spezifiziert werden, z. B. für eine eventuelle Verarbeitung von Daten zwecks Trainings und Weiterentwicklung der KI-/LLM-Modelle.

4. Art der personenbezogenen Daten

a) Stammdaten wie Namen und geschäftliche Kontakt-daten von Anwendern und IT-Dienstleistern

b) Personenbezogene Daten von Dritten, die von dem Auftragsverarbeiter für den Verantwortlichen verarbeitet werden.

Die Daten können ggf. folgenden Geheimnis-schutzregeln unterliegen: Berufsgeheimnis nach § 203 StGB, Bankgeheimnis, Fernmeldegeheimnis nach dem TKG und TMG, Sozialgeheimnis oder Sonstiges. Sollte dies der Fall sein, informiert der Verantwortliche den Auftragsverarbeiter schriftlich.

c) Kommunikationsdaten (z. B. Zugriff auf die Anwendung)

d) Authentifizierungsdaten (z. B. Benutzername, Kennwort oder PIN-Code)

e) Vertragsdaten (z. B. Endkunde, Produkt)

f) Abrechnungsdaten (z. B. Zahlungsdaten)

g) Schulungsdaten (z. B. Teilnehmer), sofern im Einzelfall beauftragt

h) im Falle der Beauftragung von Spracherkennungs-software und KI-Dokumentationslösungen als SaaS: Gesprächs-/Audiodaten (z. B. Transkriptionen und Diktate)

i) im Falle der Beauftragung medizinischer KI-Dokumentationslösungen: Gesundheitsdaten (z. B. Behandlungsdaten, Befunde).

5. Verantwortlichkeiten, Pflichte und Rechte der Vertragsparteien

a) Der Auftragsverarbeiter verarbeitet vom Verantwortlichen erhaltene personenbezogene Daten der betroffenen Personen nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, der Auftragsverarbeiter ist nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtliche Anforderung vor der Verarbeitung mit, sofern eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt ist.

b) Der Auftragsverarbeiter verwendet die im Rahmen der Verarbeitung überlassenen oder zur Kenntnis gelangten personenbezogenen Daten nur soweit dies zur Vertragserfüllung erforderlich ist; eine Verwendung für sonstige eigene Zwecke erfolgt nicht.

c) Der Auftragsverarbeiter gewährleistet, dass sich die in seiner Verantwortung tätigen zur Verarbeitung der personenbezogenen Daten Befugten zur Vertraulichkeit verpflichtet haben.

d) Der Auftragsverarbeiter sichert zu, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet.

e) Der Auftragsverarbeiter sichert zu, dass alle gemäß Art. 32 DSGVO erforderlichen Maßnahmen ergriffen sind, insbesondere, dass – unter Berücksichtigung des Stands der Technik, der Implementierungs–kosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der jeweiligen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen – geeignete technische und organisatorische Maßnahmen getroffen sind, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Anlage 2).

f) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

g) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Haupt-leistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers, auch bei ausgelagerten Nebenleistungen, angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Der Verantwortliche stimmt der Beauftragung der in der Anlage 1 genannten Unter-Auftragsverarbeiter unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO. zu.

Der Verantwortliche erteilt die vorherige allgemeine Genehmigung für die Inanspruchnahme weiterer Auftragsverarbeiter gem. Art. 28 II, S. 1, 2. Alt. DSGVO, jedoch nur, sofern hiervon nicht das Berufsgeheimnis gem. 4b betroffen ist, über das der Verantwortliche den Auftragsverarbeiter schriftlich informiert hat. Der Auftragsverarbeiter informiert den Verantwortlichen über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit des Einspruchs erhält. Der Auftragsverarbeiter weist bereits jetzt da-rauf hin, dass im Einspruchsfall eine Auftragsaus-führung eventuell nicht mehr gewährleistet werden kann. Erhebt der Auftraggeber Einspruch, ist der Auftragnehmer berechtigt, den Hauptvertrag und diesen Vertrag mit einer Frist von drei (3) Monaten zu kündigen.

Der Auftragsverarbeiter erlegt jedem Unter-Auftragsverarbeiter vertraglich dieselben Daten-schutzpflichten auf, die ihm selber nach diesem Vertrag obliegen, insbesondere muss hinreichende Garantie dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSG-VO erfolgt. Kommt der weitere Unter-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes Unter-Auftragsverarbeiters.

Der Verantwortliche willigt insbesondere ein, dass weitere Auftragsverarbeiter in Anspruch genommen werden, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, insbesondere:

i. dass der Auftragsverarbeiter zur Kundenbetreuung (Beratung, Angebotserstellung, Auftragsabwicklung) externe Vertriebsbeauftragte einsetzt

ii. 1. dass der Auftragsverarbeiter, sofern er benutzerbezogen zu lizenzierende Softwareprodukte einkauft und an den Verantwortlichen weiterverkauft, Namen, geschäftliche Anschriften und geschäftliche E-Mail-Adressen von Anwendern an die Lieferanten dieser Softwareprodukte weitergibt, soweit zur Auftragserfüllung notwendig, oder 2. dass der Auftragsverarbeiter, sofern zur Lizenzierung oder Auslieferung von Produkten, die der Auftragsverarbeiter einkauft und an den Verantwortlichen weiterverkauft, notwendig, Name und geschäftliche Kontaktdaten eines Ansprechpartners des Verantwortlichen an die Lieferanten weitergibt. Die Lieferanten dürfen ihrerseits unter Einhaltung der Vorschriften der DSGVO:

- Unter-Auftragsverarbeiter einsetzen, auch außerhalb des Europäischen Wirtschaftsraumes
- diese Daten, soweit zur Auftragserfüllung notwendig, an die Hersteller der zu lizenzierenden Softwareprodukte, auch außerhalb des Europäischen Wirtschaftsraumes, weitergeben.

iii. dass der Auftragsverarbeiter im Einzelfall Kontaktdaten des Verantwortlichen, seiner Mitarbeiter oder IT-Dienstleister an den Lieferanten eines supporteten Produkts weitergibt, damit dieser zur Lösung eines Supportfalls den Verantwortlichen, seine Mitarbeiter oder IT-Dienstleister direkt kontaktieren kann.

iv. dass der Auftragsverarbeiter und der Verantwortliche eine Korrespondenz per E-Mail führen, die ggf. unverschlüsselt ist, kein sicherer Übertragungsweg ist und ggf. über externe Dienstleister erfolgt. Daten, die einem Berufs-geheimnis unterliegen, dürfen auf diesem Wege nicht übermittelt werden.

v. dass der Auftragsverarbeiter zum Durchführen einer Fernwartung ein Fernwartungssystem eines externen Dienstleisters verwendet, sofern die Verbindungen über gesicherte und verschlüsselte Datenkanäle erfolgen, die auch vom Dienstleister nicht ausgelesen werden können (Ende-zu-Ende-Verschlüsselung).

h) Der Auftragsverarbeiter unterstützt den Verantwortlichen angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel 3 der DSGVO genannten Rechte der betroffenen Person nachzukommen.

i) Der Auftragsverarbeiter unterstützt unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in Art. 32 - 36 der DSGVO genannten Pflichten, insbesondere bzgl. der Sicherheit der Verarbeitung, der Meldung von Datenschutzverletzungen, der Benachrichtigung der betroffenen Person, ggf. der Datenschutzfolgen–

abschätzung sowie der vorherigen Konsultation. Insbesondere werden Verletzungen des Schutzes personenbezogener Daten, die den Verantwortlichen betreffen, im Hinblick auf ggf. bestehende Meldepflichten sofort dem Verantwortlichen mitgeteilt.

j) Grundsätzlich löscht der Auftragsverarbeiter nach Abschluss der Verarbeitung alle personenbezogenen Daten, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung besteht.

Jedoch dürfen die zum unter 3f genannten Zweck erhobenen Daten vom Auftragsverarbeiter so lang gespeichert werden wie:

- das Vertragsverhältnis besteht und
- Schadenersatzansprüche, zu deren Abwehr die Dokumentation notwendig sein könnte, gegen den Auftragsverarbeiter geltend gemacht werden könnten.

k) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der im Zusammenhang mit der Auftragsverarbeitung bestehenden gesetzlichen Verpflichtungen zur Verfügung und ermöglicht Über-prüfungen – einschließlich Inspektionen –, die von dem Verantwortlichen oder einem anderen von ihm beauftragten Prüfer durchgeführt werden, und trägt dazu bei. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

l) Der Verantwortliche und deren Anwender und IT-Dienstleister ermöglichen dem Auftragsverarbeiter Einblick in Daten nur, sofern dies für die Erbringung der Vertragsleistung erforderlich oder nicht zu vermeiden ist. Beispielsweise sollten vor Beginn einer Fernwartungssitzung von den Anwendern oder IT-Dienstleistern alle nicht benötigten Programmfenster, auch aus Fremdsystemen, in denen personenbezogene Daten oder solche, die einem Berufsgeheimnis unterliegen, sichtbar sind, geschlossen werden. Für Schulungen und zur Fehleranalyse etc. sollten nach Möglichkeit Testdatensätze, welche keine echten solchen Daten enthalten, eingerichtet werden.

m) Unbeschadet der Artikel 82 bis 84 der DSGVO gilt ein Auftragsverarbeiter, der unter Verstoß gegen die DSGVO die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

a) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Auftraggeber-Daten nach Maß-gabe dieses Vertrages Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

b) Ist der Auftragnehmer 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 Auftraggeber verpflichtet, den Auftragnehmer auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

n) Der Auftragnehmer wird die Auftraggeber-Daten nach Beendigung dieses Vertrages löschen, sofern nicht gesetzlich eine Verpflichtung des Auftrag-nehmers zur weiteren Speicherung der Auftraggeber-Daten besteht. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung von Auftraggeber-Daten dienen, dürfen durch den Auftragnehmer auch nach Vertragsende aufbewahrt werden.

6. Weisungsberechtigte und Weisungsempfänger

Weisungsberechtigte Personen des Auftraggebers sind, sofern nicht anders vereinbart, alle Mitarbeiter.

Weisungsempfänger beim Auftragnehmer sind die Geschäftsführung, die Assistenz der Geschäftsführung und die Support-Mitarbeiter.

Weisungen können erteilt werden: telefonisch, per E-Mail, postalisch.

Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre sowohl seitens des Auftraggebers als auch des Auftragnehmers zu dokumentieren. Die Dokumentation darf elektronisch erfolgen.

7. Verantwortliche für den Datenschutz und die Datenverarbeitung

Seitens des Auftragsverarbeiters sind die Verantwortlichen für den Datenschutz und die Datenverarbeitung die Geschäftsführer Marc Bartsch und Thorsten Bartsch. Ein Datenschutzbeauftragter ist nicht bestellt.

8. Vertragsdauer und Kündigung

Der Vertrag ist auf unbestimmte Zeit geschlossen. Er endet automatisch zum Jahresende, wenn drei Jahre lang kein Vertragsverhältnis gemäß Präambel mehr vorliegt und keine Auftragsverarbeitung stattgefunden hat. Zusätzlich kann er jederzeit in Textform ohne Ein-haltung einer Frist gekündigt werden, solange kein Hauptvertrag besteht. Eine isolierte Kündigung dieses Vertrags bei noch bestehendem Hauptvertrag ist ausgeschlossen.

9. Haftung

a) Für die Haftung des Auftragnehmers nach diesem Vertrag gelten die Haftungsausschlüsse und -begrenzungen gemäß dem Hauptvertrag. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.

b) Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von allen etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

10. Schlussbestimmungen

a) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden oder eine Lücke enthalten, so bleiben die übrigen Bestimmungen hier-von unberührt. Die Parteien verpflichten sich, anstelle der unwirksamen Regelung eine solche gesetzlich zulässige Regelung zu treffen, die dem Zweck der unwirksamen Regelung am nächsten kommt und dabei den Anforderungen des Art. 28 DSGVO genügt.

b) Im Fall von Widersprüchen zwischen diesem Vertrag und sonstigen Vereinbarungen zwischen den Parteien, insbesondere dem Hauptvertrag, gehen die Regelungen dieses Vertrags vor.

Auftragsverarbeitungsvertrag – Thax Software GmbH

(Fassung vom 26.10.2026)

Anlage 1: Unter-Auftragsverhältnisse

1. Vertriebsbeauftragter und Unterauftragnehmer für Schulungen

Faustmann UG (haftungsbeschränkt), Stefan G. Faustmann, Bahnhofstraße 47, 65551 Limburg an der Lahn

2. Lieferanten und 2nd- und 3rd-Level-Support

a) Distributor für jegliche Software und 2nd-Level-Support dafür sowie Spracherkennungscloud Bereitstellung als SaaS und 2nd-Level-Support dafür:
EGS Computer Vertrieb GmbH, Steinhof 5a, 40699 Erkrath

b) Softwarehersteller sowie Bereitstellung DMO als SaaS und 3rd-Level-Support für Dragon-Spracherkennung:
Nuance Communications Ireland Limited, 20 Merrion Road, Ballsbridge, Dublin, 4, Irland

c) Softwarehersteller und 3rd-Level-Support für Corti Assistant:
Corti ApS, Kuglegårdsvej 2, 1434 Kopenhagen, Dänemark

d) Distributor von Hardware, insbesondere Headsets, mit Direktlieferung an Kunden im Auftrag und Namen von Thax Software GmbH:
INGRAM MICRO Distribution GmbH, Heisenbergbogen 3, 85609 Dornbach bei München

e) Softwarehersteller sowie Bereitstellung Microsoft Dragon Copilot als SaaS und 3rd-Level-Support für Dragon-Spracherkennung:
Microsoft Ireland Operations Ltd., One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland („Microsoft“)

f) Softwarehersteller und 3rd-Level-Support für Ambivio KI-Dokumentation und Ambivio Voice Legal, Med, Professional:
Ambivio GmbH, Speditionstraße 15A, 40221 Düsseldorf

3. Dienstleister für E-Mail

Microsoft Ireland Operations, Ltd., 70 Sir John Rogerson’s Quay, Dublin 2, Irland

4. Dienstleister für Fernwartung

TeamViewer Germany GmbH, Bahnhofsplatz 2, 73033 Göppingen

Anlage 2: Technische und organisatorische Maßnahmen / Datenschutzkonzept

Der Auftragsverarbeiter sichert zu, dass er die nachfolgend beschriebenen Mindestanforderungen im Rahmen seines Datenschutzkonzeptes einhält. Es beschreibt die im Rahmen der Auftragsverarbeitung erforderlichen Maßnahmen beim Auftragsverarbeiter zum sicheren Umgang mit personenbezogenen Daten. Hierbei orientiert sich der Auftragsverarbeiter im Wesentlichen an den Vorgaben der Artikel 24, 25 und 32 DSGVO. Auf Anforderung weist der Auftragsverarbeiter die Einhaltung entsprechend nach.

1. Vertraulichkeit

a) Zutrittskontrolle:
Die Räume, in denen die Verarbeitung personen-bezogener Daten erfolgt oder Datenverarbeitungsanlagen installiert sind, sind nicht frei zugänglich. Sie sind bei Abwesenheit der Mitarbeiter verschlossen und durch eine Alarmanlage gesichert. Besucher und unternehmensfremde Personen werden innerhalb der Geschäftsräume beaufsichtigt.

b) Zugangskontrolle:
Für jeden Netzwerkbenutzer ist ein persönlich zu-geordneter Benutzer mit einem mindestens 9-stelligen Passwort mit Groß- und Kleinbuchstaben und Ziffern eingerichtet. Beim Fernzugriff auf das Netzwerk des Auftragsverarbeiters erfolgt die Nutzeranmeldung zusätzlich mittels Multi-Faktor-Authentifizierung (Zertifikat, One-Time-Passwort, Benutzeranmeldung und Kennwort). Die Netzwerkbenutzer sind auf die Einhaltung der Benutzerzugangsrichtlinie verpflichtet. Die Einrichtung, Änderung und der Entzug von Zugangsberechtigungen erfolgen in einem dokumentierten Verfahren. Eingerichtete Zugangsberechtigungen werden regelmäßig hinsichtlich ihrer Erforderlichkeit über-prüft. Die Netzwerkzugriffe werden überwacht und protokolliert, dies beinhaltet auch nicht erfolgreiche Anmeldeversuche. Ein Netzwerkzugang wird automatisiert nach spätestens 6 Fehlversuchen systemseitig gesperrt. Die IT-Systeme werden durch Einsatz von Anti-Viren-Software, Software-Firewall und Hardware-Firewall geschützt.

c) Zugriffskontrolle:
Für die Zugriffe auf personenbezogene Daten ist ein dokumentiertes, rollenbasiertes Berechtigungskonzept vorhanden, welches die Zugriffe in der Form einschränkt, dass nur berechtigte Personen auf die für ihre Aufgabe notwendigen personenbezogenen Daten zugreifen können (Minimumprinzip). Die Passwortregelungen aus der Zugangskontrolle werden auch im Rahmen der Zugriffskontrolle umgesetzt. Die administrativen Tätigkeiten sind auf einen kleinen Kreis von Administratoren eingeschränkt.

d) Trennungskontrolle:
Die Trennung von personenbezogenen Daten wird durch unterschiedliche Speicherorte oder durch eine Mandantentrennung sichergestellt.

2. Integrität

a) Weitergabekontrolle:
Im Rahmen der Weitergabekontrolle wird sicher-gestellt, dass nur berechtigte Personen die personenbezogenen Daten zur Kenntnis nehmen können. Bei einer Übermittlung per E-Mail sind entsprechende Schutzmaßnahmen (z. B. Verschlüsselung der Kommunikation zwischen unseren Clients und dem Mail-Server) eingerichtet. Mobile Geräte oder mobile Speichermedien werden verschlüsselt, wenn auf ihnen personenbezogene Daten gespeichert werden

b) Eingabekontrolle:
Eingabe und Änderung personenbezogener Daten können dem Durchführenden zugeordnet werden

c) Auftragskontrolle:
Im Rahmen der Auftragskontrolle wird sichergestellt, dass die im Auftrag durchgeführten Datenverarbeitungsvorgänge ausschließlich auf Weisung des Verantwortlichen erfolgen. Hierzu werden die in der Datenverarbeitung Tätigen geschult und unterwiesen. Die Auftragsverarbeitung wird durch interne Kontrollen überwacht.

Unter-Auftragsverarbeiter werden nur auf Basis der mit dem Verantwortlichen vereinbarten Regelungen beauftragt. Die Übermittlung oder der Zugriff auf personenbezogene Daten erfolgt erst dann, wenn der Unter-Auftragsverarbeiter eine Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO unterzeichnet hat und die Einhaltung der Regelungen des Datenschutzkonzeptes bestätigt hat. Die Prüfpflicht des Auftragnehmers gegenüber seinem Unter-Auftragsverarbeiter ergibt sich aus der mit dem Auftraggeber abgeschlossenen Vereinbarung zur Auftragsverarbeitung.

3. Verfügbarkeit und Belastbarkeit

Die Verarbeitung von personenbezogenen Daten erfolgt auf Datenverarbeitungssystemen, die einem regelmäßigen Patch-Management unterliegen. Es sind keine Systeme im Netz mit Internetzugang verbunden, die außerhalb der Wartungszyklen der Hersteller liegen (insb. kein Windows XP, Windows Server 2003 etc.). Sicherheitsrelevante Patches werden innerhalb von 72 Stunden nach Bekanntgabe eingespielt, sofern keine Risiken für den Systembetrieb vermutet werden. Die durchgängige Verfügbarkeit von personenbezogenen Daten wird mittels redundanter Speichermedien und Datensicherungen gemäß dem Stand der Technik gewährleistet. Die Server verfügen über eine unterbrechungsfreie Stromversorgung (USV) mit einer Notversorgung über Akkus über eine gewisse Zeit, die im Notfall ein geregeltes Herunterfahren ohne Datenverlust sicherstellt.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Es ist ein Verfahren zur Überwachung des Datenschutzes im Unternehmen implementiert. Dieses beinhaltet die Verpflichtung der Beschäftigten auf das Datengeheimnis, die Schulung und Sensibilisierung der Beschäftigten und die regelmäßige Auditierung der Datenverarbeitungsverfahren. Ebenso ist die Dokumentation des für den Auftraggeber durchgeführten Verarbeitungsverfahrens sichergestellt. Für Datenschutzverletzungen und die Wahrung der Betroffenenrechte ist ein durchgängiger Melde- und Bearbeitungsprozess eingeführt. Dieser beinhaltet auch die Informierung des Verantwortlichen.