

Vertrag über die Verarbeitung personenbezogener Daten im Auftrag eines Verantwortlichen gemäß Art. 28 DSGVO

zwischen [Name und Anschrift des Kunden] - als Verantwortlicher nachfolgend ·AG· für Auftraggeber genannt - und

Herr Said El Ouaziky Hassan, Wuhlestraße 7a, 12683 Berlin

- als Auftragsverarbeiter nachfolgend ·AN· für Auftragnehmer genannt -

- beide gemeinsam als ·Parteien· bezeichnet -

Präambel

(1) Der AG hat den AN mit der Bereitstellung und dem Betrieb des Software-Dienstes Aktegra zur Erstellung von Klassifizierungs- und Dokumentationsberichten auf Grundlage der vom AG eingegebenen Fragebogen-, Organisations- und sonstigen Inhaltsdaten beauftragt.

(2) Teil der Vertragsdurchführungen ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ·betroffene Person·) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DSGVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DSGVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen sowie genetische Daten gem. Art. 4 Abs. 13 DSGVO, biometrischen Daten gem. Art. 4 Abs. 14 DSGVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DSGVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(6) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DSGVO eine von einem Mitgliedstaat gem. Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle.

§ 2 Angabe der zuständigen Datenschutz-Aufsichtsbehörde

(1) Zuständige Aufsichtsbehörde für den AG ist die Aufsichtsbehörde im Bundesland des Geschäftssitzes des AG, vgl. https://www.bfdi.bund.de/DE/Service/Anschriften/anschriften_node.html.

(2) Zuständige Aufsichtsbehörde für den AN ist die Aufsichtsbehörde im Bundesland des Geschäftssitzes des AN, vgl. https://www.bfdi.bund.de/DE/Service/Anschriften/anschriften_node.html.

(3) Die Parteien und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 3 Vertragsgegenstand und -dauer

(1) Bei der Leistungserbringung erhält der AN Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des AG. Umfang und Zweck der Datenverarbeitung durch den AN ergeben sich aus den vereinbarten Leistungen. Dem AG obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit der Leistungserbringung in Zusammenhang stehen und bei denen der AN und seine Beschäftigten oder durch den AN Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom AG stammen oder für den AG erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der vereinbarten Vertragslaufzeit, sofern sich aus den nachfolgenden Bestimmungen nicht darüber hinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 4 Weisungsrecht

(1) Der AN wird Daten nur im Rahmen des Vertrages und gemäß den Weisungen des AG verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der AN durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem AG diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des AG werden anfänglich durch diesen Vertrag festgelegt und können vom AG danach in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der AG ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

(3) Alle erteilten Weisungen sind sowohl vom AG als auch vom AN zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der AN der Ansicht, dass eine Weisung des AG gegen datenschutzrechtliche Bestimmungen verstößt, hat er den AG unverzüglich darauf hinzuweisen. Der AN ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den AG bestätigt oder geändert wird. Der AN darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 Art der verarbeiteten Daten, Kreis der Betroffenen

(1) Im Rahmen der Durchführung des Vertrages erhält der AN Zugriff auf die in Anlage a) näher spezifizierten personenbezogenen Daten.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist ebenfalls in Anlage a) dargestellt.

§ 6 Schutzmaßnahmen des AN

(1) Der AN ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des AG erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der AN wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des AG gem. Art. 32 DSGVO, insbesondere mindestens die in Anlage b) aufgeführten Maßnahmen der

- a) Zutrittskontrolle
- b) Zugangskontrolle
- c) Zugriffskontrolle
- d) Weitergabekontrolle
- e) Eingabekontrolle
- f) Auftragskontrolle
- g) Verfügbarkeitskontrolle
- h) Trennungskontrolle

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem AN jederzeit vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Den bei der Datenverarbeitung durch den AN beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten. Der AN wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b) DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem AN bestehen bleiben. Dem AG sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

§ 7 Informationspflichten des AN

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des AN, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den AN, bei ihm im Rahmen des Auftrages beschäftigten Personen oder durch Dritte wird der AN den AG unverzüglich in Textform, spätestens jedoch innerhalb von Stunden nach Bekanntwerden informieren, soweit der Vorfall den Auftragsgegenstand betrifft. Dasselbe gilt für Prüfungen des AN durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

- a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
- b) eine Beschreibung der von dem AN ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Der AN trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den AG und ersucht um weitere Weisungen.

(3) Der AN ist darüber hinaus verpflichtet, dem AG jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Sollten die Daten des AG beim AN durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der AN den AG unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist.

(5) Der AN wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim AG als ·Verantwortlichem· im Sinne der DSGVO liegt.

(6) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 6 Abs. 2 dieses Vertrages hat der AN den AG unverzüglich zu unterrichten.

(7) Der AN und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des AG durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Das Verzeichnis ist dem AG auf Anforderung zur Verfügung zu stellen.

(8) An der Erstellung des Verzeichnisses durch den AG hat der AN im angemessenen Umfang mitzuwirken. Er hat dem AG die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(9) Die Entscheidung über eine Meldung an die zuständige Aufsichtsbehörde gemäß Art. 33 DSGVO sowie über die Benachrichtigung betroffener Personen gemäß Art. 34 DSGVO obliegt dem AG als Verantwortlichem. Der AN nimmt entsprechende Meldungen oder Benachrichtigungen nur auf dokumentierte Weisung des AG vor, soweit nicht eine gesetzliche Pflicht des AN zu einer eigenen Meldung oder Information besteht.

§ 8 Kontrollrechte des AG

(1) Der AN weist dem AG auf dessen angemessene Anforderung die Einhaltung dieser Vereinbarung und seiner Pflichten nach Art. 28 DSGVO durch geeignete Unterlagen und Nachweise nach. Der Nachweis kann insbesondere durch aktuelle TOM-Beschreibungen, Datenschutz- oder Sicherheitskonzepte, Fragebögen, Prüfberichte, Zertifikate, Selbstauskünfte oder vergleichbare Dokumentationen erfolgen.

(2) Soweit die nach Absatz 1 vorgelegten Unterlagen und Nachweise im Einzelfall nicht ausreichen oder ein begründeter Anlass besteht, ist der AG berechtigt, nach vorheriger Abstimmung eine Prüfung durchzuführen oder durch einen zur Vertraulichkeit verpflichteten Prüfer durchführen zu lassen.

(3) Vor-Ort-Prüfungen sind grundsätzlich mindestens zehn Werktage vorher in Textform anzukündigen, während der üblichen Geschäftszeiten durchzuführen und so auszugestalten, dass Geschäftsabläufe, Geschäftsgeheimnisse sowie die Vertraulichkeit gegenüber anderen Kunden nicht unangemessen beeinträchtigt werden. Bei erheblichen Sicherheitsvorfällen, behördlichen Anordnungen oder einem konkreten Verdacht eines wesentlichen Verstoßes kann eine kürzere angemessene Ankündigungsfrist gelten.

(4) Die Kosten einer über die gewöhnliche Nachweisführung hinausgehenden Prüfung trägt der AG, sofern die Prüfung keinen wesentlichen vom AN zu vertretenden Vertragsverstoß ergibt.

(5) Feststellungen und Ergebnisse von Prüfungen sind vertraulich zu behandeln.

§ 9 Einsatz von Subunternehmern

(1) Die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung von nachfolgenden Subunternehmern durchgeführt:

- Supabase Inc., c/o Incorporating Services, Ltd., 3500 S. DuPont Highway, Dover, Kent 19901, Delaware, USA zur Bereitstellung und zum Betrieb der Datenbank, Nutzerverwaltung und Authentifizierung,
- Vercel Inc., 440 N Barranca Avenue #4133, Covina, CA 91723, USA zur Bereitstellung, Auslieferung und zum technischen Betrieb der Aktegra-Anwendung,
- ImprovMX, 8 The Green, STE D, Dover, Delaware 19901, USA, zur Weiterleitung der an kontakt@aktegra.com eingehenden E-Mails an das E-Mail-Postfach des AN, soweit über die E-Mail-Kommunikation personenbezogene Daten des AG oder seiner Nutzer verarbeitet werden,
- Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland zur Bereitstellung und Verwaltung des E-Mail-Postfachs, soweit über die E-Mail-Kommunikation personenbezogene Daten des AG oder seiner Nutzer verarbeitet werden,
- Plus Five Five, Inc. (Resend), 2261 Market Street #5039, San Francisco, CA 94114, USA, zum Versand von AnmeldeLinks, Transaktions-E-Mails und Formular-E-Mails, soweit hierbei personenbezogene Daten des AG oder seiner Nutzer verarbeitet werden.

(2) Der AN ist darüber hinaus im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern (-Subunternehmerverhältnis-) befugt, soweit er den AG hiervon vorab in Kenntnis setzt. Der AG kann innerhalb von 14 Tagen ab Inkennntnissetzung aus sachlichen Datenschutz- oder Sicherheitsgründen widersprechen. Im Fall eines berechtigten Widerspruchs werden die Parteien eine zumutbare Alternative prüfen. Kann keine zumutbare Lösung gefunden werden, ist jede Partei berechtigt, die von der Änderung betroffene Leistung mit angemessener Frist zu beenden; die übrigen Leistungen bleiben unberührt.

(3) Der AN wählt Unterauftragsverarbeiter sorgfältig unter Berücksichtigung ihrer Eignung, Zuverlässigkeit sowie der für die jeweilige Verarbeitung erforderlichen technischen und organisatorischen Maßnahmen aus. Der AN verpflichtet jeden Unterauftragsverarbeiter durch Vertrag gemäß Art. 28 Abs. 4 DSGVO auf Datenschutzpflichten, die den in dieser Vereinbarung vorgesehenen Pflichten im Wesentlichen entsprechen. Der AN bleibt gegenüber dem AG für die Erfüllung der datenschutzrechtlichen Pflichten des eingesetzten Unterauftragsverarbeiters verantwortlich. Der AN ermöglicht dem AG die Wahrnehmung seiner Kontrollrechte hinsichtlich der Unterauftragsverarbeitung durch geeignete Nachweise und Informationen über den AN. Ein unmittelbares Prüf-, Weisungs- oder Kontrollrecht des AG gegenüber dem jeweiligen Unterauftragsverarbeiter wird hierdurch nicht begründet.

(4) Soweit ein Unterauftragsverarbeiter personenbezogene Daten außerhalb des Europäischen Wirtschaftsraums verarbeitet oder aus einem Drittland auf personenbezogene Daten zugreift, stellt der AN sicher, dass die Voraussetzungen des Kapitels V DSGVO erfüllt sind. Hierzu wird, soweit erforderlich, insbesondere ein Angemessenheitsbeschluss, der Abschluss von EU-Standardvertragsklauseln oder eine sonstige geeignete Garantie gemäß Art. 46 DSGVO herangezogen sowie eine Bewertung des Drittlandtransfers vorgenommen und angemessene ergänzende Schutzmaßnahmen umgesetzt.

(5) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der AN Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der AN für den AG erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den AG genutzt werden.

§ 10 KI-spezifische Sonderregeln

(1) Der AN setzt bei der auftragsbezogenen Verarbeitung derzeit keine KI-Dienste oder Sprachmodelle ein.

(2) Beabsichtigt der AN künftig den Einsatz eines KI-Dienstes zur Verarbeitung personenbezogener Daten des AG, darf dieser Einsatz erst erfolgen, nachdem der AG hierüber in Textform informiert wurde.

(3) Soweit künftig ein KI-Dienst im Rahmen der auftragsbezogenen Verarbeitung eingesetzt wird, darf der AN personenbezogene Daten des AG nur verarbeiten, soweit dies für den jeweils vereinbarten Zweck erforderlich ist. Der AN stellt dabei sicher, dass die Daten nicht zum Training, Fine-Tuning oder zur allgemeinen Verbesserung von KI-Modellen des jeweiligen Anbieters verwendet werden, soweit dies technisch und vertraglich ausgeschlossen werden kann.

(4) Automatisierte Entscheidungen mit rechtlicher Wirkung oder ähnlich erheblicher Beeinträchtigung für betroffene Personen im Sinne von Art. 22 DSGVO sind nicht Gegenstand dieses Vertrags, sofern sie nicht ausdrücklich vereinbart, rechtlich geprüft und dokumentiert freigegeben wurden.

§ 11 Anfragen und Rechte Betroffener

(1) Der AN unterstützt den AG unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen im angemessenen Umfang durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung der Pflichten des AG nach Art. 12 bis 22 sowie Art. 32 bis 36 DSGVO, insbesondere bei Betroffenenanfragen, Datenschutzverletzungen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen. Soweit die Unterstützung über die vertraglich geschuldete Leistung oder die gesetzlichen Pflichten des AN hinausgehenden Aufwand verursacht, ist dieser vom AG angemessen zu vergüten.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem AN geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen unverzüglich an den AG und wartet dessen Weisungen ab.

§ 12 Beendigung

(1) Nach Beendigung des Hauptvertrags ermöglicht der AN dem AG für 30 Kalendertage den Export der im Auftrag verarbeiteten aktiven Datenbestände in einem üblichen, maschinenlesbaren und dem jeweiligen System entsprechenden Format. Während dieser Frist können keine neuen Berichte erstellt oder bestehende Inhalte bearbeitet werden.

(2) Nach Ablauf der Exportfrist löscht der AN die aktiven Datenbestände innerhalb von 30 Kalendertagen, soweit keine gesetzliche Aufbewahrungspflicht oder dokumentierte Weisung des AG entgegensteht.

(3) Technisch unvermeidbare Sicherungskopien, Archivkopien, Protokolldaten und sonstige redundante Kopien dürfen bis zur turnusmäßigen Überschreibung oder Löschung nach dem jeweils geltenden Backup- und Löschrhythmus gespeichert bleiben. Sie werden bis zu ihrer Löschung nicht produktiv verarbeitet und durch angemessene technische und organisatorische Maßnahmen geschützt.

(4) Der AN bestätigt die Löschung auf begründete Anforderung des AG in Textform.

§ 13 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum AN alleine der AG gegenüber dem Betroffenen verantwortlich.

(2) Der AG hält den AN von Geldforderungen Dritter im Zusammenhang mit der Auftragsverarbeitung von Daten auf erstes Anfordern des AN in wirtschaftlicher Hinsicht frei. Dies gilt nicht, wenn und soweit der AN seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus der DSGVO nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des AG oder gegen diese Anweisungen gehandelt hat und die Geldforderung sich hieraus begründet. Art. 82 Abs. 2 bis 4 DSGVO bleiben hiervon unberührt.

(3) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

§ 14 Schlussbestimmungen

(1) Mündliche Nebenabreden sind nicht getroffen. Änderungen, Ergänzungen und Zusätze dieses Vertrages haben nur Gültigkeit, wenn sie zwischen den Vertragsparteien in Textform vereinbart werden. Dies gilt nicht für individuelle Vertragsabreden i. S. v. § 305 b BGB mit einem vertretungsbefugten Vertreter des Anbieters. Im Übrigen kann das Formerfordernis nicht durch mündliche Vereinbarung, konkludentes Verhalten oder stillschweigend außer Kraft gesetzt werden.

(2) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nichtig oder unwirksam sein oder werden, so wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. An die Stelle von nicht einbezogenen oder unwirksamen Bestimmungen tritt das Gesetzesrecht. Sofern solches Gesetzesrecht im jeweiligen Fall nicht zur Verfügung steht (Regelungslücke) oder zu einem untragbaren Ergebnis führen würde, werden die Parteien in Verhandlungen darüber eintreten, anstelle der nicht einbezogenen oder unwirksamen Bestimmung eine wirksame Regelung zu treffen, die ihr wirtschaftlich möglichst nahekommt.

(3) Diese Vereinbarung unterliegt deutschem Recht.

(4) Ist der AG Kaufmann, eine juristische Person des öffentlichen Rechts oder ein öffentlich-rechtliches Sondervermögen, ist der ausschließliche Gerichtsstand für alle Streitigkeiten aus dieser Vereinbarung der Sitz des AN.

Anlagen zum AVV

Anlage a) - Beschreibung der Arten der verarbeiteten personenbezogenen Daten/
Betroffenen/Betroffenengruppe

Anlage b) - Technisch organisatorische Maßnahmen

Anlage a) - Beschreibung der Arten der verarbeiteten personenbezogenen Daten/ Betroffenen/Betroffenengruppe/ Zweck der Verarbeitung

1. Kategorien personenbezogener Daten

1.1 Nutzerkonto-, Identifikations- und Authentifizierungsdaten

- Name, soweit vom AG oder den Nutzern angegeben
- Geschäftliche E-Mail-Adresse der Nutzer
- Nutzer- bzw. Konto-ID
- Rolle und Berechtigungsumfang innerhalb des Kundenkontos
- Status des Nutzerkontos
- Daten zur Anmeldung und Authentifizierung, insbesondere Magic-Link-Informationen, Sitzungs- und Token-Daten
- Zeitpunkt der Kontoerstellung, Anmeldung und letzter Nutzung

1.2 Organisations- und Kontaktdaten

- Firmenname und gegebenenfalls Rechtsform des AG
- Geschäftsanschrift und geschäftliche Kontaktdaten
- Namen, Funktionen und geschäftliche Kontaktdaten von Ansprechpartnern des AG
- Angaben zu Abteilungen, Zuständigkeiten und Rollen innerhalb der Organisation
- Informationen zu verbundenen Unternehmen oder Organisationseinheiten, soweit vom AG in Aktegra hinterlegt

1.3 Fragebogen- und Systemdaten

- Angaben zu dem vom AG bewerteten oder eingesetzten System
- Bezeichnung, Zweck, Einsatzbereich und Funktionsweise des bewerteten Systems
- Angaben zu Nutzern, Nutzergruppen, Verantwortlichkeiten und internen Zuständigkeiten, soweit diese im Fragebogen angegeben werden
- Angaben zu Datenarten, Datenquellen, Verarbeitungsprozessen, technischen und organisatorischen Maßnahmen sowie Risiken
- Angaben zu Dokumentationen, Freigaben, Kontrollmechanismen und weiteren Compliance-bezogenen Informationen
- Sonstige Inhalte, die der AG im Rahmen des Fragebogens oder der Nutzung von Aktegra eingibt

1.4 Klassifizierungs-, Dokumentations- und Berichtsdaten

- Ergebnisse der regelbasierten Klassifizierung
- Erzeugte Klassifizierungs- und Dokumentationsberichte
- Zuordnung eines Berichts zu einem Nutzerkonto, einer Organisation oder einem bewerteten System
- Bearbeitungs- und Erstellungszeitpunkte
- Versionsstände, interne Berichtskürzel und Statusinformationen
- Gespeicherte Zwischenstände sowie vom AG vorgenommene Ergänzungen oder Korrekturen

1.5 Nutzungs-, Sicherheits- und technische Protokolldaten

- Zeitpunkt des Zugriffs auf Aktegra
- Genutzte Funktionen und aufgerufene Bereiche innerhalb der Anwendung
- IP-Adresse
- Browsertyp, Browserversion und Betriebssystem
- Technische Verbindungsdaten und HTTP-Statuscodes
- Fehler-, Sicherheits- und Containerprotokolle, soweit diese im Einzelfall anfallen
- Daten zur Erkennung und Abwehr missbräuchlicher oder unbefugter Zugriffe

1.6 Support- und Kommunikationsdaten

- Inhalte von Supportanfragen des AG oder seiner Nutzer
- Name und E-Mail-Adresse des anfragenden Nutzers
- Zeitpunkt sowie Gegenstand der Anfrage

- Sonstige im Rahmen einer Supportanfrage freiwillig übermittelte Angaben

1.7 Besondere Kategorien personenbezogener Daten Die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO sowie von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO ist für die vertragsgemäße Nutzung von Aktegra grundsätzlich nicht vorgesehen und nicht erforderlich. Der AG stellt sicher, dass solche Daten nicht in Fragebögen, Freitextfeldern, Dokumenten oder sonstigen Eingaben verarbeitet werden, soweit dies nicht im Einzelfall ausdrücklich vereinbart und rechtlich abgesichert wurde.

2. Kategorien betroffener Personen

- Beschäftigte, Nutzer und sonstige berechtigte Personen des AG, die ein Nutzerkonto in Aktegra verwenden
- Ansprechpartner, Projektverantwortliche, Datenschutzbeauftragte, IT-Verantwortliche, Compliance-Verantwortliche und sonstige Kontaktpersonen des AG
- Personen, deren Daten der AG im Rahmen der Fragebogenangaben, Organisationsdaten oder Dokumentationen eingibt
- Personen, die als Verantwortliche, Ansprechpartner, Nutzergruppen oder sonstige Beteiligte eines bewerteten Systems genannt werden
- Personen, die Supportanfragen im Namen des AG stellen
- Sonstige natürliche Personen, deren personenbezogene Daten vom AG ausnahmsweise im Rahmen der vertragsgemäßen Nutzung von Aktegra eingegeben werden

3. Zweck der Verarbeitung

3.1 Bereitstellung und Betrieb des Software-Dienstes Aktegra

- Bereitstellung des Kundenkontos und der geschützten Anwendungsumgebung
- Einrichtung, Verwaltung und Authentifizierung von Nutzerkonten
- Verwaltung von Rollen, Berechtigungen und Zugriffsrechten
- Speicherung und Bereitstellung der vom AG eingegebenen Daten

3.2 Erstellung von Klassifizierungs- und Dokumentationsberichten

- Verarbeitung der vom AG im Fragebogen eingegebenen Angaben
- Durchführung einer regelbasierten Klassifizierung des bewerteten Systems
- Erstellung und Bereitstellung von Klassifizierungs- und Dokumentationsberichten
- Speicherung von Zwischenständen, Berichten und Versionen
- Ermöglichung des Abrufs, Downloads und gegebenenfalls Exports der Berichte durch den AG

3.3 Technischer Betrieb und IT-Sicherheit

- Sicherstellung der Verfügbarkeit, Stabilität und Sicherheit der Anwendung
- Fehleranalyse, Fehlerbehebung und Wartung
- Erkennung, Analyse und Abwehr von Angriffen, Missbrauch und unberechtigten Zugriffen
- Verarbeitung technisch erforderlicher Protokoll- und Verbindungsdaten

3.4 Support und Unterstützung des AG

- Bearbeitung technischer und fachlicher Supportanfragen
- Unterstützung bei der Nutzung des Kundenkontos und der Software-Funktionen
- Unterstützung des AG bei der Erfüllung von Betroffenenrechten, soweit dies im Rahmen der Auftragsverarbeitung erforderlich ist

3.5 Beendigung des Vertragsverhältnisses

- Bereitstellung von Daten zum Export innerhalb einer gegebenenfalls vereinbarten Exportfrist
- Löschung oder Rückgabe der im Auftrag verarbeiteten Daten nach Maßgabe des AVV und der Weisungen des AG
- Aufbewahrung technisch unvermeidbarer Sicherungskopien bis zur turnusmäßigen Überschreibung oder Löschung gemäß dem geltenden Backup- und Löschzyklus des AN

Anlage b) · Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO

Die technischen und organisatorischen Maßnahmen des AN im Sinne des Art. 32 DSGVO werden gesondert dokumentiert und dem AG auf Anforderung in Textform zur Verfügung gestellt; sie sind damit Gegenstand des Nachweises nach § 8 Abs. 1 dieses Vertrages. Anforderungen bitte an kontakt@aktegra.com.

Düsseldorf, den 14.08.2026

Rechtsanwältin Sulmann