Nutzungsbedingungen

Stand 02.11.2026

Nutzungsbedingungen Invecorum

Die Invecorum GmbH, Sophienstraße 40, 38118 Braunschweig, Deutschland, E-Mail: info@invecorum.com, Tel: +49 (0) 160 98481812 (nachfolgend: „**Wir**" oder "**Uns**") stellt dem Kunden die im Folgenden näher beschriebene Anwendung Invecorum unter Maßgabe dieser Nutzungsbedingungen Invecorum (nachfolgend: „**Nutzungsbedingungen**") zur Verfügung.

Für die Nutzung der Anwendung Invecorum ist die Zustimmung des Kunden zu diesen Nutzungsbedingungen erforderlich.

1 Vertragsgrundlagen

1.1 Vertragsparteien

1.1.1 Vertragsparteien sind ausschließlich Wir und der Kunde. Kunden können nur Unternehmer sein. Unternehmer ist eine natürliche oder juristische Person oder eine rechtsfähige Personengesellschaft, die bei Abschluss eines Rechtsgeschäfts in Ausübung ihrer gewerblichen oder selbständigen beruflichen Tätigkeit handelt; eine rechtsfähige Personengesellschaft ist eine Personengesellschaft, die mit der Fähigkeit ausgestattet ist, Rechte zu erwerben und Verbindlichkeiten einzugehen.

1.1.2 Sofern der Kunde eine natürliche Person ist, ist Voraussetzung der Nutzung von Invecorum, dass der Kunde mindestens 18 Jahre alt ist.

1.2 Vertragsgegenstand

1.2.1 Vertragsgegenstand ist die zeitlich auf die Dauer des Vertrags begrenzte Gewährung der Nutzung von Invecorum durch Uns gegenüber dem Kunden und – mit dessen Genehmigung – einer begrenzten Anzahl an Nutzern (nachfolgend: „Leistungen"). Die Gewährung erfolgt entgeltlich; ausschließlich während einer Testphase gemäß Ziffer 1.5 erfolgt sie unentgeltlich.

1.2.2 „Invecorum" ist eine souveräne, KI-gestützte SaaS-Anwendung für das deutsche Steuerrecht.

1.2.3 Das Angebot von Invecorum stellt keine Steuerberatung dar. Zum Leistungsumfang von Invecorum gehört insbesondere keine individuelle Prüfung von Steuererklärungen oder eine sonstige Einzelfallberatung.

1.3 Vertragsschluss

1.3.1 Mit Abschluss der Registrierung kommt zwischen Uns und dem Kunden zunächst ein unentgeltlicher Vertrag über die Nutzung von Invecorum während der Testphase (Ziffer 1.5) auf Grundlage dieser Nutzungsbedingungen zustande. Einen zahlungspflichtigen Vertrag über die Leistungen schließt der Kunde, indem der Kunde auf die mit den Worten „zahlungspflichtigen Vertrag abschließen", „zahlungspflichtig bestellen" oder mit einer entsprechenden eindeutigen Formulierung beschriftete Schaltfläche klickt. Dem Kunden wird zur Berichtigung von Eingabefehlern vor Abgabe der jeweiligen Vertragserklärung noch einmal die Möglichkeit zur Korrektur eingeräumt.

1.3.2 Wir bestätigen dem Kunden den Abschluss des zahlungspflichtigen Vertrags unverzüglich auf elektronischem Weg, z.B. durch Zusendung einer Bestätigungs-E-Mail an die vom Kunden im Rahmen der Registrierung angegebene E-Mailadresse. Eine im Zusammenhang mit der Registrierung zur Testphase versandte Willkommens-E-Mail ist keine Bestätigung eines zahlungspflichtigen Vertragsschlusses. Kunden können den Vertragstext einschließlich dieser Nutzungsbedingungen vor Abschluss der Registrierung speichern und ausdrucken, um über diesen zum Zweck der Dokumentation, der künftigen Bezugnahme und der unveränderten Wiedergabe zu verfügen. Im Übrigen speichern wir den Vertragstext als solchen nicht.

1.3.3 Die jeweils aktuelle Version der Nutzungsbedingungen kann auf unserer Webseite abgerufen und gespeichert werden.

1.3.4 Der Abschluss des Vertrages sowie die Kommunikation zur dessen Erfüllung erfolgt ausschließlich in deutscher Sprache (Vertragssprache).

1.4 Geltungsbereich

Die Bereitstellung von Invecorum erfolgt ausschließlich auf Grundlage dieser Nutzungsbedingungen. Entgegenstehende Geschäftsbedingungen oder einseitige Abänderungen dieser Bedingungen durch Kunden werden von Uns nicht akzeptiert. Abweichende individuelle Vertragsabreden bleiben vorbehalten.

1.5 Kostenlose Testphase

1.5.1 Neue Kunden erhalten mit der Registrierung eine kostenlose Testphase von 7 Tagen ab Bereitstellung des Zugangs (nachfolgend: „Testphase“). Die Dauer der Testphase kann im Einzelfall (z.B. im Rahmen von Aktionen gemäß Ziffer 5.4) abweichen; maßgeblich ist die dem Kunden bei der Registrierung angezeigte Dauer.

1.5.2 Während der Testphase ist keine Zahlungsmethode zu hinterlegen; ein Entgelt fällt nicht an.

1.5.3 Die Testphase geht nicht automatisch in einen zahlungspflichtigen Vertrag über. Schließt der Kunde nicht spätestens mit Ablauf der Testphase einen zahlungspflichtigen Vertrag gemäß Ziffer 1.3.1 Satz 2, endet der unentgeltliche Vertrag mit Ablauf der Testphase, ohne dass es einer Kündigung bedarf.

1.5.4 Mit Ablauf der Testphase endet das Recht zur Nutzung der Leistungen; der Zugriff auf die Funktionen von Invecorum wird gesperrt. Der Kunde kann sich jedoch weiterhin anmelden, um innerhalb eines Zeitraums von 30 Tagen ab dem Ende der Testphase seine Kundeninhalte zu exportieren (Ziffer 12.1.11 gilt entsprechend) oder einen zahlungspflichtigen Vertrag gemäß Ziffer 1.3.1 Satz 2 abzuschließen. Nach Ablauf des Exportzeitraums werden die Daten des Kunden unwiderruflich gelöscht.

1.5.5 Jedem Kunden steht die Testphase nur einmal zu. Wir sind berechtigt, weitere oder wiederholte Testphasen (auch bei erneuter Registrierung derselben Kanzlei bzw. derselben wirtschaftlich verantwortlichen Person) abzulehnen und die Testphase bei Missbrauch vorzeitig zu beenden.

1.5.6 Der Leistungsumfang während der Testphase entspricht grundsätzlich dem regulären Leistungsumfang. Da die Überlassung während der Testphase unentgeltlich erfolgt, gilt abweichend von den übrigen Bestimmungen: (a) Die Verfügbarkeitszusage gemäß Ziffer 2.4 findet keine Anwendung; ein Anspruch auf eine bestimmte Verfügbarkeit besteht nicht. (b) Für Mängel haften Wir nur, soweit Wir einen Mangel arglistig verschwiegen haben (entsprechend §§ 523, 524, 600 BGB). (c) Im Übrigen ist Unsere Haftung auf Vorsatz und grobe Fahrlässigkeit beschränkt (entsprechend §§ 521, 599 BGB). Die Haftungsbeschränkungen nach (b) und (c) gelten nicht für Schäden aus der Verletzung des Lebens, des

Körpers oder der Gesundheit, für Ansprüche nach dem Produkthaftungsgesetz, für Ansprüche nach der Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz sowie im Fall der Übernahme einer Garantie.

2 Bereitstellung der Leistungen

2.1 Bereitstellung von Invecorum

2.1.1 Wir stellen Invecorum passwortgeschützt über unsere Website unter der Internetadresse invecorum.com sowie gegebenenfalls zusätzlich als App zur Verfügung.

2.1.2 Die Software von Invecorum verbleibt – abgesehen von temporären (d.h. laufzeitbezogenen) kundenseitigen Komponenten (wie Applets oder Skripten) sowie, sofern diese angeboten und bereitgestellt wird, der App auf Endgeräten des Kunden oder der Nutzer – auf Unseren Servern und/oder eines von Uns beauftragten Drittanbieters.

2.1.3 Wir sind nicht für die Datenverbindung zwischen den Endgeräten und Systemen des Kunden oder der berechtigten Nutzer und den bei Uns oder für Uns betriebenen Systemen, namentlich dem Router, am Übertragungspunkt, der mit der Internetadresse von Uns verbunden ist, verantwortlich.

2.2 Inhalt der Leistungen

2.2.1 Wir räumen dem Kunden die Möglichkeit ein, Invecorum in Übereinstimmung mit diesen Nutzungsbedingungen angemessen zu nutzen.

2.2.2 Wir erbringen die Leistungen nach dem jeweils aktuellen Stand der Technik.

2.2.3 Der Leistungsumfang ergibt sich aus der Leistungsbeschreibung im Rahmen der Registrierung.

2.2.4 Wir können gesondert freizuschaltende Zusatzfunktionen oder verschiedene Abonnements für die Nutzung von Invecorum anbieten, die sich im Leistungsumfang unterscheiden (z.B. Basis- und Premium-Abonnement). Der Leistungsumfang ergibt sich in diesem Fall aus der jeweiligen Leistungsbeschreibung.

2.3 Berechtigte Nutzer

2.3.1 Wir gestatten dem Kunden, die bei der Bestellung angegebene Anzahl von Nutzern (nachfolgend: „Berechtigte Nutzer“) zur Nutzung von Invecorum zu berechtigen, indem der Kunde für die Berechtigten Nutzer während der Laufzeit und gemäß den Bestimmungen dieser Vereinbarung ein Nutzer-Konto einrichtet und den Berechtigten Nutzern Zugriff darauf gewährt.

2.3.2 Die Einrichtung von Nutzer-Konten, deren Verwaltung und die Vornahme von Einstellungen erfolgt durch den Kunden in eigener Verantwortung über ein Benutzerverwaltungstool (Admin-Panel), auf das Wir dem Kunden Zugriff gewähren.

2.3.3 Berechtigte Nutzer können der Kunde selbst, Organe des Kunden, Mitarbeiter des Kunden und/oder Personen sein, deren Dienste der Kunde zur Erfüllung seiner Verpflichtungen in Anspruch nimmt (nachfolgend: „Erfüllungsgehilfen“; z. B. Subunternehmer des Kunden) und deren Mitarbeiter, sofern es sich jeweils um natürliche Personen handelt. Mitarbeiter von verbundenen Unternehmen, d.h. jede (i) Person, die direkt oder indirekt den Kunden kontrolliert, von diesem kontrolliert wird oder mit diesem unter gemeinsamer Kontrolle steht; sowie in Bezug auf den Nutzer (ii) jede Person, an der eine unter (i) genannte Person eine direkte oder indirekte Beteiligung hält (im Folgenden: „verbundene Unternehmen“), können nur dann Berechtigte Nutzer sein, wenn das verbundene Unternehmen als Erfüllungsgehilfe für den Kunden auftritt oder wenn ausdrücklich zwischen dem Kunden und Uns ist, dass Mitarbeiter verbundener Unternehmen einbezogen sind. Der Kunde hat sicherzustellen, dass

Berechtigte Nutzer über das Benutzerverwaltungstool gelöscht werden, sobald die vorgenannten Bedingungen nicht mehr erfüllt sind (z. B. wenn der Nutzer nicht mehr Mitarbeiter des Kunden ist).

2.4 Verfügbarkeit der Leistungen

Aus technischen Gründen kann es zu zeitlichen und/oder inhaltlichen Einschränkungen der Verfügbarkeit von Invecorum kommen; ein Anspruch des Kunden auf einschränkungslosen Zugriff auf Invecorum besteht nicht. Die Verfügbarkeit von Invecorum beträgt mindestens 98% im Jahresmittel. Hiervon ausgenommen sind Fälle, in denen Invecorum aufgrund von höherer Gewalt, d.h ein außerhalb des Einflussbereichs der Vertragsparteien liegendes Ereignis, durch das Wir ganz oder teilweise an der Bereitstellung von Invecorum gehindert sind, einschließlich Feuerschäden, Überschwemmungen, Streiks und rechtmäßige Aussperrungen, unerwartet auftretende Pandemien oder Epidemien, nicht von Uns oder Unseren Erfüllungsgehilfen verschuldete Betriebsstörungen oder behördliche Verfügungen, nicht über das Internet zu erreichen ist.

2.5 Anpassungen

Wir entwickeln Invecorum kontinuierlich weiter. Wir sind insbesondere zum Zweck der Durchführung von Aktualisierungen berechtigt, Invecorum einschließlich der Benutzeroberfläche, Dialogfelder sowie der Schnittstellen während der Vertragsdauer nach freiem Ermessen anzupassen, soweit dies zur Aufrechterhaltung der Vertragsmäßigkeit nach § 327e Abs. 2 und Abs. 3 BGB und § 327f BGB (insbesondere Anpassung an aktuelle Hardware, Gewährleistung eines gleichbleibenden Niveaus an Sicherheit) erforderlich ist. Die Berechtigung zur Anpassung von Invecorum gemäß Satz 2 umfasst auch die Berechtigung, Funktionen zu entfernen, die für die vertragsgemäße Bereitstellung von Invecorum nicht oder nicht mehr erforderlich sind, soweit dies für die Kunden zumutbar ist. Anpassungen der Services gemäß Satz 2 und Satz 3 erfordern keine Änderung des Vertrages.

2.6 Support-Leistungen

Wir können nach unserem eigenen Ermessen einen Kundensupport für Invecorum anbieten. Sofern dem Kunden die Möglichkeit eingeräumt wird, dem Support den Zugriff auf seine Daten zu untersagen und der Kunde diese Möglichkeit nutzt, können Supportleistungen eingeschränkt sein.

3 Nutzung der Leistungen

3.1 Nutzung von Invecorum

3.1.1 Für den Zugriff auf Invecorum über Unsere Website muss der Kunde, um diesen nutzen zu können, über das Internet (z.B. mittels eines Web-Browsers) hierauf zugreifen. Weitere Einzelheiten können sich aus einer Leistungsbeschreibung (z.B. auf unserer Website) ergeben.

3.1.2 Sofern Wir eine Invecorum App anbieten, muss der Kunde, um diese nutzen zu können, vorerst – gegebenenfalls über den App Store eines Drittanbieter (z. B. über den Apple App Store oder über den Google Play Store) – herunterladen und auf einem unterstützten Endgerät installieren. Für den Zugriff auf Funktionen von Invecorum innerhalb einer App kann eine Internetverbindung erforderlich sein. Weitere

Einzelheiten können sich aus einer Leistungsbeschreibung (z.B. im jeweiligen App Store des Drittanbieters) ergeben.

3.2 Ausgaben von Invecorum und KIErgebnisse

3.2.1 Bestandteil von Invecorum können Funktionen sein, durch die Eingaben des Kunden analysiert und verarbeitet werden. Bei den Ergebnissen einer solchen Verarbeitung handelt es sich jeweils lediglich unverbindliche Vorbereitungs- bzw. Hilfsarbeiten, die den Kunden bei der Bearbeitung unterstützen sollen. Es ist stets eine Einzelfallprüfung durch den Kunden erforderlich.

3.2.2 Wir weisen insoweit ausdrücklich darauf hin, dass die angebotenen Funktionen teilweise auf Techniken der künstlichen Intelligenz (nachfolgend: „KI“) basieren (z.B. der KI-Chatbot) und nach derzeitigem Stand der Technik nicht ausgeschlossen werden kann, dass die Ausgaben fehlerhaft oder inhaltlich unzutreffend sind (insbesondere aufgrund sogenannter Halluzinationen).

3.2.3 Außerdem weisen wir darauf hin, dass die Ergebnisse verarbeitender Funktionen maßgeblich durch die Eingaben des Kunden beeinflusst werden. Soweit unzutreffende Kundendaten – gegebenenfalls auch von einem anderen Berechtigten Nutzer bei dem jeweiligen Kunden – hochgeladen werden, basieren auch die Ergebnisse der jeweiligen Funktion von Invecorum auf diesen unzutreffenden Daten.

3.3 Pflichten des Kunden und Berechtigter Nutzer

3.3.1 Der Kunde hat alle Aufgaben und Pflichten, insbesondere Mitwirkungspflichten, zu erfüllen, die in seinem vertraglichen Verantwortungsbereich zur Erfüllung dieses Vertrages erforderlich sind. Der Kunde wird insbesondere, aber nicht ausschließlich, auf eigene Kosten

a) Zugangsdaten (z.B. Passwörter) vertraulich behandeln und in angemessenem Umfang gegen die Kenntnisnahme durch unbefugte Dritte schützen;

b) Invecorum nicht durch unbefugte Dritte nutzen zu lassen;

c) Uns unverzüglich, z.B. über die in diesem Vertrag oder auf Unserer Webseite angegebenen Kontaktdaten, über Verstöße des Kunden oder anderer Kunden gegen diese Ziffer informieren, von denen der Kunde Kenntnis erlangt; und

d) Uns unverzüglich über etwaige Mängel, Fehlfunktionen oder Schäden an Invecorum informieren.

3.3.2 Der Kunde darf auf Invecorum nur für rechtmäßige Zwecke zugreifen oder Invecorum nutzen. Der Kunde darf Invecorum nicht in einer Weise nutzen oder Dritte bei der Nutzung von Invecorum unterstützen, die

a) Unsere Rechte, die Rechte anderer Kunden oder Dritter (einschließlich Datenschutzrechte, Veröffentlichungsrechte, Rechte an geistigem Eigentum oder andere Eigentumsrechte) verletzen; insbesondere wird der Kunde nur Inhalte auf Invecorum hochladen und/oder speichern, soweit er die erforderlichen Rechte besitzt;

b) rechtswidrig, obszön, missbräuchlich, bedrohlich, einschüchternd, belästigend, hasserfüllt, rassistisch oder ethnisch anstößig ist oder zu einem Verhalten anregt oder ermutigt, das ungesetzlich oder anderweitig unangemessen ist, einschließlich der Verherrlichung von Gewaltverbrechen, der Gefährdung oder Ausbeutung von Kindern oder anderen Personen oder der Koordinierung der Zufügung von Leiden;

c) die Veröffentlichung von Unwahrheiten, falschen Darstellungen oder irreführenden Aussagen beinhaltet;

d) eine Nutzung umfasst, die nicht von dem Abonnement des Kunden abgedeckt ist.

3.3.3 Der Kunde darf weder direkt noch indirekt, durch automatisierte oder andere Methoden oder in irgendeiner nicht autorisierten Weise Uns, Invecorum, Unsere Systeme, andere Kunden oder Dritte, beeinträchtigen oder schädigen, Invecorum nutzen, kopieren, anpassen, modifizieren, verteilen, lizenzieren, unterlizenzieren, übertragen, anzeigen, vorführen oder anderweitig verwerten oder auf Invecorum zugreifen oder abgeleitete Werke auf Basis von Invecorum erstellen (oder andere dabei unterstützen). Dies schließt ein, dass der Kunde Folgendes weder direkt noch durch automatisierte Methoden tun darf:

a) Invecorum zurückzuentwickeln, zu verändern, zu modifizieren, abgeleitete Versionen zu erstellen, zu dekompilieren oder jeglichen Code aus Invecorum extrahieren (sog. Reverse Engineering);

b) Viren oder anderen schädlichen Computercode über Invecorum übertragen oder solchen Code von Invecorum speichern;

c) Massen-E-Mails, Werbeaktionen, Anzeigen oder andere Aufforderungen auf oder mit Invecorum erstellen, verbreiten oder veröffentlichen;

d) sich unbefugten Zugang zu Invecorum verschaffen oder versuchen, sich unbefugten Zugang zu Invecorum zu verschaffen;

e) die Integrität oder Leistung von Invecorum gefährden, beeinträchtigen oder stören; Penetrationstests sind nur nach Unserer vorherigen Zustimmung und in Abstimmung mit Uns zulässig;

f) Konten für Invecorum durch nicht autorisierte Mittel erstellen;

g) Invecorum über ein Netzwerk verbreiten oder verfügbar machen, in dem sie von mehreren Geräten gleichzeitig genutzt werden kann;

h) Software entwickeln, die im Wesentlichen wie Invecorum funktioniert, und diese zur Nutzung durch nicht autorisierte Dritte zur Verfügung stellen; oder

i) Meldekanäle missbrauchen, z.B. indem der Kunde betrügerische oder unbegründete Meldungen oder Einwände macht.

3.3.4 Der Kunde ist verpflichtet, seine Berechtigten Nutzer über die vorstehenden Bestimmungen aufzuklären und ist für Verstöße gegen diese Bestimmungen wie für eigenes Verschulden verantwortlich.

3.3.5 Im Falle des Verstoßes gegen vorstehende Bestimmungen sind wir, unbeschadet weitergehender Rechte (insbesondere einer Kündigung) berechtigt, den Zugriff eines Berechtigten Nutzers bzw. sämtlicher Berechtigter Nutzer des Kunden nach billigem Ermessen vorübergehend zu sperren. Wir werden den Kunden über den Umstand, dass der Zugriff auf Invecorum gesperrt wurde sowie den Grund für die Sperrung informieren. Der Kunde bleibt in diesem Fall auch für die Zeit der Aussetzung der Bereitstellung des Zugriffs zur Zahlung der vereinbarten Vergütung verpflichtet.

3.4 Keine Dateisicherung durch Uns

Wir bieten keine eigenen Leistungen der Datensicherung an. Es obliegt den Kunden, durch zeitlich und inhaltlich ausreichende Maßnahmen für die Sicherung seiner Daten oder der Berechtigten Nutzer Sorge zu tragen. Eine alleinige Ablage der Daten innerhalb von Invecorum (z.B. auf Unseren Servern) ist keine ausreichende Sicherungsmaßnahme in diesem Sinne.

3.5 Anbindung von Drittdiensten (Connectoren)

3.5.1 Invecorum ermöglicht es dem Kunden, von ihm genutzte E-Mail- und Ablagedienste von Drittanbietern (z. B. Microsoft 365, Google Workspace; nachfolgend: „**Drittdienste**“) über die von dem jeweiligen Drittanbieter bereitgestellten Schnittstellen mittels eines Autorisierungsverfahrens (OAuth) an Invecorum anzubinden (nachfolgend: „**Connectoren**“).

3.5.2 Das Vertragsverhältnis über die Nutzung des jeweiligen Drittdienstes besteht ausschließlich zwischen dem Kunden und dem jeweiligen Drittanbieter. Wir werden weder Vertragspartei dieses Vertragsverhältnisses, noch beauftragen Wir den Drittanbieter mit der Verarbeitung von Daten des Kunden. Der Kunde ist dafür verantwortlich, dass die Anbindung und die Nutzung der Drittdienste über Invecorum nach seinem Vertragsverhältnis mit dem Drittanbieter sowie nach den für den Kunden geltenden gesetzlichen und berufsrechtlichen Vorgaben (insbesondere berufsrechtliche Verschwiegenheitspflichten und § 203 StGB) zulässig sind.

3.5.3 Die Anbindung eines Connectors erfolgt ausschließlich durch eine aktive Handlung eines hierzu berechtigten Nutzers des Kunden. Wir protokollieren den Zeitpunkt der Anbindung und der Trennung, den handelnden Nutzer sowie die erteilten Zugriffsberechtigungen (Scopes). Die Anbindung eines Connectors sowie die Nutzung der Connector-Funktionen stellen dokumentierte Weisungen des Kunden im Sinne der Vereinbarung zur Auftragsverarbeitung (Anhang) dar.

3.5.4 E-Mails werden ausschließlich anlassbezogen über den jeweiligen Connector abgerufen bzw. versendet; eine dauerhafte Speicherung abgerufener E-Mails durch Uns erfolgt nicht. In Invecorum erstellte und über einen Connector versendete E-Mails werden als Bestandteil des jeweiligen Chat-Verlaufs in Invecorum gespeichert. Inhalte angebundener Ablagedienste werden in die Bibliothek des Kunden synchronisiert und dort gespeichert.

3.5.5 Der Versand von E-Mails erfolgt technisch über den angebundenen Drittdienst des Kunden und unter der dort hinterlegten Absenderadresse. Es gelten insoweit die technischen und vertraglichen Beschränkungen des Drittanbieters (z. B. Versandlimits und Filterregeln). Für den Inhalt und die rechtliche Zulässigkeit der über Connectoren versendeten Kommunikation ist der Kunde verantwortlich.

3.5.6 Wir schulden weder die Verfügbarkeit der Drittdienste noch die Verfügbarkeit der Schnittstellen der Drittanbieter. Ändert oder beendet ein Drittanbieter seine Schnittstellen oder deren Nutzungsbedingungen, sind Wir berechtigt, die betroffenen Connector-Funktionen entsprechend anzupassen oder einzustellen; Ziffer 13.3 gilt entsprechend.

3.5.7 Die Trennung eines Connectors beendet ausschließlich den künftigen Abruf und Versand von E-Mails sowie die künftige Synchronisation. Bei der Trennung löschen Wir die zugehörigen Zugangstokens unverzüglich in Unseren Systemen und widerrufen sie bei dem Drittanbieter, soweit der Drittanbieter dies technisch unterstützt. Bereits in die Bibliothek synchronisierte Dokumente sowie in Chat-Verläufen gespeicherte E-Mails verbleiben in Invecorum, bis der Kunde sie löscht; die Löschung ist jederzeit über die Anwendung möglich.

3.6 Anbindung von DATEV über das Riecken Cloud Gateway

3.6.1 Invecorum ermöglicht es dem Kunden, die von ihm genutzten DATEV-Anwendungen über das Cloud Gateway der Riecken Webservice & Application GmbH, Nussdorfer Straße 4/1/112, 1090 Wien, Österreich (nachfolgend: „**Riecken**“), an Invecorum anzubinden (nachfolgend: „**DATEV-Anbindung**“). Riecken betreibt die technische Schnittstelle zwischen Invecorum und den DATEV-Schnittstellen des Kunden.

3.6.2 Die Einrichtung der DATEV-Anbindung erfolgt ausschließlich durch eine aktive Handlung eines hierzu berechtigten Nutzers des Kunden. Im Rahmen der Einrichtung schließt der Kunde unmittelbar mit Riecken eine Vereinbarung zur Auftragsverarbeitung ab und erteilt die Zugriffsberechtigungen für die DATEV-Daten seiner Mandanten selbst (z. B. durch Signatur mit einem DATEV-Authentifizierungsmittel). Wir werden nicht Vertragspartei dieses Vertragsverhältnisses.

3.6.3 Abweichend von Ziffer 3.5.2 verarbeitet Riecken bei der Weiterleitung von Anfragen und Daten zwischen Invecorum und DATEV Kundendaten auch in Unserem Auftrag. Riecken ist insoweit Unterauftragnehmer im Sinne der Vereinbarung zur Auftragsverarbeitung (Anhang) und in der Anlage „Unterauftragnehmer“ aufgeführt. Wir haben mit Riecken einen Vertrag zur Auftragsverarbeitung vom 07.08.2026 sowie eine gesonderte Vereinbarung über die Verpflichtung zur Wahrung des Berufsgeheimnisses nach §§ 203, 204 StGB einschließlich Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung (§ 62a StBerG) geschlossen; Ziffer 8.1.5 gilt ergänzend.

3.6.4 Die von Riecken für die DATEV-Anbindung ausgestellten Zugangsdaten werden von Uns verschlüsselt gespeichert und weder Nutzern noch Dritten offengelegt. Aus DATEV abgerufene Daten der vom Kunden ausgewählten Mandanten werden in Invecorum in Rechenzentren in Deutschland gespeichert und ausschließlich den vom Kunden hierzu berechtigten Nutzern zugänglich gemacht. Der Abruf und die Übermittlung von DATEV-Daten, die Auswahl der Mandanten sowie die Freigabe von DATEV-Daten für den KI-Assistenten stellen dokumentierte Weisungen des Kunden im Sinne der Vereinbarung zur Auftragsverarbeitung (Anhang) dar.

3.6.5 Die Ziffern 3.5.6 und 3.5.7 gelten entsprechend. Bei der Trennung der DATEV-Anbindung löschen Wir die Zugangsdaten unverzüglich in Unseren Systemen und veranlassen die Beendigung des Zugriffs bei Riecken. Bereits abgerufene DATEV-Daten verbleiben in Invecorum, bis der Kunde sie löscht.

4 Nutzungsrechte

4.1 Rechteinräumung

Wir gewähren dem Kunden für die Dauer des Vertrages das widerrufliche (im Falle der nicht nur unwesentlichen Verletzung dieser Nutzungsbedingungen), nicht ausschließliche, nicht übertragbare und nicht unterlizenzierbare Recht, der vereinbarten Anzahl an Berechtigten Nutzern die Nutzung von Invecorum im Rahmen des Vertragszwecks und unter Berücksichtigung der Nutzungsbedingungen zu gestatten.

4.2 Rechte an Invecorum

Ungeachtet des oben gewährten Nutzungsrechts behalten Wir alle Rechte, insbesondere die Rechte am geistigen Eigentum an Invecorum.

5 Gebühren und Zahlung

5.1 Gebühren

5.1.1 Der Kunde ist verpflichtet, die im Rahmen des Vertragsschlusses angegebenen Gebühren an Uns zu zahlen. Die Gebühren für die Nutzung von Invecorum richten sich nach der Anzahl der zulässigen Berechtigten Nutzer und gegebenenfalls einem gewählten Abonnement.

5.1.2 Sofern nicht anders angegeben, verstehen sich die angegebenen Gebühren inklusive aller gemäß den gesetzlichen Bestimmungen zu berücksichtigenden Steuern.

5.2 Zahlungsbedingungen

5.2.1 Sofern nicht anders angegeben, sind die Gebühren für jeden Kalendermonat oder einen Teil davon ab dem späteren der beiden Termine fällig: dem Datum der operativen Bereitstellung von Invecorum oder dem Datum des Vertragsschlusses. Hat der Kunde den Vertrag aus wichtigem Grund außerordentlich gekündigt, sind die Gebühren – vorbehaltlich Unseres Aufrechnungsrechts – zeitanteilig zurückzuerstatten.

5.2.2 Mit Abschluss des zahlungspflichtigen Vertrags muss der Kunde eine gültige, akzeptierte Zahlungsmethode hinterlegen; während der Testphase (Ziffer 1.5) ist keine Zahlungsmethode zu hinterlegen. Die akzeptierten Zahlungsmethoden (z.B. Kreditkarte oder Lastschrift) werden dem Kunden im Rahmen des Abschlusses des zahlungspflichtigen Vertrags angezeigt. Sofern diese Funktion verfügbar ist, kann der Kunde die ausgewählte Zahlungsmethode im Einstellungsmenü von Invecorum ändern.

5.2.3 Wir belasten das vom Kunden angegebene Zahlungsmittel mit der Nutzungsgebühr am ersten Tag des jeweiligen Abrechnungszeitraums. Sollte die Zahlungsmethode ungültig werden (z. B. durch eine abgelaufene Kreditkarte oder aus sonstigen Gründen) und sollte dadurch im nächsten Abrechnungszeitraum keine Belastung durch Uns möglich sein, behalten Wir uns vor, den Zugriff auf die Funktionen von Invecorum zu sperren, bis der Kunde eine gültige Zahlungsmethode hinterlegt und die offenen Forderungen ausgeglichen sind. Die Anmeldung zum Zweck der Hinterlegung einer Zahlungsmethode, des Ausgleichs offener Forderungen und des Exports der Kundeninhalte bleibt von der Sperrung unberührt. Wir werden den Kunden über den Umstand, dass der Zugriff auf die Funktionen von Invecorum gesperrt wurde sowie den Grund für die Sperrung informieren. Der Kunde bleibt in diesem Fall auch für die Zeit der Aussetzung der Bereitstellung des Zugriffs zur Zahlung der vereinbarten Vergütung verpflichtet. Gibt der Kunde nach diesem Hinweis nicht innerhalb eines angemessenen Zeitrahmens (in der Regel sieben Tage ab dem Hinweis auf die fehlgeschlagene Belastung) eine gültige Zahlungsmethode an und besteht ein Zahlungsverzug mindestens in Höhe des auf zwei volle Monate entfallenden Preises, behalten Wir Uns vor, den Vertrag außerordentlich zu kündigen. Die außerordentliche Kündigung ist ausgeschlossen, wenn sich der Kunde von seiner Zahlungspflicht durch Aufrechnung befreien konnte und unverzüglich nach der außerordentlichen Kündigung die Aufrechnung erklärt. Nach vollständigem Ausgleich der offenen Forderungen wird der Zugang unverzüglich wieder freigeschaltet. Unser Recht zur ordentlichen Kündigung gemäß Ziffer 11.2.1 bleibt von den vorstehenden Regelungen unberührt.

5.2.4 Ist dies verfügbar und wählt der Kunde das Lastschriftverfahren als Zahlungsmethode, ermächtigt er Uns durch ein SEPA-Lastschriftmandat, den Rechnungsbetrag von seinem Bankkonto einzuziehen. Die Ermächtigung gilt auch für künftige Rechnungen, kann jedoch jederzeit widerrufen werden.

5.2.5 Der Kunde ist – vorbehaltlich vertraglicher Einschränkungen gemäß den gesetzlichen Bestimmungen – berechtigt, Ansprüche aus dem Vertrag, die auf die Zahlung der Vergütung durch Uns gerichtet sind, mit dem Zahlungsanspruch wegen Nichterfüllung der Leistungspflicht oder wegen Mängeln der Leistung aufzurechnen. Andere als die in Satz 1 genannten Forderungen darf der Kunde nur mit Unseren Forderungen verrechnen, soweit diese unbestritten oder rechtskräftig festgestellt sind oder in einem Rechtsstreit entscheidungsreif sind.

5.2.6 Der Kunde ist nur insoweit zur Ausübung eines Zurückbehaltungsrechts berechtigt, als seine Gegenforderung auf demselben Vertragsverhältnis beruht.

5.3 In-App-Käufe

Wir können dem Kunden ermöglichen die kostenpflichtige Nutzung über Drittanbieter, insbesondere den Apple App Store oder Google Play in Anspruch zu nehmen (nachfolgend: „**In-App-Käufe**“). Das Vertragsverhältnis entsteht dabei durch die E-Mail-Bestätigung von Uns dem Kunden gegenüber. Die Drittanbieter haben für den Abschluss des Vertrages, die Bezahlung sowie die Beendigung des Vertragsverhältnisses vorgeschriebene Regelwerke, die der Kunde über die Nutzungsbedingungen des Drittanbieters akzeptiert und auf die Wir keinen Einfluss haben. Entscheidet sich der Kunde, einen Vertrag mit Uns über den Drittanbieter zu schließen, so ist es eine Obliegenheit des Kunden, die in den Nutzungsbedingungen des Drittanbieters vorgegebenen Regelungen über den Abschluss, die Bezahlung und die Beendigung von Verträgen einzuhalten. Bei etwaigen Widersprüchen zwischen den Regelungen des Drittanbieters und diesen Nutzungsbedingungen von Uns gehen insofern die Regelungen des Drittanbieters vor. Insbesondere kann der Kunde von dem Drittanbieter aufgefordert werden, seinen Kauf ihm gegenüber zu bestätigen. Als Zahlungsmethode gilt dann diejenige, die der Kunde mit dem Drittanbieter vereinbart hat (z.B. zahlt der Kunde bei dem Apple App Store über die in seiner Apple-ID hinterlegte Zahlungsmethode). Möchte der Kunde eine etwaige in-App gekaufte Premium-Mitgliedschaft ändern oder beenden, ist es erforderlich, dies über sein Konto bei dem Drittanbieter vorzunehmen, sich dort einzuloggen und den Anweisungen des Drittanbieters zu der Beendigung, dem Widerruf oder der Kündigung folgen. Etwaige Rückerstattungen erfolgen je nach Regelwerk des Drittanbieters entweder im Verhältnis des Drittanbieters mit dem Kunden oder im Verhältnis des Kunden mit Uns.

5.4 Aktionscodes und Rabatte

5.4.1 Wir können zeitlich oder inhaltlich begrenzte Aktionen anbieten, bei denen Kunden durch Eingabe eines Aktions- oder Gutscheincodes (nachfolgend: „Aktionscode“) vergünstigte Konditionen erhalten (z.B. einen prozentualen Rabatt für eine bestimmte Anzahl von Abo-Monaten oder eine verlängerte Testphase). Dies gilt entsprechend für von Partnern ausgegebene Codes (Partnercodes), soweit diese die Gebühren verändern.

5.4.2 Für Aktionscodes gilt, soweit in den jeweiligen Aktionsbedingungen nichts Abweichendes bestimmt ist: (a) Der Rabatt gilt nur für den beworbenen Zeitraum bzw. die beworbene Dauer; danach gelten die regulären Gebühren. (b) Eine Barauszahlung oder nachträgliche Verrechnung ist ausgeschlossen. (c) Pro Kunde kann nur ein Aktionscode eingelöst werden; die Kombination mehrerer Aktionscodes ist ausgeschlossen. (d) Der Aktionscode muss spätestens bei Abschluss des zahlungspflichtigen Vertrags angegeben werden; eine nachträgliche Anrechnung ist ausgeschlossen. (e) Bei Missbrauch (z.B. Mehrfachregistrierung oder Weitergabe entgegen den Aktionsbedingungen) sind Wir berechtigt, den Rabatt zu versagen oder zu widerrufen.

6 Datenschutz und -sicherheit

6.1 Datenschutz

6.1.1 Jede Partei hat alle geltenden Datenschutzgesetze und -vorschriften zum Schutz personenbezogener Daten im Zusammenhang mit ihrer jeweiligen Vertragserfüllung einzuhalten. Der Kunde stellt sicher, dass Wir personenbezogene Daten in dem für die Erfüllung und sonstige Durchführung des Vertrags erforderlichen Umfang verarbeiten dürfen. Im Falle eines Verstoßes durch die Verarbeitung solcher Daten unter Nutzung Unserer Dienste stellt der Kunde Uns von allen Ansprüchen Dritter frei, soweit der Kunde für den Verstoß verantwortlich ist; weitere Ansprüche oder Rechte von Uns bleiben unberührt. Soweit der Kunde Uns beauftragt, personenbezogene Daten im Auftrag des Kunden gemäß Art. 28 DSGVO zu verarbeiten, schließen die Parteien eine Auftragsverarbeitungsvereinbarung ab.

Vereinbaren die Parteien eine gemeinsame Verantwortlichkeit gemäß Art. 26 DSGVO, schließen die Parteien vor der Verarbeitung personenbezogener Daten eine Vereinbarung über die gemeinsame Verantwortlichkeit ab. Der Anbieter ist nicht verpflichtet, vor Abschluss einer Datenverarbeitungsvereinbarung oder einer Vereinbarung über die gemeinsame Verantwortlichkeit Leistungen im Rahmen des Vertrags zu erbringen.

6.1.2 In der Datenschutzerklärung – Invecorum (abrufbar unter https://app.invecorum.com/legal/datenschutz) wird erläutert, wie Wir mit den personenbezogenen Daten des Kunden umgehen und dessen Daten schützen,

6.2 IT-Sicherheit

Wir sorgen in Unserem Verantwortungsbereich für die IT-Sicherheit von Invecorum.

7 Geheimhaltung

7.1 Vertrauliche Informationen

Vertrauliche Informationen im Sinne dieses Vertrages sind

a) Geschäftsgeheimnisse einer Partei im Sinne des GeschGehG (d. h. Informationen, (i) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich sind und daher von wirtschaftlichem Wert sind und (ii) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber sind und (iii) bei denen ein berechtigtes Interesse an der Geheimhaltung besteht),

b) sowie sämtliche Informationen, welche die offenlegende Partei ab Inkrafttreten des Rahmenvertrages bis zur Beendigung des Rahmenvertrages und etwaiger Einzelverträge, an die jeweils andere Partei (nachfolgend: „**Empfänger**“) weitergibt oder diesem zugänglich macht, unabhängig davon, ob dies schriftlich, mündlich, in elektronischer Form oder in sonstiger Art und Weise erfolgt, und

aa) die von der offenlegenden Partei ausdrücklich und für den Empfänger erkennbar als „vertraulich“ oder „geheim“ gekennzeichnet sind oder

bb) deren Vertraulichkeit sich aufgrund eines für den Empfänger erkennbaren Geheimhaltungsinteresses der offenlegenden Partei aus der Natur der Sache ergibt und bei denen ein berechtigtes Interesse an der Geheimhaltung besteht oder

cc) deren Vertraulichkeit die Parteien einvernehmlich vereinbaren. Als vertraulich vereinbaren die Parteien hiermit den Umstand der Geschäftsbeziehung der Parteien und den Inhalt des Vertrages.

Die offenlegende Partei wird die Kennzeichnung nach vorstehendem Buchst. aa) nach billigem Ermessen entsprechend § 315 BGB vornehmen und im Falle der mündlichen oder fernmündlichen Kennzeichnung nach Aufforderung des Empfängers unverzüglich in Textform bestätigen.

7.2 Vertraulichkeitsverpflichtung

Der Empfänger ist verpflichtet,

a) vertrauliche Informationen der offenlegenden Partei

aa) als anvertraute Geschäftsgeheimnisse zu behandeln,

bb) nicht an Dritte weiterzugeben oder diesen zugänglich zu machen und

cc) durch angemessene technische und organisatorische Maßnahmen vor der Kenntnisnahme durch Dritte zu schützen und

b) es zu unterlassen,

aa) vertrauliche Informationen der offenlegenden Partei zu verwenden, soweit dies nicht zur Erreichung des Zwecks von Vereinbarungen zwischen den Parteien erforderlich ist,

bb) vertrauliche Informationen der offenlegenden Partei in irgendeiner Weise selbst wirtschaftlich zu verwerten oder nachzuahmen oder durch Dritte verwerten oder nachahmen zu lassen und insbesondere auf die vertraulichen Informationen der offenlegenden Partei gewerbliche Schutzrechte – insbesondere Marken, Designs/Geschmacksmuster, Patente oder Gebrauchsmuster – anzumelden.

7.3 Ausnahmen von der Vertraulichkeitsverpflichtung

7.3.1 Der Empfänger darf vertrauliche Informationen der offenlegenden Partei vorbehaltlich abweichender Regelungen an mit ihm verbundene Unternehmen i.S.v. §§ 15 ff. AktG und Erfüllungsgehilfen (z.B. Arbeitnehmer oder Unterauftragnehmer des Empfängers), weitergeben und diesen zugänglich machen,

a) soweit die Weitergabe bzw. Zugänglichmachung der jeweiligen vertraulichen Information zur Erreichung des Zwecks von Vereinbarungen zwischen den Parteien erforderlich ist (Need to know-Prinzip) und

b) soweit die verbundenen Unternehmen i.S.v. §§ 15 ff. AktG und Erfüllungsgehilfen vor der Weitergabe bzw. Zugänglichmachung der vertraulichen Information zumindest in vergleichbarer Weise wie der Empfänger zur Geheimhaltung verpflichtet worden sind, wobei eine solche Verpflichtung gegenüber Arbeitnehmern des Empfängers auch durch den jeweiligen Arbeitsvertrag und ergänzende Weisungen des Empfängers gegenüber seinen Arbeitnehmern erfolgen kann und die Verpflichtung zur Geheimhaltung durch die Beendigung des Arbeitsvertrages nicht enden darf.

7.3.2 Die Pflichten des Empfängers gelten nicht, soweit

a) die offenlegende Partei der Weitergabe oder Zugänglichmachung der vertraulichen Information an Dritte ausdrücklich zugestimmt hat, dies mit Wirkung ab dem Zeitpunkt des Zugangs der Zustimmung bei dem Empfänger,

b) die vertrauliche Information zur Zeit ihrer Weitergabe oder Zugänglichmachung durch die offenlegende Partei an den Empfänger insgesamt oder auch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich war,

c) die vertrauliche Information nach ihrer Weitergabe oder Zugänglichmachung durch die offenlegende Partei – ohne dass dies der Empfänger veranlasst oder zu vertreten hätte – insgesamt oder auch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich geworden ist, dies mit Wirkung ab dem Zeitpunkt des Bekanntwerdens,

d) die vertrauliche Information an den Empfänger von einem Dritten auf gesetzliche Weise und ohne Einschränkung in Bezug auf Geheimhaltung oder Verwendung weitergegeben oder zugänglich gemacht wird,

e) der Empfänger die vertrauliche Information selbstständig und unabhängig von ihrer Weitergabe oder Zugänglichmachung durch die offenlegende Partei erstellt oder entwickelt hat, wobei es dem Empfänger

im Streitfall obliegt, die hierfür erforderlichen Tatsachen darzulegen und zu beweisen, oder

f) die vertrauliche Information aufgrund vollziehbarer Entscheidung von Gerichten, Behörden oder sonstigen staatlichen Organen oder aufgrund gesetzlicher Anordnung weitergegeben oder zugänglich gemacht werden muss; der Empfänger bleibt in diesem Fall verpflichtet, der offenlegenden Partei die beabsichtigte Weitergabe bzw. Zugänglichmachung der vertraulichen Information rechtzeitig zuvor schriftlich anzeigen, um der offenlegenden Partei die Prüfung der Pflicht, die Geltendmachung von Rechten und die Einlegung von Rechtsbehelfen zu ermöglichen, um die Weitergabe bzw. Zugänglichmachung zu verhindern. Die Verpflichtung, der offenlegenden Partei die beabsichtigte Weitergabe bzw. Zugänglichmachung der vertraulichen Information rechtzeitig zuvor schriftlich anzuzeigen, besteht nicht, soweit der Empfänger hierdurch gegen gesetzliche Vorschriften und/oder vollziehbare Anordnungen eines Gerichts oder einer zuständigen Behörde oder von sonstigen staatlichen Organen verstoßen würde.

7.3.3 Zusätzlich erklärt die offenlegende Partei gegenüber dem Empfänger unwiderruflich ihre Zustimmung in die Weitergabe bzw. Zugänglichmachung einer vertraulichen Information

a) gegenüber Gerichten und/oder Behörden, soweit dies zur Durchsetzung von oder zur Verteidigung gegen Ansprüche bzw. Rechte erforderlich ist, und

b) gegenüber aufgrund ihres Berufes gesetzlich zur Verschwiegenheit verpflichteten Beratern des Empfängers (insbesondere von Rechtsanwälten, Wirtschaftsprüfern oder Steuerberatern), soweit dies zur Beratung des Empfängers durch den Berater erforderlich ist (auch im Rahmen einer Due Diligence oder Durchführung einer Transaktion) und der Berater von dem Empfänger nicht von seiner Pflicht zur Geheimhaltung befreit ist.

Der Empfänger hat ein Verschulden seines Beraters in gleichem Umfang zu vertreten wie eigenes Verschulden.

7.3.4 Es obliegt dem Empfänger, darzulegen und zu beweisen, dass die Voraussetzungen für den jeweiligen Ausnahmetatbestand erfüllt sind.

7.4 Reichweite der Vertraulichkeitsverpflichtung

7.4.1 § 5 des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) wird durch die vorstehenden Bestimmungen weder beschränkt noch ausgeschlossen.

7.4.2 Die Pflichten aus diesem Vertrag in Bezug auf vertrauliche Informationen, welche die offenlegende Partei an den Empfänger zwischen Beginn und Beendigung des Vertrages weitergegeben bzw. ihm zugänglich gemacht hat, bleiben auch nach Beendigung des Vertrages bestehen, und zwar im Falle von Geschäftsgeheimnissen und Mandatsgeheimnissen sowie von personenbezogenen Daten i.S.d. Datenschutzrechts nach Maßgabe des gesetzlichen Schutzes ohne zeitliche Beschränkung durch den Vertrag, im Übrigen in Bezug auf alle vertraulichen Informationen jedenfalls für zwei Jahre ab Beendigung des Vertrages. Der Empfänger sorgt dafür, dass die mit ihm verbundenen Unternehmen und Erfüllungsgehilfen sämtliche erforderlichen Maßnahmen treffen, damit der Empfänger gegenüber der offenlegenden Partei seine Pflichten nach Beendigung des Vertrages erfüllen kann.

7.5 Folgen der Beendigung des Vertrags

7.5.1 Der Empfänger ist gegenüber der offenlegenden Partei verpflichtet, bei Beendigung dieses Vertrages sämtliche vertraulichen Informationen,

a) soweit der Empfänger diese in körperlicher Form (z.B. auf Papier) oder auf einem beweglichen Datenträger in elektronischer Form (z.B. auf USB-Stick oder DVD) erhalten hat, unaufgefordert und

unverzüglich an die offenlegende Partei zurückzugeben oder

b) auf Verlangen der offenlegenden Partei unverzüglich zu vernichten und der offenlegenden Partei anschließend unverzüglich und in Schriftform die durchgeführte Vernichtung zu bestätigen.

Die Verpflichtungen nach Satz 1 bestehen – ungeachtet der fortbestehenden Geheimhaltungspflicht – nicht,

a) soweit und solange die vertraulichen Informationen einer gesetzlichen Verpflichtung oder Berechtigung des Empfängers zur Speicherung oder sonstigen Aufbewahrung unterliegen oder auch

b) soweit und solange der Empfänger die vertraulichen Informationen aufgrund technisch und organisatorischer notwendiger routinemäßiger Datensicherungen elektronisch speichert (z.B. als temporäre Datensicherung (etwa Backup) auf einem Datenträger des Empfängers).

Soweit und sobald die gesetzlichen Verpflichtungen oder Berechtigungen des Empfängers nicht mehr bestehen und auch die Datensicherung nicht mehr technisch und organisatorisch notwendig ist, finden die Verpflichtungen nach Satz 1 entsprechend Anwendung, dies mit der Maßgabe, dass der Empfänger auch ohne Verlangen der offenlegenden Partei unverzüglich zur Vernichtung gemäß Satz 1 Buchst. b) verpflichtet ist.

7.5.2 Dem Empfänger steht gegenüber den Ansprüchen auf Herausgabe oder Vernichtung vertraulicher Informationen der offenlegenden Partei kein Recht zur Zurückbehaltung zu.

7.5.3 Weitergehende Vereinbarungen über die Geheimhaltung von Informationen und deren Verwertung sowie gesetzliche Pflichten, etwa nach dem Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) und dem jeweils anwendbaren Datenschutzrecht, bleiben unberührt.

8 Besondere Bestimmungen für Mandatsgeheimnisse

8.1 Mandatsgeheimnisse als Teil der Kundendaten

8.1.1 Soweit der Kunde Berufsgeheimnisträger (z.B. Steuerberater, Wirtschaftsprüfer oder Rechtsanwalt) ist, ist nicht ausgeschlossen, dass Mandatsgeheimnisse (d.h. Informationen, die dem Kunden als Berufsgeheimnisträger in Ausübung seines Berufs bekannt geworden ist und bekannt werden) Teil der von dem Kunden Invecorum hochgeladenen bzw. gespeicherten Daten sind.

8.1.2 Insoweit weisen Wir darauf hin, dass diese Kundendaten auf dezidiert dem jeweiligen Kunden zugewiesenen Speicherplatz bei den von Uns eingesetzten Cloud-Anbietern Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland (nachfolgend: „Hetzner“), und IONOS SE, Elgendorfer Str. 57, 56410 Montabaur, Deutschland (nachfolgend: „IONOS SE“), in Rechenzentren in Deutschland gespeichert werden.

8.1.3 Der Kunde stimmt hiermit dem Einsatz von Hetzner und der IONOS SE als Cloud-Anbieter für Hosting, Speicher, Dokumentenverarbeitung und GPU-Infrastruktur zu. Die IONOS SE wurde von Uns entsprechend der folgenden Ziffer 8.2 verpflichtet und hat Uns gegenüber versichert, dass ihrerseits von dieser eingesetzte Dritt-Anbieter entsprechend zur Geheimhaltung verpflichtet wurden. Mit Hetzner haben Wir eine gesonderte Zusatzvereinbarung zur Verpflichtung auf die Geheimhaltung nach § 203 StGB abgeschlossen, die sämtliche von Uns bei Hetzner eingesetzten Server erfasst. Hetzner wurde damit entsprechend der folgenden Ziffer 8.2 verpflichtet.

8.1.4 Für die Sprachmodell-Infrastruktur und die hierfür eingesetzte GPU-Infrastruktur setzen Wir die TensorX Ltd., Unit 25, Classon House, Dundrum Business Park, Dublin 14, Irland (nachfolgend: „TensorX“), ein. Die Verarbeitung erfolgt ausschließlich in Rechenzentren in der Europäischen Union.

TensorX verarbeitet die Inhalte der Anfragen ausschließlich temporär, ohne sie zu speichern, zu protokollieren oder zum Training von KI-Modellen zu verwenden. Der Kunde stimmt hiermit dem Einsatz von TensorX sowie der von TensorX für Rechenzentren, Cloud- und Netzwerkinfrastruktur in der Europäischen Union eingesetzten weiteren Dienstleister zu. Wir haben mit TensorX einen Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO sowie eine gesonderte Vereinbarung über die Verpflichtung zur Wahrung des Berufsgeheimnisses nach §§ 203, 204 StGB einschließlich Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung geschlossen. TensorX wurde damit entsprechend der folgenden Ziffer 8.2 verpflichtet.

8.1.5 Für die DATEV-Anbindung gemäß Ziffer 3.6 setzen Wir die Riecken Webservice & Application GmbH, Nussdorfer Straße 4/1/112, 1090 Wien, Österreich, Firmenbuch FN 412181z (nachfolgend: „Riecken"), ein. Riecken leitet Anfragen und Daten zwischen Invecorum und den DATEV-Schnittstellen des Kunden weiter. Der Kunde stimmt hiermit dem Einsatz von Riecken zu. Wir haben mit Riecken einen Vertrag zur Auftragsverarbeitung vom 07.08.2026 sowie eine gesonderte Vereinbarung über die Verpflichtung zur Wahrung des Berufsgeheimnisses nach §§ 203, 204 StGB einschließlich Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung (§ 62a StBerG) geschlossen. Riecken wurde damit entsprechend der folgenden Ziffer 8.2 verpflichtet. Unberührt bleibt die Vereinbarung zur Auftragsverarbeitung, die der Kunde im Rahmen der Einrichtung unmittelbar mit Riecken schließt.

8.1.6 Der Kunde wird Mandatsgeheimnisse als Teil der Kundendaten nur auf Invecorum speichern bzw. hochladen, soweit er hierzu berechtigt ist.

8.2 Geheimhaltungspflicht in Bezug auf Mandatsgeheimnisse

8.2.1 Soweit eine Verpflichtung des Kunden besteht, mit Uns besondere Regelungen in Bezug auf Mandatsgeheimnisse zu vereinbaren, und zwar z.B. Steuerberater gemäß § 62a des Steuerberatungsgesetz (StBerG), Wirtschaftsprüfer gemäß § 50a der Wirtschaftsprüferordnung (WPO) und Rechtsanwälte gemäß § 43e der Bundesrechtsanwaltsordnung (BRAO), vereinbaren Wir mit dem Kunden Folgendes.

8.2.2 Wir werden hiermit unter Belehrung über die strafrechtlichen Folgen einer Pflichtverletzung zur Verschwiegenheit verpflichtet.

Die Strafbestimmungen (§§ 203, 204 StGB) sind in Auszügen in Ziffer 8.2.4 wiedergegeben. Eine Straftat nach § 203 Abs. 4 StGB wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe, eine Straftat nach § 203 Abs. 6 oder nach § 204 StGB mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

Wir wurden insbesondere darauf hingewiesen, dass Wir uns nach § 203 Abs. 4 Satz 1 Nr. 2 StGB strafbar machen, wenn Wir uns einer weiteren mitwirkenden Person bedienen, die unbefugt ein fremdes, Uns bei der Ausübung oder bei Gelegenheit Unserer Tätigkeit bekannt gewordenes Geheimnis offenbart, ohne dass Wir dafür Sorge getragen haben, dass die weitere mitwirkende Person zur Geheimhaltung verpflichtet wurde.

Wir dürfen Uns nur insoweit Kenntnis von Mandatsgeheimnissen verschaffen, als dies zur Erfüllung der Leistungsvereinbarung zwischen Uns und dem Kunden erforderlich ist.

Soweit Wir von dem Kunden die Zustimmung erhalten, weitere Personen zur Erfüllung der Leistungsvereinbarung zwischen dem Kunden und Uns heranzuziehen, und wenn diese Personen Mandatsgeheimnisse erhalten oder ihnen solche zugänglich gemacht werden, sind Wir verpflichtet, diese Personen in vergleichbarer Weise wie nach dieser Vereinbarung zur Verschwiegenheit und zur Weitergabe der Pflichten aus dieser Vereinbarung zu verpflichten. Bei der Inanspruchnahme von Dienstleistungen, die

im Ausland erbracht werden, dürfen Wir den Personen den Zugang zu Mandatsgeheimnissen unbeschadet der weiteren Voraussetzungen nur dann eröffnen, wenn der dort bestehende Schutz der Mandatsgeheimnisse dem Schutz in der Bundesrepublik Deutschland vergleichbar ist, es sei denn, dass der Schutz der Mandatsgeheimnisse dies nicht gebietet.

8.2.3 Für Mandatsgeheimnisse gilt – dies zur Klarstellung – die Verschwiegenheitspflicht nach Maßgabe der gesetzlichen Bestimmungen ohne zeitliche Beschränkung nach dem Vertrag.

8.2.4 Auszüge aus den gesetzlichen Bestimmungen zum Geheimnisschutz:

§ 203 des Strafgesetzbuchs. Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

(…)

3. Rechtsanwalt, Kammerrechtsbeistand, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten,

3a. Organ oder Mitglied Wirtschaftsprüfungs-, Buchprüfungs- oder einer Berufsausübungsgesellschaft von Steuerberatern und Steuerbevollmächtigten, einer Berufsausübungsgesellschaft von Rechtsanwälten oder europäischen niedergelassenen Rechtsanwälten oder einer Berufsausübungsgesellschaft von Patentanwälten oder niedergelassenen europäischen Patentanwälten im Zusammenhang mit der Beratung und Vertretung der Wirtschaftsprüfungs-, Buchprüfungs- oder Berufsausübungsgesellschaft im Bereich der Wirtschaftsprüfung, Buchprüfung oder Hilfeleistung in Steuersachen oder ihrer rechtsanwaltlichen oder patentanwaltlichen Tätigkeit,,

(…)

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) (…)

(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.

(4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist. Ebenso wird bestraft, wer

1. als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind,

2. als im Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis

offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder

3. nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat.

(5) Die Absätze 1 bis 4 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

(6) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

§ 204 des Strafgesetzbuchs. Verwertung fremder Geheimnisse

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein Betriebs- oder Geschäftsgeheimnis, zu dessen Geheimhaltung er nach § 203 verpflichtet ist, verwertet, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) § 203 Absatz 5 gilt entsprechend.

§ 53 der Strafprozessordnung. Zeugnisverweigerungsrecht der Berufsgeheimnisträger

(1) Zur Verweigerung des Zeugnisses sind ferner berechtigt

(…)

3. Rechtsanwälte und Kammerrechtsbeistände, Patentanwälte, Notare, Wirtschaftsprüfer, vereidigte Buchprüfer, Steuerberater und Steuerbevollmächtigte, (…) über das, was ihnen in dieser Eigenschaft anvertraut worden oder bekanntgeworden ist; (…);

(2) Die in Absatz 1 Satz 1 Nr. 2 bis 3b Genannten dürfen das Zeugnis nicht verweigern, wenn sie von der Verpflichtung zur Verschwiegenheit entbunden sind. Die Berechtigung zur Zeugnisverweigerung der in Absatz 1 Satz 1 Nr. 5 Genannten über den Inhalt selbst erarbeiteter Materialien und den Gegenstand entsprechender Wahrnehmungen entfällt, wenn die Aussage zur Aufklärung eines Verbrechens beitragen soll oder wenn Gegenstand der Untersuchung

1. eine Straftat des Friedensverrats und der Gefährdung des demokratischen Rechtsstaats oder des Landesverrats und der Gefährdung der äußeren Sicherheit (§§ 80a, 85, 87, 88, 95, auch in Verbindung mit § 97b, §§ 97a, 98 bis 100a des Strafgesetzbuches),

2. eine Straftat gegen die sexuelle Selbstbestimmung nach den §§ 174 bis 174c, 176a, 176b, 177 Absatz 2 Nummer 1 des Strafgesetzbuches oder

3. eine Geldwäsche, eine Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 Abs. 1 bis 4 des Strafgesetzbuches

ist und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Der Zeuge kann jedoch auch in diesen Fällen die Aussage verweigern, soweit sie zur Offenbarung der Person des Verfassers oder Einsenders von Beiträgen und Unterlagen oder des sonstigen Informanten oder der ihm im Hinblick auf seine Tätigkeit nach Absatz 1 Satz 1 Nr. 5 gemachten Mitteilungen oder deren Inhalts führen würde.

§ 53a der Strafprozessordnung. Zeugnisverweigerungsrecht der mitwirkenden Personen

(1) Den Berufsgeheimnisträgern nach § 53 Absatz 1 Satz 1 Nummer 1 bis 4 stehen die Personen gleich, die im Rahmen

1. eines Vertragsverhältnisses einschließlich der gemeinschaftlichen Berufsausübung,

2. einer berufsvorbereitenden Tätigkeit oder

3. einer sonstigen Hilfstätigkeit

an deren beruflicher Tätigkeit mitwirken. Über die Ausübung des Rechts dieser Personen, das Zeugnis zu verweigern, entscheiden die Berufsgeheimnisträger, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann.

(2) Die Entbindung von der Verpflichtung zur Verschwiegenheit (§ 53 Absatz 2 Satz 1) gilt auch für die nach Absatz 1 mitwirkenden Personen.

9 Gewährleistung

Es besteht ein gesetzliches Gewährleistungsrecht. Unsere Mängelhaftung richtet sich nach den gesetzlichen Vorschriften. Für Schadens- und Aufwendungsersatzansprüche besteht eine Haftungsbegrenzung gemäß nachfolgender Ziffer 10.

10 Haftung und Haftungsbeschränkungen

10.1 Haftung ohne vertragliche Beschränkung

Wir haften ohne vertragliche Beschränkung nach den gesetzlichen Vorschriften

a) für Schäden, soweit diese auf dem Fehlen einer Beschaffenheit, für die Wir eine Garantie übernommen haben, beruhen;

b) wegen Vorsatzes;

c) für Schäden, soweit diese darauf beruhen, dass Wir einen Mangel arglistig verschwiegen haben;

d) für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit, die auf einer vorsätzlichen oder fahrlässigen Pflichtverletzung von Uns oder sonst auf vorsätzlichem oder fahrlässigem Verhalten eines gesetzlichen Vertreters oder Erfüllungsgehilfen von Uns beruhen;

e) für andere als die unter verstehendem Buchst. d) dieser Nutzungsbedingungen aufgeführten Schäden, die auf einer vorsätzlichen oder grob fahrlässigen Pflichtverletzung von Uns oder sonst auf vorsätzlichem oder grob fahrlässigem Verhalten eines gesetzlichen Vertreters oder Erfüllungsgehilfen von Uns beruhen;

f) nach dem Produkthaftungsgesetz, nach der Datenschutz-Grundverordnung und nach dem Bundesdatenschutzgesetz.

10.2 Haftungsbeschränkung

In anderen als den in der vorstehenden Ziffer 10.1 dieser Nutzungsbedingungen aufgeführten Fällen ist die Haftung von Uns auf den Ersatz des vertragstypischen und vorhersehbaren Schadens beschränkt, soweit der Schaden auf einer fahrlässigen

Verletzung von wesentlichen Pflichten durch Uns oder durch einen gesetzlichen Vertreter oder Erfüllungsgehilfen von Uns beruht. Wesentliche Pflichten (auch „Kardinalpflichten“) sind Pflichten, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Kunde regelmäßig vertraut und vertrauen darf.

10.3 Haftungsausschluss

In anderen als den in den beiden vorstehenden Ziffern 10.1. und 10.2. dieser Nutzungsbedingungen aufgeführten Fällen ist Haftung von Uns, den gesetzlichen Vertretern von Uns und den Erfüllungsgehilfen von Uns wegen Fahrlässigkeit begrenzt auf den vertragstypischen und vorhersehbaren Schaden.

10.4 Mitverschulden

Der Einwand des Mitverschuldens bleibt unberührt.

10.5 Reichweite der Haftungsbeschränkungen und -ausschlüsse

Die vorstehenden Bestimmungen in Ziffer 10 dieser Nutzungsbedingungen gelten für alle vertraglichen und außervertraglichen Schadensersatzansprüche unabhängig von ihrem Rechtsgrund sowie entsprechend auch für die Haftung auf Ersatz vergeblicher Aufwendungen.

11 Vertragslaufzeit und Kündigung

11.1 Laufzeit

Der Vertrag beginnt mit Vertragsschluss und wird auf unbestimmte Zeit geschlossen. Es besteht keine Mindestlaufzeit. Der Abrechnungszeitraum beträgt jeweils einen Monat (nachfolgend: „Abo-Monat“).

11.2 Ordentliche Kündigung

11.2.1 Soweit nicht ausdrücklich etwas Abweichendes vereinbart ist, kann jede Partei den Vertrag jederzeit ohne Einhaltung einer Frist mit Wirkung zum Ende des jeweiligen Abo-Monats (Abrechnungszeitraums) ordentlich kündigen.

11.2.2 Im Falle der Einstellung des Angebots von Invecorum oder der Einstellung oder Kündigung gegenüber Uns, von Invecorum zugrundliegen Services, die für dessen Bereitstellung wesentlich sind (z.B. Cloud-Services), können Wir den Vertrag abweichend von vorstehender Ziffer 11.2.1 mit einer Frist von einem Monat zum Ende eines Kalendermonats ordentlich kündigen. Ist Uns die Einhaltung dieser Frist aufgrund von Umständen außerhalb Unseres Einflussbereichs (z.B. der kurzfristigen Einstellung oder Kündigung eines für die Bereitstellung wesentlichen Drittdienstes) nicht möglich, können Wir mit einer entsprechend kürzeren, jedoch so lang wie möglichen und zumutbaren Frist kündigen. Das Recht des Kunden, seine Kundeninhalte innerhalb von 30 Tagen nach Vertragsbeendigung zu exportieren, bleibt unberührt.

11.3 Kündigung aus wichtigem Grund

11.3.1 Das Recht zur Kündigung des Vertrags aus wichtigem Grund bleibt unberührt. Ein wichtiger Grund liegt vor, wenn der kündigenden Partei unter Berücksichtigung aller Umstände des Einzelfalls und unter Abwägung der beiderseitigen Interessen die Fortsetzung des Vertragsverhältnisses nicht mehr zugemutet werden kann.

11.3.2 Besteht der wichtige Grund in der Verletzung einer Vertragspflicht, ist die außerordentliche Kündigung erst nach erfolglosem Ablauf einer zur Abhilfe bestimmten Frist oder nach erfolgloser Abmahnung zulässig, es sei denn, eine solche ist aus den gesetzlich bestimmten Gründen entbehrlich.

11.3.3 Die Berechtigung, Schadensersatz zu verlangen, wird durch eine außerordentliche Kündigung nicht ausgeschlossen.

11.3.4 Wenn Wir gegenüber dem Kunde berechtigt eine außerordentliche Kündigung aufgrund einer Pflichtverletzung des Kunden erklären, steht Uns ein Anspruch auf Ersatz des hierdurch entstehenden Schadens zu. Dies gilt nicht, soweit der Kunde die Pflichtverletzung nicht zu vertreten hat.

12 Besondere Bedingungen für Wechsel unter dem Data Act

Die in dieser Ziffer dargestellten besonderen Bedingungen finden Anwendung, soweit der Kunde (a) von den Leistungen (nachfolgend: „**Datenverarbeitungsdienste**“) zu den Diensten eines anderen Anbieters wechseln möchte, (b) alle seine Kundeninhalte aus den Datenverarbeitungsdiensten exportieren möchte, um sie auf seine eigene IKT-Infrastruktur (z.B. PC oder mobile Endgeräte) zu übertragen oder (c) seine Kundeninhalte löschen möchte. Die in (a) und (b) beschriebenen Szenarien werden nachfolgend jeweils als „Wechsel“ bezeichnet:

12.1.1 Der Kunde kann sämtliche Kundeninhalte bis einschließlich eines Zeitraums von 30 Tagen nach Vertragsbeendigung exportieren, auch im Falle eines Wechsels. „Kundeninhalte“ sind alle Daten, die der Kunde oder seine Berechtigten Nutzer in den Datenverarbeitungsdiensten hochladen, speichern, erstellen oder anderweitig verarbeiten.

12.1.2 Generell ist der Kunde nicht verpflichtet, Uns darüber zu informieren, dass er einen Wechsel beabsichtigt. Unbeschadet sonstiger vertraglicher Bestimmungen, hat der Kunde jederzeit Zugang zu seinen Kundeninhalten und kann diese jederzeit löschen oder exportieren. Diese Rechte werden durch diese besonderen Bedingungen nicht berührt. Ebenso berühren diese besonderen Bedingungen nicht die vertraglichen oder gesetzlichen Kündigungsrechte des Kunden. Möchte der Kunde jedoch die in diesen besonderen Bedingungen beschriebenen zusätzlichen Rechte geltend machen, muss er Uns dies mitteilen. In dieser Mitteilung kann der Kunde Uns mitteilen, dass er eine der folgenden Optionen ausüben möchte:

a) Wechsel zu einem anderen Anbieter

b) Export aller Kundeninhalte, um sie auf seine eigene IKT-Infrastruktur zu übertragen. Der Kunde ist für den Export von Kundeninhalten selbst verantwortlich. Eine Anzeige ist notwendig, wenn technische Gegebenheiten einen Export nicht möglich machen sollten.

c) Löschung seiner Kundeninhalte

12.1.3 Der Kunde kündigt den Wechsel über die Mitteilung an und definiert den Start des „Übergangszeitraums“. Diese Anzeige des Wechsels muss mindestens 30 Tage vor Beginn des Übergangszeitraums vorliegen. Durch die Mitteilung wird der 30-tägige „Übergangszeitraum“ festgelegt,

in dem die nachfolgenden Bestimmungen zugunsten des Kunden gelten. Der Kunde kann den Übergangszeitraum einmalig um einen Zeitraum verlängern, den er zum Zwecke seines Wechsels für angemessen erachtet. Eine solche Verlängerung ist nur wirksam, wenn der Kunde dies Uns spätestens 30 Tage vor Ablauf des ursprünglichen Überganszeitraums in Textform mitteilt. Falls eine Verlängerung des Übergangszeitraums aus Gründen der technischen Durchführbarkeit erforderlich ist, teilen Wir dies dem Kunden innerhalb von 14 Arbeitstagen nach Erhalt der Wechselankündigung mit, verbunden mit einer Begründung und der Dauer der Verlängerung (wobei der Übergangszeitraum in keinem Fall sieben Monate überschreiten wird). Eine Verlängerung des Übergangszeitraums kann gemäß den anwendbaren vertraglichen Bestimmungen zur Folge haben, dass der Vertrag während des Übergangszeitraums als ungekündigt zu den vereinbarten Konditionen weiterläuftDie Wechsel- und Kündigungsrechte des Kunden gemäß diesen besonderen Bedingungen bleiben hiervon unberührt.

12.1.4 Wenn der Kunde Uns einen Wechsel gemäß diesen besonderen Bedingungen ankündigt, werden wir diesem oder von ihm nachweislich autorisierten Dritte angemessene Unterstützung beim Wechsel leisten.

12.1.5 Wir werden im Falle eines Wechsels mit der gebotenen Sorgfalt handeln, um die Datenverarbeitungsdienste auch während des Wechsels weiterzuerbringen und dadurch den Kunden dabei zu unterstützen, die Kontinuität des Geschäftsbetriebs aufrechtzuerhalten. Wir weisen aber darauf hin, dass der Kunde selbst für die Durchführung des Wechsels verantwortlich ist, insbesondere für den Export seiner Kundeninhalte, die Verfügbarkeit einer Internetverbindung mit ausreichender Bandbreite, das Übertragen seiner Kundeninhalte in die eigene IKT-Infrastruktur bzw. in die Infrastruktur oder Systeme eines anderen Anbieters, sowie für die Auswahl und Konfiguration der Dienste dieses Anbieters. Wir übernehmen ausdrücklich keine Haftung für den Erfolg des Wechsels.

12.1.6 Wir verlangen keine gesonderte Vergütung für einen Wechsel. Dies gilt ausdrücklich auch für die vorstehend beschriebenen Unterstützungsleistungen, nicht jedoch für gesondert vom Kunden bei Uns beauftragte Zusatzleistungen, bei denen Wir Tätigkeiten aus dem Verantwortungsbereich des Kunden im Zusammenhang mit dem Wechsel in dessen Auftrag übernehmen. Damit der Kunde für Kosten aus den Datenverarbeitungsdiensten oder andere Leistungen, die unmittelbar im Zusammenhang mit dem Wechsel stehen, während des Übergangszeitraums keine oder eine etwaige anteilige separate Vergütung bezahlen muss, ist es erforderlich, dass der Kunde Uns rechtzeitig über den Wechsel informiert.

12.1.7 Ein Wechsel oder eine Löschung von Kundeninhalten verpflichten den Kunden nicht dazu, den Vertrag zu kündigen und führen auch nicht automatisch zu einer Vertragsbeendigung. Ebenso führt der Ablauf des Übergangszeitraums nicht automatisch zu einer Vertragsbeendigung. Der Kunde kann jedoch auch eine Kündigung des Vertrags für die Datenverarbeitungsdienste nach Maßgabe der vertraglichen Bestimmungen aussprechen. Der Kunde kann auch eine Vertragsbeendigung herbeiführen, indem er Uns vor Ablauf des Übergangszeitraums informiert.

12.1.8 Der Kunde arbeitet nach Treu und Glauben mit Uns zusammen, damit der Wechsel effektiv vollzogen wird, Kundendaten rechtzeitig übertragen werden können und die Kontinuität der Datenverarbeitungsdienste aufrechterhalten wird. Das beinhaltet insbesondere, dass der Kunde:

a) etwaige Hinweise oder Vorgaben von Uns zu erforderlichen Einstellungen oder Konfigurationen der Dienste befolgt,

b) vorgegebene Termine für Wechselaktivitäten einhält und Erklärungen abgibt, sowie alle erforderlichen Informationen rechtzeitig und vollständig bereitstellt,

c) innerhalb seines Verantwortungsbereichs angemessene Sicherungs- und Redundanzkonzepte für seine Kundeninhalte erstellt und implementiert,

d) ggf. vom Kunden in Vorbereitung eines Datenexports für erforderlich erachtete Maßnahmen zur Datenvalidierung, Datenbereinigung, Datenformatierung, etc. in den Datenverarbeitungsdiensten vornimmt,

e) den Export bzw. die Löschung der Daten durch entsprechende Eingaben und Einstellungen in den Datenverarbeitungsdiensten initiiert,

f) den Fortschritt eines laufenden Datenexports bzw. einer laufenden Datenlöschung überwacht, und für die Tätigkeit des Anbieters, zu dem er wechselt, sowie jedes ggf. vom Kunden im Rahmen des Wechsels eingesetzten Dienstleisters verantwortlich ist und deren Tätigkeiten selbst koordinieren muss.

12.1.9 Die vertraglich vereinbarten Bestimmungen bezüglich der Sicherheit von Kundeninhalten gelten auch im Falle eines Wechsels und somit auch während des Übergangszeitraums.

12.1.10 Wir weisen darauf hin, dass ein Wechsel insbesondere mit typischen Risiken verbunden ist, die sich aus dem Ausstieg aus Datenverarbeitungsdiensten ergeben und die speziell auf die Datenverarbeitungsdienste zurückgehen. Es obliegt dem Kunden, sich über die Risiken der Nutzung seiner IKT-Infrastruktur oder der Dienste eines anderen Anbieters, einschließlich einer Migration zu diesem Anbieter, zu informieren.

12.1.11 Mit Vertragsbeendigung wird der Zugriff der Berechtigten Nutzer des Kunden auf die Funktionen von Invecorum gesperrt. Die Anmeldung bleibt für die Dauer des Exportzeitraums zum Zweck des Exports der Kundeninhalte möglich: Der Kunde kann seine Kundeninhalte innerhalb eines Zeitraums von 30 Tagen nach Vertragsbeendigung exportieren. Nach Ablauf dieses Zeitraums werden die Daten des Kunden gelöscht. Das Recht beider Parteien zur außerordentlichen Kündigung bleibt hiervon unberührt.

13 Einseitige Änderung von Vertragsbestimmungen

13.1 Unser Recht den Vertrag zu ändern

Wir sind berechtigt, vertragliche Bestimmungen, die keine wesentlichen Vertragsinhalte wie die Vergütung oder die Vertragslaufzeit darstellen, nach billigem Ermessen (§ 315 BGB) und unter den Voraussetzungen des nachfolgenden Verfahrens anzupassen, soweit hierdurch nicht das Verhältnis zwischen vertraglich vereinbarter Leistung und

Gegenleistung (nachfolgend „Äquivalenzinteresse“) zulasten des Kunden verändert wird oder die Änderung dem Kunden im Übrigen unzumutbar ist.

13.2 Preisänderungen

Wir sind nur unter den folgenden Voraussetzungen berechtigt, Gebühren im Sinne der Ziffer 5 unter Berücksichtigung der Gesamtkosten, die für die Berechnung der vereinbarten Gebühren maßgeblich sind, anzupassen:

13.2.1 Die Gesamtkosten bestehen insbesondere aus den Kosten für die zur Bereitstellung von Invecorum erforderlichen, technischen Infrastruktur sowie die hierzu erforderlichen Energiekosten, den Servicekosten (insbesondere Kosten der zur Kundenbetreuung eingerichteten Kanäle) und Personalkosten (Lohn- und Lohnnebenkosten sowie Kosten von zur Leistungserbringung eingesetzten Dritt-Dienstleistern).

13.2.2 Eine Preiserhöhung kommt in Betracht und eine Preisermäßigung ist vorzunehmen, wenn sich die Gesamtkosten erhöhen oder absenken. Steigerungen bei einer Kostenart dürfen nur in dem Umfang für eine Preiserhöhung herangezogen werden, in dem kein Ausgleich durch rückläufige Kosten in anderen Bereichen erfolgt. Bei Kostensenkungen sind die Preise zu ermäßigen, soweit diese Preise nicht durch Steigerungen in anderen Bereichen ganz oder teilweise ausgeglichen werden.

13.2.3 Wir werden bei der Ausübung des billigen Ermessens die jeweiligen Zeitpunkte einer Preisänderung so wählen, dass Kostensenkungen nicht nach für den Kunden ungünstigeren Maßnahmen Rechnung getragen wird, also Kostensenkungen mindestens in gleichem Umfang preiswirksam werden wie Kostenerhöhungen. Wir werden keine Änderungen vornehmen, die einer Abwälzung vorherzusehender, wirtschaftlicher Risiken sowie Fehlkalkulationen und wirtschaftlicher oder technischer Fehlannahmen bei Vertragsschluss auf den Kunden dienen.

13.2.4 Unabhängig von der vorstehenden Regelung sind Wir für den Fall der Erhöhung der gesetzlichen Umsatzsteuer berechtigt und für den Fall einer Senkung verpflichtet, die Preise zum Zeitpunkt der jeweiligen Anpassung anzupassen.

13.3 Sonstige Änderungen

13.3.1 Wir sind nur unter den folgenden Voraussetzungen berechtigt, Invecorum einschließlich der Benutzeroberfläche, Dialogfelder sowie der Schnittstellen während der Vertragsdauer über das zur Aufrechterhaltung der Vertragsmäßigkeit erforderliche Maß nach freiem Ermessen zu ändern, was auch die Entfernung von Funktionen einschließt, um Invecorum an eine neue technische Umgebung, neue technische Entwicklungen und Funktionen insbesondere den aktuellen Stand der Technik, Kompatibilitätsanforderungen insbesondere von im Zusammenhang mit Invecorum verwendeter Hard- oder Software oder an eine erhöhte Nutzerzahl anzupassen und wenn dies aus anderen wichtigen betriebstechnischen oder lizenztechnischen Gründen erforderlich ist.

13.3.2 Die Berechtigung zur Änderung steht unter dem Vorbehalt, dass dem Kunden keine zusätzlichen Kosten entstehen und der Kunde klar und verständlich über die Änderung informiert wurde. Im Anwendungsbereich des § 327r BGB werden Wir, sofern durch die Änderung die Zugriffsmöglichkeit auf Invecorum oder die Nutzbarkeit von Invecorum mehr als nur unerheblich beeinträchtigt wird, den Kunden gemäß den Anforderungen des § 327r Abs. 2 BGB informieren. Dem Kunden stehen im vorgenannten Fall die unter § 327r Abs. 3 und Abs. 4 BGB beschriebenen Rechte zu.

13.4 Anpassungsverfahren

13.4.1 Wir werden den Kunden zum Zwecke einer Vertragsanpassung rechtsverbindlich eine Vertragsänderung anbieten (Anpassungsmitteilung).

13.4.2 Die Anpassungsmitteilung muss den Inhalt der angebotenen Vertragsänderung, das Änderungsdatum (d.h. der Wirksamkeitszeitpunkt der Vertragsänderung), die Berechtigung des Kunden, Uns gegenüber innerhalb einer Frist von einem Monat ab Zugang der Anpassungsmitteilung zu widersprechen, die Textformbedürftigkeit des Widerspruchs sowie die Rechtsfolge des Unterlassens des Widerspruchs durch den Kunden enthalten. Die Zustimmung zur Vertragsänderung gemäß Anpassungsmitteilung gilt als erteilt, wenn der Kunde nicht innerhalb von 30 Tagen nach Zugang der Anpassungsmitteilung in Textform ausdrücklich der Änderung widerspricht.

13.4.3 Bei form- und fristgerechtem Widerspruch bleiben die vertraglichen Bestimmungen unverändert. In diesem Fall kann Uns jedoch ein wichtiger Grund für eine außerordentliche Kündigung zustehen, insbesondere wenn Uns die Erbringung der Leistungen bis zur nächstmöglichen Vertragsbeendigung nicht mehr möglich oder zumutbar ist.

14 Allgemeine Bestimmungen

14.1 Anwendbares Recht

Auf diesen Vertrag findet das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Übereinkommens über den internationalen Warenkauf (CISG) und unter Ausschluss von Rück- und Weiterverweisungen Anwendung.

14.2 Gerichtsstand

Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit dem Vertrag zwischen Uns und einem Kunden, der Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist, ist München, Deutschland. Die Gerichtsstandsvereinbarung gilt nicht, wenn ein ausschließlicher

Gerichtsstand für die Klage oder das jeweilige Verfahren gesetzlich festgelegt ist oder eine Gerichtsstandsvereinbarung aus anderen Gründen unzulässig ist.

14.3 Streitbeilegung

Wir nehmen an einem freiwilligen Streitbeilegungsverfahren vor einer deutschen Verbraucherschlichtungsstelle derzeit nicht teil. Eine gesetzliche Verpflichtung besteht nicht.

14.4 Verhaltenskodizes

Wir haben Uns keinen Verhaltenskodizes unterworfen.

14.5 Änderungen

Änderungen oder Ergänzungen des Vertrages bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für die Änderung oder Aufhebung dieser Klausel. Abweichende individuelle Vertragsabreden haben Vorrang.

14.6 Schriftform

Soweit die Parteien vereinbart haben oder künftig vereinbaren, dass eine Erklärung zu ihrer Wirksamkeit der Schriftform bedarf, genügt zu deren Wahrung die telekommunikative Übermittlung mittels Telefax oder eine E-Mail, die den Anforderungen der Textform genügt, und im Falle des Abschlusses eines Vertrages der Austausch von der Schriftform genügenden Erklärungen.

14.7 Sprache

Soweit dieser Vertrag nicht nur in deutscher, sondern auch in englischer oder einer anderen Sprache ausgefertigt wird, hat im Falle von Abweichungen zwischen der deutschen Fassung und der anderssprachigen Fassung die deutsche Fassung Vorrang.

14.8 Salvatorische Klausel

Wenn eine Bestimmung des Vertrages ganz oder teilweise nicht Vertragsbestandteil geworden oder unwirksam oder undurchführbar ist oder wird, bleibt der Vertrag im Übrigen wirksam. Die unwirksame oder undurchführbare Bestimmung ist im Wege der Auslegung oder hilfsweise Umdeutung oder hilfsweise einer gesonderten Vereinbarung durch diejenige wirksame und durchführbare Bestimmung zu ersetzen, welche dem Sinn und Zweck der unwirksamen oder undurchführbaren Bestimmung entspricht oder am nächsten kommt, soweit der Inhalt des Vertrages dadurch nicht wesentlich geändert wird. Entsprechendes gilt für Vertragslücken.

*****

Anhang – Vereinbarung zur Auftragsverarbeitung

1 Gegenstand und Dauer des Auftrags

(1) Der Gegenstand des Auftrags ergibt sich aus dem in den vorstehenden Nutzungsbedingungen dargestellten Vertrag zwischen den Parteien (nachfolgend: „**Leistungsvereinbarung**“), auf deren Grundlage Wir (im Rahmen dieses Anhangs nachfolgend auch: „**Auftragnehmer**“) als Auftragsverarbeiter für den Kunden (im Rahmen dieses Anhangs nachfolgend auch: „**Auftraggeber**“) als Verantwortlichen IT-Dienstleistungen im Zusammenhang mit der Erbringung der Leistungen, insbesondere der Bereitstellung von Invecorum, erbringen. Die Leistungsvereinbarung umfasst auch die unentgeltliche Nutzung von Invecorum während der Testphase gemäß Ziffer 1.5 der Nutzungsbedingungen; diese Vereinbarung zur Auftragsverarbeitung gilt ab der Registrierung.

(2) Die Dauer und Kündbarkeit dieses Auftrags richten sich nach der Laufzeit und Kündbarkeit der Leistungsvereinbarung. Soweit der Vertrag auf unbestimmte Zeit geschlossen ist und nichts Abweichendes vereinbart ist (vgl. insoweit Ziffer 11 der Nutzungsbedingungen), ist der Vertrag nach Maßgabe der gesetzlichen Bestimmungen ordentlich kündbar. Das Recht zur außerordentlichen Kündigung bleibt unberührt.

Der Auftraggeber kann die Vereinbarung zur Auftragsverarbeitung jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung zur Auftragsverarbeitung 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 dieser Vereinbarung zur Auftragsverarbeitung vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

(3) Der Vertrag gilt unbeschadet des vorstehenden Absatzes 2 so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet (einschließlich Backups).

(4) Soweit sich aus anderen Vereinbarungen zwischen Auftraggeber und Auftragnehmer anderweitige Abreden zum Schutz personenbezogener Daten ergeben, hat diese Vereinbarung zur Auftragsverarbeitung in ihrem Anwendungsbereich Vorrang, es sei denn die Parteien vereinbaren ausdrücklich etwas anderes.

2 Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich aus dem Auftrag und sind darüber hinaus in der Leistungsvereinbarung konkret beschrieben. Die Verarbeitung umfasst insbesondere auch den anlassbezogenen Abruf, die Anzeige und den Versand von E-Mails über vom Auftraggeber angebundene Drittdienste, die Speicherung in Invecorum erstellter und versendeter E-Mails als Bestandteil von Chat-Verläufen sowie die Synchronisation und Speicherung von Dokumenten aus vom Auftraggeber angebundenen Ablagediensten (vgl. Ziffer 3.5 der Nutzungsbedingungen). Die Verarbeitung umfasst ferner die Verarbeitung von Eingaben und Kundendaten durch Sprachmodelle zur Erzeugung von Ergebnissen gemäß Ziffer 3.2 der Nutzungsbedingungen sowie die technische Verarbeitung von Dokumenten.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Bestandsdaten (Personen-Stammdaten, Namen oder Adressen)

- Kontaktdaten (Anschriften, E-Mail-Adressen und Telefonnummern)

- Inhaltsdaten (Texte, Bilddaten)

- E-Mail-Inhaltsdaten (Inhalte und Anhänge abgerufener, in Invecorum erstellter und versendeter E-Mails; abgerufene E-Mails werden lediglich temporär verarbeitet, versendete E-Mails als Bestandteil von Chat-Verläufen gespeichert)

- E-Mail-Metadaten (z. B. Absender, Empfänger, Betreff und Zeitstempel)

- Dokumente und Dateien einschließlich Metadaten aus vom Auftraggeber angebundenen Ablagediensten

- Nutzungsdaten (Zugriffszeiten und User-Account-Informationen)

- Meta-/Kommunikationsdaten (z.B. Geräte-Informationen, Endgerätedaten und IP-Adressen)

- Zugangs- und Authentifizierungsdaten (Passwörter sowie OAuth-Zugangs- und Refresh-Tokens für angebundene Drittdienste)

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Mandanten und deren Organe und Beschäftigte sowie sonstige im Zusammenhang mit der Mandatsbearbeitung durch den Auftraggeber betroffene Personen

- Interessenten und deren Organe und Beschäftigte

- Nutzer/Anwender der IT-Systeme des Auftraggebers

- Organe und Beschäftigte sowie Gesellschafter, insbesondere des Auftraggebers, von verbundenen Unternehmen des Auftraggebers und von Kooperationspartner des Auftraggebers

- Dienstleister/Lieferanten und deren Organe und Beschäftigte

- Kommunikationspartner des Auftraggebers und seiner Nutzer (z. B. Absender und Empfänger von E-Mails) sowie Personen, deren Daten in Dokumenten der angebundenen Ablagedienste enthalten sind

3 Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer ergreift in seinem Verantwortungsbereich alle erforderlichen technisch-organisatorischen Maßnahmen gem. Art. 32 DS-GVO zum Schutz der personenbezogenen Daten und übergibt dem Auftraggeber die Dokumentation zur Prüfung (Anlage „Technische und organisatorische Maßnahmen). Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Vertrags.

(2) Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(3) Die vereinbarten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer zukünftig gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Über wesentliche Änderungen, die durch den Auftragnehmer zu dokumentieren sind, ist der Auftraggeber unverzüglich in Kenntnis zu setzten.

4 Rechte von betroffenen Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich mittels geeigneter technisch-organisatorischer Maßnahmen bei der Beantwortung und Umsetzung von Anträgen betroffener Personen hinsichtlich ihrer Datenschutzrechte. Er darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers beauskunften, portieren, berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind die Rechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung sowie Datenportabilität nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat, zusätzlich zu der Einhaltung der Regelungen dieses Vertrags, eigene gesetzliche Pflichten gemäß der DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 Buchst. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die berechtigterweise Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten, einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

b) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

c) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

d) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten, einem anderen Anspruch oder einem Informationsersuchen im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

e) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

f) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 8 dieses Vertrags.

g) Der Auftragnehmer meldet Verletzungen des Schutzes personenbezogener Daten unverzüglich an den Auftraggeber in der Weise, dass der Auftraggeber seinen gesetzlichen Pflichten, insbesondere nach Art. 33, 34 DS-GVO nachkommen kann. Er fertigt über den gesamten Vorgang eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.

h) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung.

i) Soweit der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

(2) Dieser Vertrag entbindet den Auftragnehmer nicht von der Einhaltung anderer Vorgaben der DS-GVO.

6 Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers nach diesem Vertrag erbracht werden. 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 zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Der Auftraggeber stimmt der Beauftragung der in der Anlage „Unterauftragnehmer“ bezeichneten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO mit dem Unterauftragnehmer zu. Die vertragliche Vereinbarung mit dem Unterauftragnehmer wird dem Auftraggeber auf dessen Verlangen vorgelegt, wobei geschäftliche Klauseln ohne datenschutzrechtlichen Bezug hiervon ausgenommen sind.

Der Wechsel der gemäß der Anlage „Unterauftragnehmer“ eingesetzten Unterauftragnehmer ist zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, vorab schriftlich oder in Textform anzeigt und

- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und

- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung und Umsetzung der technisch-organisatorischen Maßnahmen beim Unterauftragnehmer wird unter Berücksichtigung des Risikos beim Unterauftragnehmer vorab der Verarbeitung personenbezogener Daten und sodann regelmäßig durch den Auftragnehmer kontrolliert. Der Auftragnehmer stellt dem Auftraggeber die Kontrollergebnisse auf Anfrage zur Verfügung. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Kontrollrechte) auch direkt gegenüber den Unterauftragnehmern wahrnehmen kann.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches

gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform). Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7 Internationale Datentransfers

(1) Jede Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation bedarf einer dokumentierten Weisung des Auftraggebers und bedarf der Einhaltung der Vorgaben zur Übermittlung personenbezogener Daten in Drittländer nach Kapitel V der DS-GVO.

(2) Soweit der Auftraggeber eine Datenübermittlung an Dritte in ein Drittland anweist, ist er für die Einhaltung von Kapitel V der DS-GVO verantwortlich.

8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, Überprüfungen bei dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Vor-Ort-Kontrollen, die in der Regel rechtzeitig, mindestens 14 Tage vorher, anzumelden und innerhalb der üblichen Geschäftszeiten des Betriebs des Auftragnehmers durchzuführen sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen. Die genannten Voraussetzungen für Vor-Ort-Kontrollen gelten nicht, soweit andernfalls (z.B. bei einer Anmeldung) der Kontrollzweck gefährdet wäre (z.B. bei besonderen Vorfällen wie der Verletzung des Schutzes personenbezogener Daten oder der Anordnung einer Kontrolle durch eine zuständigen Datenschutzbehörde oder anderen zuständigen Aufsichtsbehörde) oder soweit zwingende gesetzliche Bestimmungen entgegenstehen. Vor-Ort-Kontrollen sind so durchzuführen, dass Sie den Geschäftsbetrieb des Auftragnehmers in einem möglichst geringen Umfang beeinträchtigen.

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(4) Der Auftragnehmer ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse und -rechte des Auftraggebers und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

9 Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach Unionsrecht zu einer Verarbeitung verpflichtet. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform). Die anfänglichen Weisungen des Auftraggebers werden durch diesen Vertrag festgelegt. Die Anbindung eines Drittdienstes (Connectors) durch den Auftraggeber sowie die Nutzung der Connector-Funktionen (z. B. Abruf oder Versand einzelner E-Mails, Synchronisation angebundener Ablagen) gelten als dokumentierte Weisungen im Sinne dieses Absatzes. Der Auftragnehmer protokolliert die Anbindung und Trennung von Connectoren sowie die erteilten Zugriffsberechtigungen.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10 Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens aber mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

Papier und Datenträger mit Informationen, die dem Berufsgeheimnis (§ 43a Abs. 2 Satz 1 BRAO, § 203 Abs. 1 Nr. 3 StGB) unterliegen, sind nach DIN 66399 und mindestens nach Schutzklasse 3 und Sicherheitsstufe 4 zu vernichten.

(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.

(4) Trennt der Auftraggeber einen angebundenen Drittdienst (Connector), löscht der Auftragnehmer die zugehörigen Zugangstokens unverzüglich in seinen Systemen und widerruft sie bei dem Drittanbieter, soweit der Drittanbieter dies technisch unterstützt; Protokolldaten über die Anbindung und Trennung bleiben hiervon unberührt. Bereits in die Bibliothek synchronisierte Dokumente sowie in Chat-Verläufen gespeicherte E-Mails verbleiben als Bestandteil der Daten des Auftraggebers gespeichert, bis der Auftraggeber sie löscht oder die Leistungsvereinbarung endet; im letztgenannten Fall gilt Absatz 2.

*****

Anlage „Technisch und organisatorische Maßnahmen“ zum Anhang – Vereinbarung zur Auftragsverarbeitung

1 Vertraulichkeit

Physische Zutrittskontrolle von Personen

Der Auftragnehmer stellt sicher, dass seine Büro- und Geschäftsräume außerhalb der Büro- und Geschäftszeiten geschlossen sind.

Während der Büro- und Geschäftszeiten ist sichergestellt, dass sich Besucher oder sonstige Dritte nicht allein in Räumen bewegen können, in denen sie Zugang zu personenbezogenen Daten erhalten könnten.

Die Vergabe und Verwaltung von Schlüsseln erfolgt nach einem definierten Prozess, der die Erteilung und den Entzug von Zugangsberechtigungen zu Räumen sowohl zu Beginn als auch bei Beendigung eines Arbeitsverhältnisses regelt.

Rechenzentren

Die Server, auf denen Kundendaten gespeichert werden, befinden sich in Rechenzentren in Deutschland. Die physische Zutritts- und Zugangskontrolle zu den Rechenzentren erfolgt durch die Betreiber nach deren nach ISO/IEC 27001 zertifiziertem Informationssicherheitsmanagement. Die Übertragung von Daten an Unterauftragnehmer erfolgt ausschließlich über verschlüsselte Verbindungen.

System Zugangskontrolle

Um Zugang zu IT-Systemen zu erhalten, müssen der Auftragnehmer und seine Mitarbeiter über die entsprechende Zugangsberechtigung verfügen. Zu diesem Zweck werden von einem oder mehreren Administratoren entsprechende Benutzerberechtigungen vergeben.

Die Passwortvorgaben beinhalten eine Mindestlänge des Passwortes von 8 Zeichen, wobei das Passwort aus Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen bestehen muss.

Passwortänderungen werden nicht erzwungen.

Der Fernzugriff auf die IT-Systeme des Auftragnehmers erfolgt grundsätzlich über verschlüsselte Verbindungen.

Alle Server und Client-Systeme, die bei der Erbringung von Dienstleistungen für den Auftraggeber eingesetzt werden, sind durch Firewalls geschützt, die gewartet und mit aktuellen Updates und Patches versorgt werden.

Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen.

Passwörter, die der Auftragsverarbeiter von der verantwortlichen Stelle erhält oder für die IT-Systeme der verantwortlichen Stelle verwendet, werden stets verschlüsselt aufbewahrt und dürfen nur den Mitarbeitern zugänglich gemacht werden, die speziell mit der Erbringung von Dienstleistungen für die verantwortliche Stelle betraut sind.

Daten Zugangskontrolle

Die Berechtigungen für die IT-Systeme und -Anwendungen des Auftragsnehmers werden nach dem Need-to-know-Prinzip vergeben. Dementsprechend erhalten nur diejenigen Personen Zugriffsrechte auf Daten, Datenbanken oder Anwendungen, die diese Daten, Anwendungen oder Datenbanken pflegen und warten oder an deren Entwicklung beteiligt sind.

Anbindung von Drittdiensten (Connectoren)

Zugangstokens (OAuth) für vom Auftraggeber angebundene Drittdienste werden ausschließlich verschlüsselt gespeichert. Der Zugriff auf gespeicherte Zugangstokens ist nach dem Need-to-know-Prinzip beschränkt.

Bei der Anbindung von Drittdiensten werden nur die für die jeweilige Funktion erforderlichen Zugriffsberechtigungen (Scopes) angefordert; lesende Berechtigungen werden verwendet, soweit sie funktional ausreichend sind.

Die Anbindung und Trennung von Connectoren sowie die erteilten Zugriffsberechtigungen werden protokolliert.

Bei Trennung eines Connectors werden die zugehörigen Zugangstokens in den Systemen des Auftragnehmers unverzüglich gelöscht und, soweit der Drittanbieter dies technisch unterstützt, bei dem Drittanbieter widerrufen; die Entfernung aus Sicherungskopien erfolgt im Rahmen des regulären Sicherungszyklus.

Trennungskontrolle

Soweit der Auftragnehmer im Zusammenhang mit der Auftragsverarbeitung personenbezogene Daten vom Auftraggeber erhält, verarbeitet er diese getrennt von Daten anderer Auftraggeber. Dies gilt auch für Inhalte, die aus vom Auftraggeber angebundenen Drittdiensten synchronisiert oder abgerufen werden; diese werden logisch getrennt je Auftraggeber gespeichert.

Pseudonymisierung & Verschlüsselung

Der administrative Zugriff auf die IT-Systeme des Auftraggebers erfolgt grundsätzlich über verschlüsselte Verbindungen, soweit er nicht innerhalb der Räumlichkeiten des Auftraggebers erfolgt.

2 Integrität

Eingabekontrolle

Der Auftragnehmer hat Eingaben, Änderungen oder Löschungen personenbezogener Daten, die er im Auftrag des Auftraggebers vornimmt, in geeigneter Weise zu dokumentieren, es sei denn, es ist sichergestellt, dass das jeweilige IT-System selbst eine Protokollierung der entsprechenden Aktivitäten vornimmt.

Weitergabekontrolle

Personenbezogene Daten dürfen im Auftrag des Auftraggebers nur in dem Umfang weitergegeben werden, wie dies mit dem Auftraggeber vereinbart wurde.

Dem Auftragnehmer ist es untersagt, im Zusammenhang mit der Auftragsabwicklung für den Auftraggeber private Datenträger zu nutzen.

3 Verfügbarkeit und Belastbarkeit

Speichert oder verwaltet der Auftragnehmer personenbezogene Daten oder Zugangsdaten für den Auftraggeber, so hat er sicherzustellen, dass diese Daten mindestens täglich inkrementell und wöchentlich „vollständig“ gesichert werden. Es gibt ein Datensicherungskonzept, das auch das erfolgreiche Testen der Wiederherstellung von Daten beinhaltet.

4 Verfahren zum regelmäßigen Testen, Beurteilen und Evaluieren

Der Auftragnehmer trägt durch Richtlinien und/oder Anweisungen an die Mitarbeiter dazu bei, dass personenbezogene Daten in einer Weise verarbeitet werden, die den Anforderungen der DS-GVO entspricht.

Dazu gehört insbesondere eine regelmäßige Überprüfung der Wirksamkeit der zum Schutz personenbezogener Daten getroffenen Maßnahmen und erforderlichenfalls eine Anpassung.

Insbesondere wird sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich an den Auftraggeber gemeldet werden, wenn es sich um Daten handelt, die im Rahmen einer Auftragsverarbeitung für den Auftraggeber verarbeitet werden.

Auftragskontrolle

Bei der Einschaltung von externen Dienstleistern oder Dritten wird eine Auftragsverarbeitungsvereinbarung nach den Anforderungen des geltenden Datenschutzrechts abgeschlossen.

Die Auftragsverarbeiter werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Alle Maßnahmen, die gemäß Art. 25 DS-GVO im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftraggeber erforderlich sind, werden von dem Auftraggeber getroffen oder von ihm in ergänzenden Weisungen an den Auftragnehmer festgelegt.

*****

Anlage „Unterauftragnehmer“ zum Anhang – Vereinbarung zur Auftragsverarbeitung

Unterauftragnehmer	Adresse	Art der Verarbeitung
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen, Deutschland	Hosting, Datenbanken, Dokumentenverarbeitung und Logging. Standort der Server: Deutschland. Sämtliche eingesetzten Server sind durch eine gesonderte Zusatzvereinbarung zur Geheimhaltung nach § 203 StGB erfasst
IONOS SE	Elgendorfer Str. 57, 56410 Montabaur, Deutschland	Speicher, Dokumentenverarbeitung und GPU-Infrastruktur. Standort der Server: Deutschland
TensorX Ltd.	Unit 25, Classon House, Dundrum Business Park, Dublin 14, Irland	Sprachmodell-Infrastruktur und GPU-Infrastruktur, ausschließlich temporäre Verarbeitung ohne Speicherung, Protokollierung oder Training. Standort der Server: Europäische Union (Irland, Finnland). Gesonderte Vereinbarung zur Wahrung des Berufsgeheimnisses nach §§ 203, 204 StGB
Riecken Webservice & Application GmbH	Nussdorfer Straße 4/1/112, 1090 Wien, Österreich	Betrieb des Cloud Gateways für die DATEV-Anbindung (Ziffer 3.6): Weiterleitung von Anfragen und Daten zwischen Invecorum und den DATEV-Schnittstellen des Kunden sowie Ausstellung und Verwaltung der Zugangsdaten. Vertrag zur Auftragsverarbeitung vom 07.08.2026 und gesonderte Vereinbarung zur Wahrung des Berufsgeheimnisses nach §§ 203, 204 StGB (§ 62a StBerG). Riecken schließt zusätzlich eine

Unterauftragnehmer	Adresse	Art der Verarbeitung
		eigene Vereinbarung zur Auftragsverarbeitung unmittelbar mit dem Kunden
Scaleway SAS	8, rue de la Ville-l'Évêque, 75008 Paris, Frankreich	Versand der transaktionalen E-Mails (z.B. E-Mail-Bestätigung, Passwort-Zurücksetzen, Einladung von Mitgliedern)

*****