# Vereinbarung zur Auftragsverarbeitung

Stand 02.11.2026

**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) |

*****