



Vereinbarung zur Auftragsverarbeitung

Rechnella · Fassung 2026-10-03

gemäß Art. 28 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, DSGVO)

Vertragsparteien

Auftraggeber: Das im Nutzungsvertrag und bei der Anlage der jeweiligen Firma bezeichnete Unternehmen, vertreten durch die zum Vertragsschluss berechnigte Person (nachfolgend „Auftraggeber“).

Auftragnehmer: c.hil GmbH, Walderseest. 33, 30177 Hannover, eingetragen beim Amtsgericht Hannover unter HRB 221452, vertreten durch den Geschäftsführer Carsten Hilber (nachfolgend „Auftragnehmer“).

Kontakt des Auftragnehmers für Datenschutz und Weisungen: Carsten Hilber, c.hil GmbH, info@chil-gmbh.de. Dieser Kontakt ist Ansprechpartner und wird hierdurch nicht als Datenschutzbeauftragter bezeichnet.

Kontakt des Auftraggebers: Die im Kundenkonto für die jeweilige Firma hinterlegte Kontaktperson und E-Mail-Adresse. Der Auftraggeber kann einen abweichenden Datenschutzkontakt und gegebenenfalls seinen Datenschutzbeauftragten in Textform mitteilen.

Diese Vereinbarung ergänzt den Vertrag über die Nutzung von Rechnella („Hauptvertrag“). Sie wird einschließlich der Anlagen 1 bis 3 für die jeweilige Kundenfirma geschlossen. Identität, Anschrift und Mandantenzuordnung des Auftraggebers ergeben sich aus den zum Vertragsschluss gespeicherten Vertragsdaten. Für den elektronischen Abschluss ist eine handschriftliche Unterschrift nicht erforderlich.

§ 1 Gegenstand, Rollen und Dauer

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers, um Rechnella als internetbasierte Anwendung bereitzustellen, zu betreiben, zu warten und zu unterstützen. Art und Zweck der Verarbeitung, Datenarten und Kategorien betroffener Personen sind in Anlage 1 beschrieben.
2. Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO. Er bestimmt die Zwecke und wesentlichen Mittel der Verarbeitung und verantwortet insbesondere deren Rechtsgrundlagen, die Information betroffener Personen und die Rechtmäßigkeit seiner Weisungen. Die eigenen gesetzlichen Pflichten des Auftragnehmers bleiben unberührt.
3. Diese Vereinbarung gilt ab ihrem Abschluss, vor Beginn der Verarbeitung von Auftragsdaten, einschließlich einer kostenlosen Testphase. Ihre Dauer entspricht der Laufzeit des Hauptvertrags. Für nach Vertragsende verbleibende Daten gelten ihre Pflichten bis zur vollständigen Löschung fort.
4. Für jede Kundenfirma besteht eine eigene Zuordnung zum jeweiligen Verantwortlichen. Zugriffsrechte eines Benutzers für mehrere Firmen berechnen nicht zur Zusammenführung ihrer Daten. Soll der Auftraggeber seinerseits als Auftragsverarbeiter für Dritte handeln, ist die entsprechende Unterauftragskette vor dieser Nutzung gesondert zu vereinbaren.

5. Soweit der Auftragnehmer Daten zur Abrechnung seines eigenen Vertrags, zur Erfüllung eigener gesetzlicher Pflichten oder zur Wahrung eigener rechtlicher Ansprüche verarbeitet, handelt er insoweit als eigener Verantwortlicher. Diese Verarbeitung wird in den Datenschutzhinweisen gesondert erläutert und begründet kein Recht zur freien Verwendung der Rechnungs- oder Beleginhalte.

§ 2 Weisungen und Zweckbindung

1. Der Auftragnehmer verarbeitet Auftragsdaten ausschließlich auf dokumentierte Weisung des Auftraggebers. Hauptvertrag, diese Vereinbarung sowie bestimmungsgemäße Eingaben, Einstellungen und Aktionen berechtigter Benutzer bilden die anfänglichen Weisungen. Dies gilt auch für Übermittlungen personenbezogener Daten in ein Drittland.
2. Weitere Weisungen werden in Textform, insbesondere per E-Mail, erteilt und dokumentiert. Dringende mündliche Weisungen sind unverzüglich in Textform zu bestätigen. Der Auftragnehmer darf bei Zweifeln die Weisungsberechtigung prüfen. Beide Parteien halten ihre Kontaktangaben aktuell.
3. Hält der Auftragnehmer eine Weisung für einen Verstoß gegen die DSGVO oder andere Datenschutzbestimmungen der Union oder ihrer Mitgliedstaaten, informiert er den Auftraggeber unverzüglich. Er darf die betroffene Verarbeitung bis zur rechtmäßigen Klärung aussetzen. Eine erkennbar rechtswidrige Weisung wird nicht ausgeführt; erforderliche Maßnahmen zum Schutz der Daten bleiben zulässig.
4. Ist der Auftragnehmer durch Unionsrecht oder das Recht eines Mitgliedstaats zu einer Verarbeitung verpflichtet, informiert er den Auftraggeber vorab über diese rechtliche Verpflichtung, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet.
5. Die Nutzung von Auftragsdaten für eigene Werbung, Datenhandel, personenbezogene Profilbildung oder das Training von KI-Modellen ist ausgeschlossen. Auswertungen ohne Personen- und Firmenbezug nach § 16 der AGB dürfen nur aus wirksam anonymisierten Daten erfolgen. Soweit hierfür zunächst personenbezogene Auftragsdaten anonymisiert werden sollen, ist eine gesonderte dokumentierte Weisung erforderlich; bis zur wirksamen Anonymisierung gelten sämtliche Pflichten dieser Vereinbarung.

§ 3 Vertraulichkeit und Sicherheit

1. Der Auftragnehmer setzt nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Er unterrichtet sie über die einschlägigen Datenschutzpflichten. Die Vertraulichkeit besteht über das Ende ihrer Tätigkeit hinaus fort.
2. Berechtigungen und Zugriffe sind auf das für die jeweilige Aufgabe erforderliche Maß zu beschränken. Support- und Administrationszugriffe dürfen nur zur Auftragerfüllung, auf Weisung oder zur notwendigen Störungs- und Sicherheitsbehandlung erfolgen und sind angemessen nachvollziehbar zu dokumentieren.
3. Der Auftragnehmer trifft alle nach Art. 32 DSGVO erforderlichen Maßnahmen. Dabei berücksichtigt er Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen. Die vereinbarten Mindestmaßnahmen ergeben sich aus Anlage 2.
4. Die Wirksamkeit der Maßnahmen ist regelmäßig und bei wesentlichen Änderungen zu überprüfen. Gleichwertige technische Weiterentwicklungen sind zulässig, sofern das vereinbarte Schutzniveau nicht abgesenkt wird. Wesentliche Änderungen sind zu dokumentieren und dem Auftraggeber mitzuteilen; die aktualisierte Maßnahmenbeschreibung ist bereitzustellen.
5. Pflichten des Auftraggebers zur Sicherung seiner Endgeräte, Zugangsdaten und eigenen Exporte ersetzen nicht die Sicherheits- und Wiederherstellungspflichten des Auftragnehmers.

§ 4 Betroffenenrechte und Unterstützung

1. Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung durch geeignete technische und organisatorische Maßnahmen bei der Erfüllung der Pflichten zur Beantwortung von Anträgen nach Kapitel III DSGVO. Dies betrifft insbesondere Auskunft, Berichtigung, Löschung, Einschränkung und Datenübertragbarkeit.
2. An ihn gerichtete Anfragen betroffener Personen zu Auftragsdaten leitet der Auftragnehmer unverzüglich an den Auftraggeber weiter. Inhaltlich beantwortet er diese nur auf Weisung oder aufgrund einer eigenen gesetzlichen Verpflichtung.
3. Unter Berücksichtigung der Art der Verarbeitung und der ihm verfügbaren Informationen unterstützt der Auftragnehmer den Auftraggeber bei den Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei Sicherheitsbewertungen, der Behandlung von Datenschutzverletzungen, Datenschutz-Folgenabschätzungen und vorherigen Konsultationen der Aufsichtsbehörde.
4. Informationen und Unterstützung werden so rechtzeitig bereitgestellt, dass der Auftraggeber seine gesetzlichen Fristen einhalten kann. Gesetzlich erforderliche Unterstützung darf nicht von einer vorherigen Einigung über zusätzliche Vergütung abhängig gemacht werden. Über darüber hinausgehende Leistungen können die Parteien eine gesonderte Vergütung vereinbaren. Die Beseitigung eigener Pflichtverletzungen des Auftragnehmers wird nicht zusätzlich berechnet.

§ 5 Datenschutzverletzungen

1. Der Auftragnehmer meldet dem Auftraggeber eine ihm bekannt gewordene Verletzung des Schutzes personenbezogener Auftragsdaten unverzüglich. Die Erstmeldung darf nicht bis zur vollständigen Aufklärung oder bis zur eigenen abschließenden Risikobewertung zurückgestellt werden.
2. Soweit bekannt, enthält die Meldung die Art der Verletzung, deren Zeitpunkt oder Zeitraum, die Kategorien und ungefähre Zahl betroffener Personen und Datensätze, einen Ansprechpartner, die wahrscheinlichen Folgen sowie ergriffene oder vorgeschlagene Maßnahmen zur Behebung und Abmilderung.
3. Fehlende Angaben werden ohne unangemessene weitere Verzögerung schrittweise nachgereicht. Der Auftragnehmer dokumentiert den Vorfall, sichert geeignete Nachweise, ergreift unverzüglich erforderliche Schutzmaßnahmen und stimmt weitere Schritte mit dem Auftraggeber ab.
4. Die Entscheidung über Meldungen an Aufsichtsbehörden und betroffene Personen trifft der Auftraggeber, soweit keine eigene gesetzliche Pflicht des Auftragnehmers besteht. Die Frist von 72 Stunden nach Art. 33 Abs. 1 DSGVO ist keine Wartefrist für die Benachrichtigung durch den Auftragnehmer.

§ 6 Unterauftragsverarbeiter

1. Der Auftraggeber erteilt die allgemeine schriftliche Genehmigung zum Einsatz weiterer Auftragsverarbeiter unter den Bedingungen dieser Vorschrift. Bei Vertragsschluss sind die in Anlage 3 genannten Unternehmen für die dort beschriebenen Leistungen genehmigt.
2. Der Auftragnehmer informiert den Auftraggeber mindestens 30 Kalendertage vor einer beabsichtigten Hinzuziehung oder Ersetzung in Textform über Unternehmen, Tätigkeit, betroffene Daten, Verarbeitungsorte und gegebenenfalls Drittlandgarantien. Eine bloße Änderung einer Webseite genügt nicht.
3. Der Auftraggeber kann innerhalb dieser Frist aus datenschutzbezogenen Gründen widersprechen. Die Parteien suchen eine geeignete Alternative. Bis zur Klärung werden dem beanstandeten neuen Dienstleister keine Daten des Auftraggebers zugänglich gemacht. Ist keine zumutbare Lösung möglich,

kann jede Partei die betroffene Leistung zum vorgesehenen Wechsel außerordentlich kündigen. Bereits bezahlte Entgelte für danach entfallende Leistungen sind zu erstatten.

4. Vor Beginn der Verarbeitung hat der Auftragnehmer die Eignung des Dienstleisters zu prüfen und ihm durch Vertrag im Wesentlichen dieselben Datenschutzpflichten aufzuerlegen, die in dieser Vereinbarung festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen. Dies umfasst Unterstützung, Kontrollen, Rückgabe und Löschung sowie die Absicherung weiterer Unterauftragsketten.
5. Der Auftragnehmer kontrolliert die Einhaltung angemessen und bleibt gegenüber dem Auftraggeber für die Erfüllung der Datenschutzpflichten des weiteren Auftragsverarbeiters voll verantwortlich. Er hält eine aktuelle Übersicht auch über relevante weitere Unterauftragsketten vor und stellt sie dem Auftraggeber auf Anforderung bereit. Änderungen dieser Ketten sind nach den vorstehenden Informations- und Widerspruchsregeln zu behandeln.
6. Externe Wartung, Support, Monitoring oder Mailversand sind einzubeziehen, soweit dabei Auftragsdaten verarbeitet werden. Reine Softwarelieferanten ohne Datenzugriff sind nicht allein deshalb Unterauftragsverarbeiter. Vom Auftraggeber bestimmte Empfänger, etwa seine Kanzlei, Bank oder Rechnungskunden, werden nicht allein durch den Empfang zu Unterauftragsverarbeitern des Auftragnehmers.

§ 7 Verarbeitungsorte und Drittlandübermittlungen

1. Für den Anwendungsbetrieb und die Datensicherung wird Deutschland, für den E-Mail-Dienst die Schweiz als Verarbeitungsort vereinbart. Einzelheiten ergeben sich aus Anlage 3. Diese Festlegung umfasst auch Administration und Fernzugriffe. Weitere Länder dürfen nur unter Einhaltung dieser Vorschrift und des § 6 einbezogen werden.
2. Für die Übermittlung an den in Anlage 3 genannten Schweizer Dienstleister gilt der Angemessenheitsbeschluss der Europäischen Kommission für die Schweiz nach Art. 45 DSGVO als Übermittlungsgrundlage, solange dieser wirksam und auf die betreffende Verarbeitung anwendbar ist. Der Auftraggeber weist den Auftragnehmer mit Abschluss dieser Vereinbarung an, die für den beauftragten Maildienst erforderlichen Daten dorthin zu übermitteln.
3. Andere Verarbeitungen außerhalb des EU/EWR bedürfen einer vorherigen dokumentierten Weisung oder Zustimmung des Auftraggebers und der Einhaltung von Kapitel V DSGVO. Empfänger, Land, Zweck, Datenumfang und Übermittlungsgrundlage sind zu dokumentieren. Soweit erforderlich, sind geeignete Garantien, eine Transferbewertung und ergänzende Schutzmaßnahmen vorzusehen. Diese AVV allein ist keine Übermittlungsgrundlage nach Kapitel V DSGVO.
4. Entfällt eine erforderliche Übermittlungsgrundlage, informiert der Auftragnehmer den Auftraggeber unverzüglich und setzt betroffene Übermittlungen aus, bis eine rechtmäßige Grundlage besteht. Vom Auftraggeber veranlasste Sendungen an eigene Empfänger in Drittländern müssen ebenfalls zulässig sein; der Auftraggeber stellt hierfür die erforderliche Grundlage sicher. Eigene Pflichten des Auftragnehmers bleiben unberührt.

§ 8 Nachweise, Kontrollen und Behörden

1. Der Auftragnehmer stellt alle zum Nachweis der Einhaltung von Art. 28 DSGVO erforderlichen Informationen zur Verfügung. Er ermöglicht Überprüfungen einschließlich Inspektionen durch den Auftraggeber oder einen von ihm beauftragten Prüfer und trägt dazu bei.
2. Zunächst können geeignete aktuelle Dokumentationen, Prüfberichte und vorhandene Zertifikate genutzt werden. Sie ersetzen das Kontrollrecht nicht, wenn sie zur Prüfung nicht ausreichen. Eine bestimmte Zertifizierung des Auftragnehmers wird nicht zugesagt.

3. Regelmäßige Kontrollen werden mit angemessener Vorankündigung zu üblichen Geschäftszeiten durchgeführt. Bei Vorfällen, begründetem Verdacht oder behördlichen Anforderungen müssen auch kurzfristige Kontrollen möglich sein. Eine starre jährliche Höchstzahl besteht nicht.
4. Prüfer sind zur Vertraulichkeit zu verpflichten. Betrieb, Sicherheit, Geschäftsgeheimnisse und Daten anderer Kunden sind zu schützen, ohne die effektive Kontrolle zu vereiteln. Jede Partei trägt grundsätzlich ihre eigenen internen Kosten; Ansprüche wegen Pflichtverletzungen bleiben unberührt.
5. Der Auftragnehmer informiert den Auftraggeber unverzüglich über behördliche Maßnahmen, Ermittlungen, Beschlagnahmen oder Ansprüche Dritter, soweit sie Auftragsdaten betreffen und die Mitteilung rechtlich zulässig ist. Er wirkt im gesetzlichen Umfang mit der zuständigen Aufsichtsbehörde zusammen.

§ 9 Rückgabe und Löschung

1. Nach Ende der Verarbeitungsleistungen löscht der Auftragnehmer nach Wahl des Auftraggebers sämtliche Auftragsdaten oder gibt sie zurück und löscht danach vorhandene Kopien, sofern keine unions- oder mitgliedstaatliche Rechtsvorschrift ihn selbst zur weiteren Speicherung verpflichtet. Erfasst sind auch Dokumente, Anhänge und zugehörige personenbezogene Metadaten.
2. Entsprechend § 14 der AGB kann der Auftraggeber bis 30 Kalendertage nach Vertragsende einmalig einen Export in einem gängigen maschinenlesbaren Format verlangen. Bis dahin werden die Daten ausschließlich zur Rückgabe und Abwicklung geschützt vorgehalten. Ohne abweichende Weisung gilt als vereinbart, dass der Auftragnehmer nach Ablauf dieser 30 Tage die Daten aus aktiven Systemen unverzüglich löscht. Eine zulässige frühere Löschweisung wird unverzüglich umgesetzt.
3. Die Rückgabe umfasst die strukturierten Geschäftsdaten und vorhandenen Originaldokumente in gängigen Formaten, beispielsweise JSON, CSV, XML und PDF entsprechend dem jeweiligen Datenbestand. Die Übertragung erfolgt über einen authentifizierten verschlüsselten Download oder einen gleichwertig gesicherten Übertragungsweg. Ein bloßer Export von Stammdaten ohne zugehörige Belege genügt nicht.
4. Sicherungskopien werden mit den regulären Sicherungszyklen gelöscht oder überschrieben, spätestens innerhalb von 60 Kalendertagen nach Löschung der betreffenden Daten aus aktiven Systemen. Diese Höchstfrist gilt auch für lokale Kopien, Snapshots, replizierte Bestände und Sicherungen bei Unterauftragsverarbeitern. Für aktive Supportkopien und sonstige aktive Nebenbestände gilt Absatz 2.
5. Verbliebene Sicherungsdaten sind für den regulären Zugriff gesperrt und dürfen nur zur erforderlichen Wiederherstellung verwendet werden. Bereits vollzogene Löschungen sind vor erneuter regulärer Nutzung wiederhergestellter Daten erneut umzusetzen. Auf Anforderung bestätigt der Auftragnehmer die Löschung und benennt gegebenenfalls noch vorhandene Sicherungen und deren endgültigen Löschtermin.
6. Bei eigener gesetzlicher Speicherpflicht benennt der Auftragnehmer Rechtsgrundlage, betroffene Daten und Dauer, beschränkt die Verarbeitung auf diesen Zweck und löscht nach Wegfall der Pflicht. Aufbewahrungspflichten des Auftraggebers begründen allein keine Speicherpflicht des Auftragnehmers. Die Anwendung übernimmt keine dauerhafte handels- oder steuerrechtliche Archivierung für den Auftraggeber.
7. Sperrung, Deaktivierung oder die Kennzeichnung eines Mandanten als „gelöscht“ ersetzen keine tatsächliche Löschung. Technische Unveränderlichkeit von Rechnungen entbindet nicht von einem wirksamen datenschutzrechtlichen Löschverfahren. Rechte auf Berichtigung, Einschränkung oder Löschung während der Vertragslaufzeit bleiben unberührt und werden nach Weisung unterstützt.

§ 10 Haftung und Vertragsrang

1. Zwingende gesetzliche Haftung, insbesondere Rechte betroffener Personen nach Art. 82 DSGVO, bleibt unberührt. Diese Vereinbarung beschränkt weder Rechte betroffener Personen noch Befugnisse von Aufsichtsbehörden.
2. Im Übrigen gelten die wirksam vereinbarten Haftungsregelungen des Hauptvertrags, insbesondere § 12 der AGB, soweit zwingendes Recht nicht entgegensteht. Die Verantwortlichkeit nach Art. 28 Abs. 4 DSGVO bleibt unberührt.
3. Bei Widersprüchen geht diese Vereinbarung einschließlich ihrer Anlagen den AGB und sonstigen Vertragsbedingungen in Fragen der Auftragsverarbeitung vor. Allgemeine Leistungsbeschränkungen und Klauseln zu höherer Gewalt heben gesetzliche Datenschutzpflichten nicht auf.

§ 11 Abschluss und Änderungen

1. Der Abschluss erfolgt schriftlich oder in einem elektronischen Format gemäß Art. 28 Abs. 9 DSGVO. Beim elektronischen Abschluss werden Vertragsparteien, Kundenfirma, handelnde Person, Zeitpunkt und die konkrete Fassung einschließlich Anlagen nachvollziehbar dokumentiert. Der Auftraggeber erhält die Möglichkeit, die Vertragsfassung dauerhaft zu speichern.
2. Änderungen bedürfen einer dokumentierten Vereinbarung in schriftlichem oder elektronischem Format. Die ausdrücklich geregelten Verfahren für gleichwertige Sicherheitsmaßnahmen und Unterauftragsverarbeiter bleiben unberührt.
3. Im Übrigen gelten Rechtswahl und Gerichtsstandsregelung des Hauptvertrags, soweit wirksam und datenschutzrechtlich zulässig.

Anlage 1 — Beschreibung der Verarbeitung

1. Gegenstand und Zwecke

Bereitstellung von Rechnella für die Geschäftsprozesse der beauftragenden Firma: Kunden- und Lieferantenverwaltung; Erstellung und Verwaltung von Ausgangsrechnungen einschließlich Korrekturen und Stornierungen; Erfassung, Auslesen und Bearbeitung von Eingangsrechnungen und Belegen; Rechnungs- und Belegversand; Buchhaltungsexporte; Zahlungsabgleich, Zahlungserinnerungen und Mahnwesen. Hinzu kommen Benutzer- und Berechtigungsverwaltung, Datensicherung, Wiederherstellung, auftragsbezogene Wartung und Unterstützung.

Erfasst sind jeweils nur die vereinbarten und genutzten Funktionen. Optionale Bankanbindungen oder andere Integrationen setzen eine dokumentierte Aktivierung sowie die vorherige Klärung der Empfänger- und Unterauftragskette voraus.

2. Art, Häufigkeit und Dauer

Fortlaufende Verarbeitung durch Eingabe, Upload oder beauftragten Import; Erfassen, Ordnen, Speichern, Auslesen, Abgleichen, Berechnen, Verändern, Abrufen, Exportieren und Übermitteln an bestimmte Empfänger; Einschränken, Sichern, Wiederherstellen und Löschen. Supporteinsicht ist auf das erforderliche Maß begrenzt. Die Verarbeitung dauert während der Nutzung an; Rückgabe und Löschung richten sich anschließend nach § 9.

3. Datenarten

- Stamm- und Kontaktdaten: Namen, personenbezogene Firmenbezeichnungen, Anschriften, Ansprechpartner, E-Mail-Adressen, Telefonnummern sowie Kunden- und Lieferantenummern.
- Rechnungs- und Vertragsdaten: Rechnungsnummern, Leistungsbeschreibungen, Leistungszeiträume, Mengen, Preise, Beträge, steuerliche Angaben und Identifikatoren, Belege, Anhänge, Freitexte und Korrekturbezüge.
- Zahlungs- und Bankdaten: Kontoinhaber, IBAN/BIC, Zahlungsziele, Umsätze, Verwendungszwecke, Zahlungszuordnungen, offene Posten und Mahndaten; bei beauftragter Bankanbindung erforderliche Zugangsmittel.
- Kommunikationsdaten: Empfänger, Absender, Betreff, Nachrichtentexte, Anhänge, Versandzeitpunkte und Versandstatus.
- Benutzer- und Nachweisdaten: Namen, E-Mail-Adressen, Benutzerkennungen, Mandantenzuordnungen, Rollen, Authentifizierungsdaten, Aktionen und Zeitstempel.
- Technische Betriebsdaten: IP-Adressen, Zugriffs- und Fehlerprotokolle sowie notwendige Supportinformationen, soweit mit Personenbezug im Auftrag verarbeitet.

4. Betroffene Personen

Kunden, Interessenten, Rechnungsempfänger, Lieferanten und sonstige Geschäftspartner des Auftraggebers; deren Beschäftigte und Ansprechpartner; Beschäftigte, freie Mitarbeiter, Benutzer und Bevollmächtigte des Auftraggebers; weitere natürliche Personen in Belegen, Bankumsätzen und auftragsbezogener Kommunikation, insbesondere Zahlungspflichtige und Zahlungsempfänger.

5. Besonders schutzbedürftige Daten

Die reguläre Leistung ist nicht auf Daten nach Art. 9 oder Art. 10 DSGVO ausgerichtet. Belege und Leistungsbeschreibungen können solche Daten dennoch offenbaren, etwa Gesundheitsdaten bei medizinischen Rechnungen. Ihre beabsichtigte Verarbeitung bedarf vorab einer gesonderten Vereinbarung zu Umfang und zusätzlichen Schutzmaßnahmen; der Auftraggeber stellt die erforderliche Rechtsgrundlage sicher. Unbeabsichtigt enthaltene sensible Daten unterliegen dennoch dem Schutz dieser AVV. Die Parteien stimmen unverzüglich den rechtmäßigen Umgang damit ab.

Anlage 2 — Technische und organisatorische Maßnahmen

Die folgenden Maßnahmen werden als verbindliche Anforderungen an den Betrieb vereinbart. Der Auftragnehmer hat sie vor Beginn der jeweiligen Verarbeitung umzusetzen, während der Verarbeitung aufrechtzuerhalten und ihre Wirksamkeit nachzuweisen. Diese Anlage ist keine Zertifizierung oder Prüfbescheinigung.

1. Physische Sicherheit

Der Auftragnehmer nutzt für den Anwendungsbetrieb die Rechenzentrumsinfrastruktur von Hetzner in Nürnberg und für die Datensicherung Hetzner Object Storage in Falkenstein. Er hat sich anhand geeigneter Anbieternachweise von Zutrittsbeschränkungen, kontrolliertem Besucherzugang und Schutz gegen Stromausfall, Brand und sonstige Umwelteinflüsse zu überzeugen. Endgeräte für Administration und Support sind gegen unbefugten Zugriff und Verlust zu schützen.

2. Benutzerzugang und Berechtigungen

Für die Anmeldung ist die selbst betriebene Identitätskomponente Keycloak vorgesehen. Personenbezogene Konten, rollenbasierte Berechtigungen und die Prüfung der Mandantenzugehörigkeit begrenzen den Zugriff. Benutzerverwaltung und fachliche Berechtigungen unterscheiden insbesondere Administration, Buchhaltung und Lesezugriff. Nicht mehr benötigte Rechte sind zeitnah zu entziehen; Berechtigungen sind regelmäßig und bei personellen Änderungen zu überprüfen.

Technische Administrationszugänge sind besonders zu schützen, insbesondere durch schlüsselbasierte Anmeldung und Beschränkung der zugelassenen Netzwerkzugänge. Für Betreiberkonten ist Mehrfaktorauthentifizierung einzusetzen. Gemeinsame unkontrollierte Administrationskonten sind zu vermeiden. Zugangsmittel sind vor Offenlegung zu schützen und bei einem Kompromittierungsverdacht unverzüglich zu erneuern.

3. Mandantentrennung und interne Zugriffe

Die Anwendung hat Zugriffe je Firma gegen die Berechtigungen des angemeldeten Benutzers zu prüfen. Mandantenbezogene Schlüssel und Row-Level Security in PostgreSQL sichern die Datentrennung zusätzlich ab. Die Laufzeitrolle der Anwendung darf diese Trennung nicht durch Superuser- oder Umgehungsrechte außer Kraft setzen; Migrations- und Laufzeitberechtigungen sind zu trennen.

Betreiberrechte in der Anwendung gewähren nicht automatisch fachlichen Zugriff auf Rechnungsdaten. Erforderliche technische Administrations- und Supportzugriffe sind auf die Aufgabe zu begrenzen und nachvollziehbar zu dokumentieren. Entwicklungs- und Testzwecke verwenden grundsätzlich synthetische Daten; produktive Auftragsdaten dürfen hierfür nur auf gesonderte rechtmäßige Weisung und mit geeigneten Schutzmaßnahmen verwendet werden.

4. Übertragung und Geheimnisse

Browserzugriffe sind durch HTTPS mit aktuellen TLS-Verfahren zu schützen. Datenbank und interne Anwendungsdienste dürfen nicht unmittelbar aus dem öffentlichen Internet erreichbar sein. Der Versand zum Mailrelay ist über eine verschlüsselte TLS-Verbindung zu konfigurieren. Gewöhnlicher SMTP-Versand beinhaltet keine zugesagte Ende-zu-Ende-Verschlüsselung bis zum Empfänger.

Geheimnisse, Datenbankzugänge und Sicherheitsschlüssel sind zugriffsbeschränkt zu verwalten und von öffentlich zugänglichem Quellcode fernzuhalten. Vertrauliche Exporte werden ausschließlich über einen authentifizierten verschlüsselten Download oder ein gleichwertig geschütztes Verfahren bereitgestellt.

5. Protokollierung und Integrität

Wesentliche fachliche und sicherheitsrelevante Vorgänge sind mit erforderlicher Kennung und Zeitpunkt nachvollziehbar zu protokollieren. Protokolle sind vor unbefugtem Zugriff und Manipulation zu schützen. Passwörter, Schlüssel und unnötige Inhaltsdaten dürfen nicht protokolliert werden. Die Speicherung ist nach Zweck zu begrenzen und durch ein dokumentiertes Löschkonzept zu steuern.

Mandantenzuordnung und Dokumentintegrität sind auch bei Downloads, Exporten und Mailversand zu prüfen. Prüfsummen und festgehaltene Dokumentversionen dienen der Integritätskontrolle. Schutz vor unbefugter Veränderung darf die Umsetzung rechtmäßiger Löschweisungen nicht verhindern.

6. Sicherung und Wiederherstellung

Die getrennten PostgreSQL-Datenbanken von Rechnella und der Identitätsverwaltung sind über CloudNativePG mit täglichen Basisbackups und fortlaufender Archivierung der Transaktionsprotokolle (WAL) zu sichern. Die Ablage erfolgt in privaten, voneinander abgegrenzten Sicherungsarchiven im Hetzner Object Storage in Falkenstein. Vorgesehen ist ein Wiederherstellungsfenster von 30 Tagen; erforderliche Basisbackups und vollständige WAL-Ketten sind zusammenhängend zu verwalten. Ein Wiederherstellungsfenster ist keine Zusage, dass jeder einzelne Sicherungsbestand nach exakt 30 Tagen gelöscht wird. Die absolute Löschhöchstfrist nach § 9 Abs. 4 bleibt verbindlich.

Sicherungen sind verschlüsselt zu speichern und verschlüsselt zu übertragen. Das konkrete Verschlüsselungsverfahren und die Wiederherstellung der unabhängig vom Anwendungsserver verwahrten Schlüssel sind vor Aufnahme der Verarbeitung zu testen und zu dokumentieren. Eine automatische Verschlüsselung durch den Speicheranbieter wird nicht vorausgesetzt.

Server-Backups und VM-Snapshots sind nicht Bestandteil des Sicherungskonzepts. Alle unersetzlichen Auftragsdaten einschließlich Dokumenten und Anhängen müssen von den Datenbanksicherungen erfasst sein. Server, Kubernetes-Ressourcen und Dienste werden aus versionierter Konfiguration wiederaufgebaut; erforderliche Wiederanlaufunterlagen und Zugangsmittel sind unabhängig vom Anwendungsserver vorzuhalten.

Sicherungsläufe, Archivierungsrückstand, Speicherauslastung und externe Erreichbarkeit sind zu überwachen; Fehler sind zeitnah zu behandeln. Wiederherstellungen beider Datenbanken einschließlich zeitpunktbezogener Wiederherstellung sind vor Aufnahme des Betriebs, monatlich und nach wesentlichen Änderungen des Sicherungsverfahrens zu erproben und zu dokumentieren. Nach getrenntem Restore sind Benutzeridentitäten und Firmenberechtigungen abzugleichen; unklare Berechtigungen bleiben gesperrt. Der Einzelserverbetrieb ist keine Hochverfügbarkeitslösung. Eine bestimmte Wiederherstellungszeit wird hierdurch nicht zugesagt; die Pflicht zur rechtzeitigen Wiederherstellung nach Art. 32 DSGVO bleibt bestehen.

7. Wartung und organisatorische Kontrolle

Der Auftragnehmer führt ein dokumentiertes Verfahren für Sicherheitsupdates, Schwachstellen und Änderungen. Maßnahmen sind nach Risiko zu priorisieren; sicherheitskritische Befunde sind unverzüglich zu bewerten und erforderliche Abhilfen ohne unangemessene Verzögerung umzusetzen. Zugriffe externer Dienstleister sind zu kontrollieren.

Personen mit Datenzugriff sind zur Vertraulichkeit zu verpflichten und angemessen zu Datenschutz und sicherem Umgang mit Daten zu unterweisen. Die Maßnahmen sind regelmäßig sowie anlassbezogen auf Wirksamkeit zu prüfen; Abweichungen und ihre Beseitigung sind zu dokumentieren. Nachweise werden im Rahmen des § 8 zugänglich gemacht.

8. Vorfälle, Rückgabe und Löschung

Der Auftragnehmer hält Verfahren für die Erkennung, Bewertung und Behandlung von Datenschutzvorfällen sowie für Betroffenenanfragen vor. Die Geschäftsführung ist über info@chil-gmbh.de erreichbar und hat die Bearbeitung eingehender Meldungen und Weisungen sicherzustellen.

Export- und Löschverfahren müssen auch Archivtabellen, Anhänge, Benutzerzuordnungen, Supportkopien und Unterauftragsverarbeiter erfassen. Für firmenübergreifend genutzte Benutzerkonten sind die Daten der betroffenen Firma zu entfernen; rechtmäßig für andere Firmen benötigte Kontodaten bleiben getrennt erhalten. Sperrung allein genügt nicht. Bei Wiederherstellung sind bereits vollzogene Löschungen erneut anzuwenden.

Anlage 3 — Genehmigte Unterauftragsverarbeiter

1. Hetzner — Anwendungsbetrieb und Datensicherung

Unternehmen: Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland.

Leistung: Bereitstellung des Cloud-Servers, der Netzwerk- und Datenträgerinfrastruktur sowie des Object Storage für Sicherungen. Anwendung, Kubernetes (k3s), PostgreSQL/CloudNativePG und Keycloak werden durch c.hil auf dieser Infrastruktur betrieben.

Datenumfang: Auftragsdaten gemäß Anlage 1 einschließlich Dokumenten, Benutzer- und Authentifizierungsdaten sowie verschlüsselten Sicherungen. Zugriffe sind auf die für die beauftragte Infrastrukturleistung erforderlichen Tätigkeiten zu beschränken.

Vereinbarte Standorte: Anwendungsserver in Nürnberg; Sicherungsspeicher in Falkenstein, jeweils Deutschland. Administration und Support dürfen Daten nicht ohne das Verfahren nach §§ 6 und 7 in anderen Ländern verarbeiten.

2. Infomaniak — E-Mail-Dienst

Unternehmen: Infomaniak Network AG, Rue Eugène Marziano 25, 1227 Les Acacias, Genf, Schweiz; UID CHE-103.167.648.

Leistung: E-Mail-Versand über den Maildienst, insbesondere Rechnungen, Belege, Zahlungserinnerungen und Mahnungen sowie Kontobestätigungen und Passwortnachrichten, soweit die jeweilige Funktion genutzt wird.

Datenumfang: Absender, Empfänger, Betreff, Nachrichteninhalte, Anhänge sowie erforderliche Zustell- und technische Metadaten. Ein Zugriff auf die gesamte Rechnungsdatenbank ist nicht Bestandteil des Auftrags.

Vereinbarer Standort: Schweiz, einschließlich dienstbezogener Speicherung und Sicherungen. Grundlage der Übermittlung ist der Angemessenheitsbeschluss der Europäischen Kommission für die Schweiz nach Art. 45 DSGVO.

3. Gemeinsame Bedingungen

Mit beiden Dienstleistern hat der Auftragnehmer vor Verarbeitung der Auftragsdaten Vereinbarungen nach Art. 28 Abs. 4 DSGVO abzuschließen und geeignete Schutzmaßnahmen sowie die Einhaltung der Rückgabe- und Löschpflichten sicherzustellen. Relevante Nachweise und Informationen zu weiteren Unterauftragsketten stellt er nach § 8 bereit. Eine Anbieter-Webseite ersetzt nicht die vereinbarten Datenschutzpflichten.

Weitere direkte Unterauftragsverarbeiter sind durch diese Anlage nicht genehmigt. Ihr Einsatz sowie Änderungen von Dienstleistern, Unterauftragsketten oder Verarbeitungsorten richten sich nach §§ 6 und 7. Die Nutzung weiterer Produkte eines genannten Anbieters, insbesondere KI-Dienste, wird durch die hier genannte Beauftragung nicht mitgenehmigt.