# Allgemeine Geschäftsbedingungen ephios ASP

Baumann & Rindt Softwareentwicklung GbR

2024-10-10

## Inhalt

## § 1 Allgemeines

Diese AGB gelten für alle Verträge zwischen der Baumann & Rindt Softwareentwicklung GbR – im Folgenden "Provider" genannt – und den vertraglich berechtigten Nutzern dieser Software – im Folgenden "Kunden" genannt.

## § 2 Vertragsgegenstand

1. Vertragsgegenstand ist die Software "ephios" (nachfolgend kurz Software), die auf Servern im Einflussbereich des Providers bereitgestellt wird. Sie dient der Organisation und Personalplanung für Dienste und andere Veranstaltungen von Hilfsorganisationen.
2. Mit diesem Vertrag wird dem Kunden die Nutzungsmöglichkeit für die Software über einen Internetzugang im Rahmen eines Application Service Providing (ASP) eingeräumt. Der Kunde darf die Software für eigene Zwecke nutzen, seine Daten verarbeiten und speichern.
3. Die Software, die für die Nutzung erforderliche Rechnerleistung sowie der notwendige Speicherplatz für Daten werden vom Provider oder einem von ihm beauftragten Dritten (z.B. einem Rechenzentrum) bereitgehalten. Der dem Kunden zugewiesene Systembereich ist gegen den Zugriff Dritter geschützt.
4. Der Zugang des Kunden zum Internet ist nicht Gegenstand dieses Vertragsverhältnisses. Der Kunde trägt die alleinige Verantwortung für die Funktionsfähigkeit seines Internet-Zugangs einschließlich der Übertragungswege sowie seines eigenen Computers.
5. Der Provider führt keine Aufgaben für den Kunden durch.
6. Der Provider übermittelt dem Kunden die für die Softwarenutzung erforderlichen Zugangsdaten zur Identifikation und Authentifikation. Dem Kunden ist es nicht gestattet, diese Zugangsdaten Dritten zu überlassen.

## § 3 Leistungen des Providers

1. Auf dem Server werden die Inhalte unter der Internet-Adresse des Providers zum Abruf über das Internet bereitgehalten. Die Leistungen des Providers bei der Übermittlung von Daten beschränken sich allein auf die Datenkommunikation zwischen dem vom Provider betriebenen Übergabepunkt des eigenen Datenkommunikationsnetzes an das Internet und dem für den Kunden bereitgestellten Server. Eine Einflussnahme auf den Datenverkehr außerhalb des eigenen Kommunikationsnetzes ist dem Provider nicht möglich. Eine erfolgreiche Weiterleitung von Informationen von oder zu dem die Inhalte abfragenden Rechner ist daher insoweit nicht geschuldet.
2. Die Einzelheiten zur Systemverfügbarkeit sind in den Service Level Agreements im Anhang geregelt. Der Provider sichert die Daten des Kunden in regelmäßigen Abständen. Insbesondere trifft er Vorkehrungen gegen Datenverluste aufgrund von Computerabstürzen sowie gegen Zugriffe durch unbefugte Dritte. Die Sicherung erfolgt stets für den gesamten Serverinhalt und umfasst unter Umständen auch die Daten weiterer Kunden. Der Kunde hat daher keinen Anspruch auf Herausgabe eines der Sicherungsmedien. Im Notfall können aber gesicherte Inhalte auf den Server zurücküberspielt werden. Jenseits von Notfällen hat der Kunde keinen Anspruch auf Rückübertragung.
3. Der Provider ist berechtigt, die zur Erbringung der Leistungen eingesetzte Hard- und Software an den jeweiligen Stand der Technik anzupassen. Ergeben sich aufgrund einer solchen Anpassung zusätzliche Anforderungen an die vom Kunden auf dem Server abgelegten Inhalte, um das Erbringen der Leistungen des Providers zu gewährleisten, so wird der Provider dem Kunden diese zusätzlichen Anforderungen mitteilen. Der Kunde wird unverzüglich nach Zugang der Mitteilung darüber entscheiden, ob die zusätzlichen Anforderungen erfüllt werden sollen und bis wann dies geschehen wird. Erklärt der Kunde nicht bis spätestens vier Wochen vor dem Umstellungszeitpunkt, dass er seine Inhalte rechtzeitig zur Umstellung, das heißt spätestens drei Werktage vor dem Umstellungszeitpunkt, an die zusätzlichen Anforderungen anpassen wird, hat der Provider das Recht, das Vertragsverhältnis mit Wirkung zum Umstellungszeitpunkt zu kündigen.

## § 4 Funktionsumfang

1. Die vom Provider zu erbringenden Serviceleistungen werden im Service Level Agreement (SLA) detailliert festgelegt. Das SLA wird als Anhang zu diesem Vertrag geführt und ist Teil der vertraglichen Übereinkunft.
2. Der Provider ist berechtigt, den Inhalt der Serviceleistungen einschließlich der bereitgestellten Software zu verändern und anzupassen, insbesondere bei technologischen Weiterentwicklungen. Bei Wegfall wesentlicher Funktionsbestandteile wird er den Kunden spätestens einen Monat vor der Änderung in Kenntnis setzen. In diesem Fall steht dem Kunden ein Sonderkündigungsrecht mit einer Frist von zwei Wochen zum Änderungstermin zu.
3. Nicht in 2. eingeschlossen sind Funktionen, die als "experimentell", "beta" o.ä. gekennzeichnet sind und vom Provider ohne weitere Ankündigung abgeändert oder entfernt werden können.

## § 5 Mitwirkungspflichten des Kunden

1. Bei der Umschreibung, Eingrenzung, Feststellung und Meldung von Störungen muss der Kunde die vom Provider erteilten Hinweise befolgen. Gegebenenfalls muss der Kunde vom Provider zur Verfügung gestellte Checklisten zur Beschreibung verwenden.
2. Der Kunde muss seine Störungsmeldungen und Fragen nach Kräften präzisieren. Er muss hierfür gegebenenfalls auf kompetente Mitarbeiter zurückgreifen.
3. Der Kunde führt regelmäßige Datensicherungen durch und trifft geeignete Maßnahmen zur Sicherung seines eigenen Computers, z.B. den Einsatz eines Virenschutzprogrammes in aktueller Version.
4. Der Kunde verhindert den unbefugten Zugriff Dritter auf die Software und verpflichtet auch weitere Benutzer in seiner Zuständigkeit zur Einhaltung dieser Pflicht.
5. Der Kunde verpflichtet sich, auf dem zur Verfügung gestellten Speicherplatz keine rechtswidrigen, die Gesetze, behördlichen Auflagen oder Rechte Dritter verletzenden Inhalte abzulegen.
6. Der Kunde darf insbesondere nicht
   a. beleidigende oder verleumderische Inhalte, pornografische, gewaltverherrlichende, missbräuchliche, sittenwidrige oder Jugendschutzgesetze verletzende Inhalte, Waren oder Dienstleistungen bewerben, anbieten oder vertreiben;
   b. andere Nutzer unzumutbar belästigen, insbesondere durch Spam (vgl. § 7 Gesetz gegen den unlauteren Wettbewerb – UWG);
   c. gesetzlich (z. B. durch das Urheber-, Marken-, Patent-, Geschmacksmuster- oder Gebrauchsmusterrecht) geschützte Inhalte verwenden, ohne dazu berechtigt zu sein;
   d. gesetzlich geschützten Waren oder Dienstleistungen, ebenfalls ohne dazu berechtigt zu sein, bewerben, anbieten oder vertreiben;
   e. wettbewerbswidrige Handlungen, einschließlich progressiver Kundenwerbung (wie Ketten-, Schneeball- oder Pyramidensysteme) vornehmen oder fördern.
7. Der Kunde ist verpflichtet, die folgenden belästigenden Handlungen zu unterlassen, auch wenn diese konkret keine Gesetze verletzen sollten:
   a. Versendung von Kettenbriefen;
   b. Durchführung, Bewerbung und Förderung von Strukturvertriebsmaßnahmen (wie Multi-Level-Marketing oder Multi-Level-Network-Marketing); sowie Vornahme von anzüglicher oder sexuell geprägter Kommunikation (explizit oder implizit).
   c. jede Handlung, die geeignet ist, die Funktionalität der Infrastruktur des Providers zu beeinträchtigen, insbesondere diese übermäßig zu belasten.
8. Der Kunde ist dafür verantwortlich, dass die von ihm über das Angebot des Providers veröffentlichten Inhalte allen anwendbaren gesetzlichen Bestimmungen und behördlichen Auflagen entspricht. Hierzu zählen beispielhaft die Impressumspflicht, die Pflichten nach Art. 13 und 14 DSGVO und die Beachtung bestehender Urheberrechte. Der Kunde stellt den Provider von jeglicher Inanspruchnahme durch Dritte einschließlich der durch die Inanspruchnahme ausgelösten Kosten frei.
9. Im Falle eines unmittelbar drohenden oder eingetretenen Verstoßes gegen die vorstehenden Verpflichtungen sowie bei der Geltendmachung nicht offensichtlich unbegründeter Ansprüche Dritter gegen den Provider auf Unterlassen der vollständigen oder teilweisen Darbietung der auf dem Server abgelegten Inhalte über das Internet ist der Provider berechtigt, unter Berücksichtigung auch der berechtigten Interessen des Kunden die Anbindung dieser Inhalte an das Internet ganz oder teilweise mit sofortiger Wirkung vorübergehend einzustellen. Der Provider wird den Kunden über diese Maßnahme unverzüglich informieren.
10. Die von dem Kunden auf dem Server abgelegten Inhalte können urheber- und datenschutzrechtlich geschützt sein. Der Kunde räumt dem Provider das Recht ein, die von ihm auf dem Server abgelegten Inhalte bei Abfragen über das Internet zugänglich machen zu dürfen, insbesondere sie hierzu zu vervielfältigen und zu übermitteln sowie sie zum Zwecke der Datensicherung vervielfältigen zu können. Der Kunde prüft in eigener Verantwortung, ob die Nutzung personenbezogener Daten durch ihn datenschutzrechtlichen Anforderungen genügt.
11. Der Kunde sichert zu, dass alle durch ihn angegebenen Daten der Wahrheit entsprechen, sowie dass er kein Verbraucher im Sinne des § 13 BGB ist. Diese Angaben sind auf Anfrage durch den Provider nachzuweisen. Bei Änderungen der Firmierung, Anschrift, Bankverbindung, Ansprechpartner oder Kontaktdaten informiert der Kunde den Provider unverzüglich.

## § 6 Reseller-Ausschluss

Der Kunde darf die vom Provider zur Verfügung gestellten Leistungen Dritten nicht zur gewerblichen Nutzung überlassen.

## § 7 Vergütung

1. Der Kunde hat für die von ihm gewählten Funktionalitäten die sich aus der bei Vertragsschluss gültigen Preisliste des Providers ergebenden Entgelte zu zahlen.
2. Der Provider ist berechtigt, die seinen Leistungen zugrunde liegende Preisliste nach billigem Ermessen (§ 315 Abs. 3 BGB) zu ändern. Der Provider wird den Kunden über Änderungen in der Preisliste spätestens sechs Wochen vor Inkrafttreten der Änderungen in Textform informieren.
3. Das Entgelt wird nach Kalendermonaten berechnet. Die Rechnungsstellung erfolgt zum ersten Tag des vereinbarten Abrechnungszeitraums.
4. Wenn keine andere Zahlungsweise schriftlich vereinbart wurde, wird der Kunde den fälligen Betrag auf das Konto des Providers überweisen.
5. Der Provider stellt alle Rechnungen in Euro aus und empfängt Zahlungen ebenfalls ausschließlich in der Währung Euro.

## § 8 Vertragsschluss, Vertragslaufzeit und Kündigungen

1. Die Software wird auf der Seite ephios.de vorgestellt. Die Darstellung dort stellt kein rechtlich verbindendes Vertragsangebot dar. Der Vertrag kommt zustande, indem zunächst der Kunde auf der oben genannten Seite ein Angebot auf Abschluss des Vertrages abgibt und dann der Provider eine Erklärung abgibt, dass er den Antrag des Kunden auf Vertragsschluss annimmt.
2. Die betriebsfähige Bereitstellung der vereinbarten Leistungen erfolgt unmittelbar nach der Mitteilung des Providers über den Vertragsschluss.
3. Der ASP-Vertrag läuft auf unbestimmte Zeit. Er kann mit einer Frist von 7 Tagen zum Ende des vereinbarten Abrechnungszeitraums in Textform gekündigt werden.
4. Bei Neukunden ist der Vertrag abweichend zu 3. zunächst auf einen entgeltfreien Testzeitraum von wenigstens 4 Wochen befristet. Der Kunde hat die Möglichkeit den Vertrag kostenpflichtig auf unbestimmte Zeit zu verlängern.
5. Das Recht der Vertragsparteien zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist bleibt unberührt. Ein wichtiger Grund liegt insbesondere vor, wenn
   a. ein Vertragspartner die in diesem Vertrag ausdrücklich geregelten Pflichten grob verletzt,
   b. über das Vermögen der anderen Vertragspartei das Insolvenzverfahren eröffnet wird oder die andere Vertragspartei insolvent oder zahlungsunfähig wird,
   c. der Kunde in einem Zeitraum, der sich über mehr als zwei Monate erstreckt, mit der Entrichtung des Entgelts in Höhe eines Betrags in Verzug ist, der das Entgelt für zwei Kalendermonate erreicht,
   d. die Inhalte der vom Kunden publizierten Materialien rechtswidrige, sittenwidrige, volksverhetzende, rechtsradikale, gewaltverherrlichende oder sonstwie menschenverachtende Bestandteile enthalten,
   e. die Inhalte der vom Kunden publizierten Materialien dazu geeignet sind, den Ruf des Providers grob zu schädigen oder
   f. der Provider begründeten Anlass zur Vermutung hat, dass der Kunde in betrügerischer oder missbräuchlicher Absicht tätig ist.
6. Für den Kunden kann ein wichtiger Grund in einer erheblichen Unterschreitung der vereinbarten Verfügbarkeit der Software liegen; hiervon ist regelmäßig bei einem Unterschreiten um mehr als 10% auszugehen.

## § 9 Recht des Providers zur Sperrung bei Zahlungsverzug des Kunden

1. Der Kunde ist zur fristgerechten Zahlung des Entgelts verpflichtet. Bei einem Verzug von über 14 Tagen ist der Provider zur Sperrung des Zugangs berechtigt. Der Vergütungsanspruch bleibt von einer solchen Zugangssperrung unberührt. Die erneute Freischaltung erfolgt unmittelbar nach der Begleichung der Rückstände.
2. Die Verfolgung weitergehender Ansprüche, etwa nach dem Urheberrechtsgesetz, sowie insbesondere auch von sonstigen Schadensersatzansprüchen bleibt in allen Fällen vorbehalten.

## § 10 Mängelansprüche und Kündigungsrecht des Kunden

1. Mängel der Software einschließlich der Handbücher und sonstiger Unterlagen werden vom Provider nach entsprechender Mitteilung des Mangels durch den Kunden innerhalb der im SLA festgelegten Reaktionszeit behoben. Gleiches gilt für sonstige Störungen der Möglichkeit zur Softwarenutzung. Für die Mängelansprüche gilt mietvertragliches Mängelrecht.
2. Der Kunde darf eine Entgeltminderung nicht durch Abzug vom vereinbarten Entgelt durchsetzen. Entsprechende Bereicherungs- oder Schadensersatzansprüche bleiben unberührt.
3. Das Kündigungsrecht des Kunden wegen Nichtgewährung des Gebrauchs nach § 543 Absatz 2 Satz 1 Nr. 1 des Bürgerlichen Gesetzbuchs ist ausgeschlossen, sofern nicht die Herstellung des vertragsgemäßen Gebrauchs als

fehlgeschlagen anzusehen ist.
4. Der Kunde hat dem Provider Mängel unverzüglich anzuzeigen. Die Mängelansprüche verjähren in einem Jahr.

## § 11 Haftung

1. Die Haftung des Providers für Schäden aufgrund der Nutzung von Telekommunikationsdienstleistungen für die Öffentlichkeit richtet sich nach den Regelungen des Telekommunikationsgesetzes.
2. Außerhalb des Anwendungsbereichs von Absatz (1) richtet sich die Haftung nach den folgenden Bestimmungen. Der Provider haftet unbeschränkt nur für Vorsatz und grobe Fahrlässigkeit auch seiner gesetzlichen Vertreter und leitenden Angestellten. Für das Verschulden sonstiger Erfüllungsgehilfen wird die Haftung auf das Fünffache des durchschnittlichen monatlichen Entgelts begrenzt.
3. Für leichte Fahrlässigkeit haftet der Provider nur bei Verletzung einer wesentlichen Vertragspflicht, deren Erfüllung die ordnungsgemäße Durchführung des Vertrags überhaupt erst ermöglicht und auf deren Einhaltung der Kunde regelmäßig vertrauen darf (Kardinalpflicht) sowie bei Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit. Der Provider haftet dabei nur für vorhersehbare Schäden, mit deren Entstehung typischerweise gerechnet werden muss. Die Haftung ist im Falle leichter Fahrlässigkeit auf das Fünffache des durchschnittlichen monatlichen Entgelts begrenzt.
4. Die Haftung für Datenverlust wird auf den typischen Wiederherstellungsaufwand beschränkt, der bei regelmäßiger und gefahrentsprechender Anfertigung von Sicherungskopien eingetreten wäre. Für den Verlust von Daten und/oder Programmen haftet der Provider insoweit nicht, als der Schaden darauf beruht, dass es der Kunde unterlassen hat, Datensicherungen durchzuführen und dadurch sicherzustellen, dass verloren gegangene Daten mit vertretbarem Aufwand wiederhergestellt werden können.
5. Der Kunde erkennt an, dass eine 100%ige Verfügbarkeit der Software technisch nicht zu erreichen ist. Insbesondere Wartungs-, Sicherheits- oder Kapazitätsbelange sowie Ereignisse, die nicht im Machtbereich des Providers stehen (wie z. B. Stromausfälle, Störungen von öffentlichen Kommunikationsnetzen etc.), können zu Störungen oder zur vorübergehenden Einstellung des Dienstes führen. Der Provider haftet gegenüber dem Kunden nicht für Beeinträchtigungen des Betriebes in Folge von Ereignissen, welche nicht in seinem Einflussbereich liegen, insbesondere höherer Gewalt und Dienstleistungen, welche durch Partnerunternehmen des Providers erbracht werden.

## § 12 Datenschutz und Geheimhaltung

1. Der Provider gewährleistet die datenschutzrechtliche Sicherheit der vom Kunden eingestellten Daten und beachtet die gesetzlichen Vorschriften zum Datenschutz, insbesondere das Telemediengesetz, das Telekommunikationsgesetz und das Bundesdatenschutzgesetz in der jeweils geltenden Fassung.
2. Der Provider unterrichtet hiermit den Kunden, personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen, soweit dies für die Durchführung des ASP notwendig ist. Der Kunde ist damit einverstanden, dass seine Daten vom Provider gespeichert, übermittelt, gelöscht und gesperrt werden, soweit dies unter Abwägung der berechtigten Belange des Kunden und des Zwecks dieses Vertrags notwendig ist. Hierbei handelt es sich um eine Auftragsverarbeitung im Sinne von Art. 28 DSGVO, während der Kunde Verantwortlicher i.S.d. DSGVO bleibt. Die Vertragsparteien schließen zu diesem Zweck einen Auftragsverarbeitungsvertrag, der als Anlage B zu diesen AGB geführt wird.
3. Der Provider wird alle Informationen und Daten vertraulich behandeln, die ihm im Rahmen der Abwicklung dieses Vertragsverhältnisses vom Kunden zugänglich gemacht werden. Der Provider ist ferner verpflichtet, den unbefugten Zugriff Dritter auf die Informationen und Daten des Kunden durch geeignete Vorkehrungen zu verhindern.
4. Der Provider ist verpflichtet, die Geheimhaltung gegenüber Dritten auch durch seine Mitarbeiter sicherzustellen.
5. Die Geheimhaltungspflicht gilt nach Vertragsende noch drei weitere Jahre.
6. Bei Vertragsende wird der Provider dem Kunden auf Wunsch sämtliche Daten online übermitteln. Der Kunde hat keinen Anspruch darauf, eine Software zur Verwendung der Daten zu erhalten. Nach einer Kontrolle der Daten durch den Kunden wird der Provider sämtliche Daten des Kunden löschen. Die Daten des Kunden bleiben in Sicherungskopien noch bis zu drei Monate nach der Löschung enthalten.

## § 13 Änderung der Vertragsbedingungen

1. Soweit nicht bereits anderweitig speziell geregelt, ist der Provider berechtigt, diese Vertragsbedingungen wie folgt zu ändern oder zu ergänzen. Der Provider wird dem Kunden die Änderungen oder Ergänzungen spätestens sechs Wochen vor ihrem Wirksamwerden in Textform ankündigen. Ist der Kunde mit den Änderungen oder Ergänzungen der Vertragsbedingungen nicht einverstanden, so kann er den Änderungen mit einer Frist von einer Woche zum Zeitpunkt des beabsichtigten Wirksamwerdens der Änderungen oder Ergänzungen widersprechen.

2. Der Widerspruch bedarf der Textform. Widerspricht der Kunde nicht, so gelten die Änderungen oder Ergänzungen der Vertragsbedingungen als von ihm genehmigt. Der Provider wird den Kunden mit der Mitteilung der Änderungen oder Ergänzungen der Vertragsbedingungen auf die vorgesehene Bedeutung seines Verhaltens besonders hinweisen.

### § 14 Abtretung, Zurückbehaltungsrecht, Aufrechnung

1. Die Abtretung von Forderungen ist nur mit vorheriger schriftlicher Zustimmung der anderen Vertragspartei zulässig. Die Zustimmung darf nicht unbillig verweigert werden. Die Regelung des § 354a HGB bleibt hiervon unberührt.
2. Ein Zurückbehaltungsrecht kann nur wegen Gegenansprüchen aus dem jeweiligen Vertragsverhältnis geltend gemacht werden.
3. Die Vertragsparteien können nur mit Forderungen aufrechnen, die rechtskräftig festgestellt oder unbestritten sind.

### § 15 Schriftform

Sämtliche Vereinbarungen, die eine Änderung, Ergänzung oder Konkretisierung dieser Vertragsbedingungen beinhalten, sowie besondere Zusicherungen und Abmachungen sind schriftlich niederzulegen. Werden sie von Vertretern oder Hilfspersonen des Providers erklärt, sind sie nur dann verbindlich, wenn der Provider hierfür seine schriftliche Zustimmung erteilt.

### § 16 Salvatorische Klausel

Sollten einzelne Bestimmungen der Parteivereinbarungen ganz oder teilweise unwirksam sein oder werden, wird die Wirksamkeit der übrigen Bestimmungen hierdurch nicht berührt. Die Parteien verpflichten sich für diesen Fall, die ungültige Bestimmung durch eine wirksame Bestimmung zu ersetzen, die dem wirtschaftlichen Zweck der ungültigen Bestimmung möglichst nahe kommt. Entsprechendes gilt für etwaige Lücken der Vereinbarungen.

### § 17 Rechtswahl

Die Parteien vereinbaren hinsichtlich sämtlicher Rechtsbeziehungen aus diesem Vertragsverhältnis die Anwendung des Rechts der Bundesrepublik Deutschland.

### § 18 Gerichtsstand

Für sämtliche Streitigkeiten, die im Rahmen der Abwicklung dieses Vertragsverhältnisses entstehen, wird Potsdam als Gerichtsstand vereinbart.

---

## Anlage A: Service Level Agreement und Technische Spezifikation

### § 1 Funktion und Verfügbarkeit

1. Der Funktionsumfang der Software umfasst insbesondere
   - das Verwalten von Nutzer*innenaccounts sowie das Verwalten und Zuweisen von Qualifikationen,
   - das Erstellen und Anzeigen von Veranstaltungsterminen mit einem gruppenbasierten Rechtesystem,
   - das Verwalten von mehreren Schichten pro Veranstaltung mit individuell auswählbaren Anmeldeverfahren für die Teilnehmenden,
   - die Registrierung für die Teilnahme an Veranstaltungen durch Nutzer*innen und die Einteilung durch Verantwortliche,
   - Benachrichtigungen per E-Mail, Push sowie einen Kalenderexport.
   - das Erfassen und Betrachten von geleisteten Arbeitsstunden,
   - die Nutzung in einer mobiloptimierten Ansicht sowie als "Progressive Web App" auf den Mobilgeräten der Nutzer*innen und
   - die Nachverfolgung der in der Software getätigten Aktionen ("Audit-Log").
2. Die Software steht dem Kunden grundsätzlich rund um die Uhr zur Verfügung. Im Jahresmittel wird eine jährliche Mindestverfügbarkeit von 98,5 % zugesagt. Höhere Gewalt oder Störungen außerhalb des Einflussbereichs des Providers sind hiervon ausgenommen. Wartungsarbeiten, die zu einem kurzfristigen Ausfall des Systems führen können, werden dem Kunden mindestens 48 Stunden vorher per E-Mail angekündigt. Ausgenommen hiervon

sind solche Arbeiten, die zur Vermeidung oder Abwendung einer konkreten Gefahr (z.B. Sicherheitslücken) oder zur Behebung einer Störung kurzfristig notwendig sind. Für Funktionen, die mit "experimentell", "beta" o.ä. gekennzeichnet sind, gilt weiterhin keine Verfügbarkeitszusage.
3. Es werden geeignete, branchenübliche Maßnahmen getroffen, um die Sicherheit der Daten gegenüber unberechtigtem Zugriff sicherzustellen. Hierzu gehört der Einsatz aktueller Softwareversionen und die Verschlüsselung der Kommunikation nach aktuellen Standards. Es werden keine durch die Nutzer vergebenen Passwörter im Klartext auf unseren Servern gespeichert.
4. Der Provider fertigt mindestens einmal täglich Sicherungskopien der Daten an, die für mindestens eine Woche gespeichert werden. Die Wiederherstellung von Daten aus den Backups ist kostenlos, sofern der Anlass der Wiederherstellung durch den Provider verschuldet wurde. Andernfalls wird die Wiederherstellung nach Aufwand berechnet.

## § 2 Störungen und Support

1. Der Provider strebt an, alle technischen Störungen innerhalb von 48 Stunden nach Eingang einer ausreichend aussagekräftigen Meldung zu beheben. Aufgrund der technischen Komplexität mancher Störungen kann dies jedoch nicht verbindlich zugesagt werden.
2. Der Provider ist für den Kunden unter support@ephios.de per E-Mail rund um die Uhr erreichbar. Der Provider strebt an, alle E-Mails bis zum Abend des auf den Eingang der E-Mail folgenden Werktages zu beantworten.
3. Der Provider stellt nach Möglichkeit telefonischen Support unter der auf der Website angegebenen Telefonnummer bereit. Die Erreichbarkeit per Telefon wird nicht garantiert. Der Kunde ist aufgefordert, im Falle eines Nichterreichens per Telefon seine Anfrage per E-Mail zu stellen oder eine Nachricht auf dem Anrufbeantworter zu hinterlassen. Dem Provider bleibt vorbehalten, telefonisch eingehende Anfragen per E-Mail an die vom Kunden hinterlegt E-Mail-Adresse zu beantworten.

## § 3 Dienstleister

1. Erbringer des Services ist die Baumann & Rindt Softwareentwicklung GbR, Potsdam.
2. Zur Erfüllung der Leistungen werden IT-Dienstleistungen anderer Unternehmen gemäß Anlage C in Anspruch genommen.
3. Die Zustellung von mobilen Push-Benachrichtigungen erfolgt nach Aktivierung durch Nutzende über Dienste der Betriebssystem- und Browserhersteller wie Apple Inc. und Google LLC.

## § 4 Qualitätskontrolle

1. Der Provider verwendet branchenübliche Monitoring-Software zur Messung der Verfügbarkeit. Hierbei wird die Erreichbarkeit der für den Betrieb relevanten Systeme regelmäßig getestet und im Falle eines Fehlers automatisch eine Nachricht an die technischen Mitarbeiter des Providers versendet.
2. Die Messung der Erreichbarkeit findet mindestens alle 5 Minuten statt. Kurzfristige Unterbrechungen des Monitorings aufgrund technischer Wartung oder aufgrund von Systemausfällen sind möglich.
3. Die Ergebnisse dieser Messungen können auf Anfrage beim Provider eingesehen werden.

## § 5 Zusätzliche Dienstleistungen und Entgelte

1. Für die Nutzung der Software fällt die vereinbarte monatliche Grundgebühr an. Die Anzahl der Accounts mit Zugriff auf die Software ist auf eine gemäß Preisliste vereinbarte Anzahl Benutzende begrenzt. Eine Gebühr für höhere Benutzendenzahlen wird zwischen Provider und Kunde individuell vereinbart.
2. Abweichende Entgeltvereinbarungen erfordern die Einhaltung der Textform.
3. Für die Erbringung zusätzlicher Dienstleistungen durch den Provider wird ein Stundensatz von 80 € netto vereinbart. Derartige Dienstleistungen werden nur aufgrund schriftlicher Beauftragung durch den Kunden durchgeführt. Auf Wunsch kann ein Kostenvoranschlag angefertigt werden.
4. Datensicherungen oder -exporte werden dem Kunden grundsätzlich auf digitalem Wege (z.B. per E-Mail oder Download) zur Verfügung gestellt. Wünscht der Kunde eine Übertragung auf einem physikalischen Datenträger, so wird der Aufwand berechnet. Die Bearbeitungsgebühr kann bis zu 120 € netto betragen.

---

# Anlage B: Auftragsverarbeitungsvertrag

## § 1 Gegenstand des Auftrags

1. Der Auftragnehmer verarbeitet für den Auftraggeber personenbezogene Daten, indem er die technische Infrastruktur zur Nutzung der Software ephios bereitstellt.
2. Dazu stellt der Auftragnehmer (auch: Provider) dem Auftraggeber (auch: Kunden) auf Grundlage dieser Allgemeinen Geschäftsbedingungen, der darin enthaltenen Service Level Agreements und technischen Spezifikation, sowie ggf. kundenspezifischen Vertragsergänzungen (zusammen im Folgenden: Hauptvertrag) ein Softwareprodukt zur Nutzung über das Internet zur Verfügung. Die Software wird vom Auftragnehmer in einem Rechenzentrum betrieben und dem Auftraggeber zur Nutzung über das Internet zur Verfügung gestellt (auch als „Software as a Service“ bezeichnet).
3. Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO entsprechend der Vereinbarungen aus dem Hauptvertrag mit AGB, SLA und Technischer Spezifikation, auf die hier verwiesen wird.
4. Diese Regelungen zur Auftragsverarbeitung konkretisiert die Verpflichtungen der Parteien zum Umgang mit personenbezogenen Daten, die sich aus dem Hauptvertrag ergeben. Sie finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag im Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen.

## § 2 Dauer des Auftrags

1. Die Dauer des Auftrags richtet sich nach der Laufzeit des Hauptvertrags gemäß § 1 dieser Vereinbarung.
2. Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages 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 diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

## § 3 Konkretisierung des Auftragsinhalts

1. Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).
2. Art und Zweck der vorgesehenen Verarbeitung von Daten ergeben sich primär aus dem Hauptvertrag.
3. Die Verarbeitung der Daten besteht dabei insbesondere in der Erhebung, Erfassung, Speicherung und Auswertung der vom Auftraggeber und dessen Kunden eingegebenen Daten sowie Übermittlung dieser Daten an den Auftraggeber.
4. Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten bzw. Datenkategorien:
    a. Personenstammdaten (z.B. Name, erworbene Qualifikationen)
    b. Kommunikationsdaten (z.B. Telefon, E-Mail)
    c. Planungs- und Steuerungsdaten (z.b. Veranstaltungen, Teilnahmen)
5. Konkret geht es um folgende personenbezogene Daten:
    a. Persönliche Daten von Benutzern des Kunden (z.B. Name, E-Mail, Qualifikationen, Teilnahmen an Veranstaltungen)
    b. Technische Daten, die beim Betrieb einer öffentlichen Website anfallen (z.B. Server-Logs). Hierbei können IP-Adressen enthalten sein, auch wenn diese nur aus konkretem Anlass (z.B. Verdacht auf einen Angriff, Absturz der Software) gespeichert werden. Die Speicherdauer beträgt höchstens 90 Tage.
    c. E-Mails und Metadaten zu Supportfällen bzw. Kontaktaufnahmen des Auftraggebers oder seiner Kunden mit dem Kundendienst des Auftragnehmers.
    d. Authentifizierungsdaten der Benutzer des Auftraggebers, die zur Nutzung der Software berechtigt sind.
    e. Protokolle über die Nutzung der Software durch den Auftraggeber und seiner Benutzer zur Sicherstellung der Nachvollziehbarkeit von Änderungen.
6. Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
    a. Benutzer des Auftraggebers
    b. Vertragspartner des Auftraggebers

## § 4 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

1. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.
2. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel durch entsprechende Konfiguration, Einrichtung und Benutzung der Software. Darüber hinausgehende Weisungen, Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder per E-Mail festzulegen. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
3. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.
4. Der Auftraggeber ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise nach vorheriger Terminvereinbarung und ohne Störung des Betriebsablaufes von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen. Die Prüfung kann durch einen beauftragten Dritten erfolgen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Bei der Prüfung muss mindestens ein Mitarbeiter des Auftragnehmers anwesend sein.
5. Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

## § 5 Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

1. Weisungsberechtigte Personen des Auftraggebers sind alle Benutzer des Auftraggebers, denen der Auftraggeber in der bereitgestellten Software den Status "Administrator" zuweist.
2. Weisungsempfänger beim Auftragnehmer sind alle Mitarbeiter des Auftragnehmers, die im schriftlichen oder elektronischen Kundendienst tätig sind. Ein Datenschutzbeauftragter ist beim Auftragnehmer in Einklang mit den gesetzlichen Vorschriften nicht bestellt.
3. Weisungen sind durch entsprechende Konfiguration der Software oder per E-Mail an support@ephios.de zu erteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

## § 6 Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).
2. Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.
3. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu.
4. Die Daten des Auftraggebers werden mit den Daten anderer Auftraggeber auf gemeinsamen physischen Systemen verarbeitet. Eine Aushändigung oder Vernichtung spezifischer Datenträger ist daher nicht möglich. Möglich ist aber die Löschung bestimmter Daten des Auftraggebers auf den jeweiligen Datenträgern. Der Auftragnehmer stellt durch ein Rechtekonzept sicher, dass jeder Auftraggeber nur auf die jeweils eigenen Daten Zugriff erhält.
5. Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO).
6. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.
7. Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

8. Auskünfte über personenbezogene Daten an Dritte darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen. Eine solche Weisung zur Datenweitergabe an Dritte gilt dann als ausdrücklich erteilt, wenn der Auftraggeber entsprechende Funktionen der Software zur Kommunikation mit externen Dienstleistern oder anderen ephios-Instanzen aktiviert und konfiguriert.
9. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber – grundsätzlich nach Terminvereinbarung und ohne Störung des Betriebsablaufes – berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte, die nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen, zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme (Art. 28 Abs. 3 Satz 2 lit. h DSGVO).
10. Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt, indem er die nötigen Einsichtnahmen ermöglicht.
11. Der Auftraggeber erklärt sich damit einverstanden, dass die Mitarbeiter des Auftragnehmers ihre Beschäftigung auch von Privatwohnungen aus ausüben (Tele- bzw. Heimarbeit) und auch von dort aus zu Zwecken der Fehleranalyse Zugriff auf Datenbestände haben. Daten des Auftraggebers werden nicht über einzelne Vorgänge der Fehleranalyse hinaus in Privatwohnungen gespeichert. Die Maßnahmen nach Art. 32 DSGVO sind auch in diesem Fall sicherzustellen.
12. Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind.
13. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese Verpflichtung besteht auch nach Beendigung des Vertrages fort.
14. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

## § 7 Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

1. Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.
2. Der Auftragnehmer informiert den Auftraggeber hierzu per E-Mail an die vom Auftraggeber in der Software hinterlegte primäre Kontaktadresse.

## § 8 Unterauftragsverhältnisse mit Subunternehmern

1. Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen ohne konkreten Bezug zur Leistung. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.
2. Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Erlaubnis gemäß Art. 28 Abs. 2 DSGVO, dass der Auftragnehmer zur Erfüllung seiner vertraglichen Aufgaben Unterauftragnehmer einsetzen darf.
3. Der Auftragnehmer muss dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt.
4. Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

5. Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern.
6. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
7. Der Auftragnehmer hat die in der Anlage C mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beauftragt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.
8. Der Auftragnehmer informiert den Auftraggeber immer im Voraus über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (Art. 28 Abs. 2 Satz 2 DSGVO). Dabei wird eine Einspruchsfrist von 14 Tagen vereinbart.
9. Im Falle eines Einspruchs kann der Auftragnehmer den Vertrag entsprechend der regulären Kündigungsfristen des Hauptvertrages kündigen, falls die Fortführung der Dienstleistung ohne die beabsichtigte Änderung nicht zumutbar ist. Der Auftragnehmer muss in diesem Fall sicherstellen, dass an den neuen Unterauftragnehmer keine Daten des Auftraggebers übertragen werden.

## § 9 Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

1. Für die konkrete Auftragsverarbeitung wird ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.
2. Die vom Auftragnehmer hierbei konkret getroffenen technischen und organisatorischen Maßnahmen werden in Anlage D beschrieben.
3. Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DSGVO). Das Ergebnis wird dem Auftraggeber auf Anfrage mitgeteilt.
4. Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.
5. Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.
6. Über wesentliche Änderungen muss der Auftragnehmer den Auftraggeber in dokumentierter Form elektronisch mit einer angemessenen Vorlaufzeit informieren.

## § 10 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

1. Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber wie folgt zu löschen bzw vernichten zu lassen: Alle personenbezogenen Daten auf den Systemen des Auftragnehmers werden nach Abschluss der vertraglichen Arbeiten umgehend gelöscht oder so anonymisiert, dass eine Zuordnung zu Personen unmöglich ist, soweit keine rechtlichen Gründe wie beispielsweise Aufbewahrungspflichten nach HGB entgegenstehen. Die Daten können für einen Zeitraum von bis zu drei Monaten noch in Sicherheitskopien enthalten sein, die zur Sicherung der Integrität der Sicherheitskopien nicht bearbeitet werden können. Die Sicherungskopien werden in einem getrennten Rechenzentrum gespeichert und nach spätestens drei Monaten automatisch gelöscht.
2. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe in einem elektronischen Format dokumentiert zu bestätigen.

## § 11 Haftung

1. Auf Art. 82 DSGVO wird verwiesen.
2. Es gilt die im Hauptvertrag vereinbarte Haftungsregelung.

## § 12 Sonstiges

1. Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.
2. Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.
3. Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
4. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

---

# Anlage C: Auflistung der beauftragten Unterauftragnehmer

1. netcup GmbH, Daimlerstr. 25, 76185 Karlsruhe
   Beauftragt mit Server- und Rechenzentrumsdienstleistungen zur Datenverarbeitung und Speicherung
   Rechenzentrumsstandorte: Nürnberg (Deutschland)
2. Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen
   Beauftragt mit Server- und Rechenzentrumsdienstleistungen zur Datenverarbeitung und Speicherung
   Rechenzentrumsstandorte: Nürnberg (Deutschland) und Falkenstein (Deutschland)
3. Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg
   Beauftragt mit E-Mail-Zustellungsleistungen
   Rechenzentrumsstandorte: Schweden
4. Uberspace, Kaiserstr. 15, 55116 Mainz, Deutschland
   Beauftragt mit Server- und Rechenzentrumsdienstleistungen zur Datenverarbeitung und Speicherung
   Rechenzentrumsstandorte: Deutschland

---

# Anlage D: Allgemeine technisch-organisatorische Maßnahmen nach Art. 32 DSGVO

1. Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DSGVO)
   a. Alle Daten werden bei der Übertragung über öffentliche oder private Datennetzwerke immer nach modernen Standards verschlüsselt.
   b. Daten auf den Produktivsystemen selbst werden nicht verschlüsselt, da zur Sicherstellung der ständigen Abrufbarkeit die Schlüssel auf dem gleichen System gespeichert werden müssen und sich hieraus kein realer Sicherheitsvorteil ergäbe.
2. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)
   a. Zutrittskontrolle
      i. Auswahl von Rechenzentren von Subunternehmern, die durch geeignete Schließsysteme, Zutrittskontrollsysteme, Besucherregelung, Alarmanlage, Videoüberwachung und weitere geeignete Maßnahmen angemessen vor unberechtigtem Zutritt geschützt sind
   b. Zugangskontrolle
      i. Zugang zu Systemen nur mit persönlicher Benutzerkennung und Kennwort. Eine Richtlinie für die Vergabe der Passwörter ist definiert.
      ii. Aktivierte und konfigurierte Firewall auf allen eingesetzten Systemen
      iii. Der Wartungszugang auf Produktivsystemen ist nur mittels persönlicher, geheimer Schlüsselmöglich
      iv. Protokollierung aller Logins auf Produktivsystemen
      v. Aktivierter und aktueller Virenschutz auf allen Windows-basierten Systemen
   c. Zugriffskontrolle
      i. Benutzerrollen-/Gruppenkonzept
      ii. Regelmäßige Überprüfung der Benutzerberechtigungen
      iii. Wartungszugänge zu Produktivsystemen werden nur an eine minimale Anzahl technischer Mitarbeiter vergeben
   d. Trennungskontrolle
      i. Firmendaten (Buchhaltung, Personalverwaltung, etc.) von Kundendaten getrennt

        ii. Logische Trennung von Test- und Produktivsystemen
        iii. Physische Trennung von Datensicherungen und Produktivsystemen
3. Integrität (Art 32 Abs. 1 lit. b DS-GVO)
    a. Weitergabekontrolle
        i. Verschlüsselte Übertragung personenbezogener Daten in internen und externen Netzwerken
        ii. Identifizierung / Authentifizierung
    b. Eingabekontrolle
        i. Mitarbeiter des Auftragnehmers dürfen grundsätzlich nur zur Erfüllung einer Weisung des Auftragnehmers oder zur Diagnose eines technischen Fehlers auf diese Daten zugreifen bzw. Daten eingeben, verändern oder löschen.
        ii. Protokollierung bei Eingabe, Änderung und Löschung relevanter Daten
4. Verfügbarkeit, Belastbarkeit, Wiederherstellbarkeit (Art 32 Abs. 1 lit. b, c DS-GVO)
    a. Verfügbarkeitskontrolle
        i. Alle Server stehen in Rechenzentren in Deutschland
        ii. Rechenzentren der Unterauftragnehmer weisen geeignete Schutzmaßnahmen auf (insbesondere redundante Stromversorgung, Überspannungsschutz, Schutz gegen Feuer und Wassereintritt)
        iii. Dauerhafte automatische Überwachung der korrekten Funktionalität
        iv. Automatische Datensicherungen gemäß SLA in Anlage zum Hauptvertrag
        v. Firewalls im Einsatz
5. Regelmäßige Überprüfung, Bewertung und Evaluierung (Art 32 Abs. 1 lit. d DSGVO)
    a. Auftragskontrolle
        i. Zwischen Auftragnehmer und evtl. Unterauftragnehmer wird bei Bedarf ein Auftragsverarbeitungsvertrag geschlossen.

---