# Vertrag zur Auftragsverarbeitung

**gem. Art. 28 Abs. 3 DSGVO**

zwischen

Kundennummer (5-stellig): _____
Firma/Organisation: _____
Vor- und Nachname: _____
Straße und Hausnr.: _____
PLZ und Ort: _____
Land: _____
Telefon: _____
E-Mail: _____

- nachfolgend Auftraggeber oder Verantwortlicher genannt -

und

Weber eBusiness Services GmbH
Bahnhofstraße 16
72336 Balingen
Deutschland
Telefon: +49 7433 26080-0
E-Mail: info@weber-ebusiness.de

- nachfolgend Auftragnehmer oder Auftragsverarbeiter genannt -

**PRÄAMBEL**

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Vertrag hinsichtlich der Erbringung verschiedener Dienstleistungen durch den Auftragnehmer (Hauptvertrag).

Dieser Vertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus dem Hauptvertrag ergeben. Im Übrigen wird der Hauptvertrag durch diesen Vertrag nicht berührt. Sofern in diesem Vertrag lediglich von Daten die Rede ist, handelt es sich ausschließlich um personenbezogene Daten im Sinne der DSGVO.

**I. Gegenstand und Dauer**

1. Der Auftragnehmer erhebt/verarbeitet/nutzt personenbezogene Daten im Auftrag des Auftraggebers.

2. Gegenstand des Auftrags:
   Gegenstand des Auftrags ist die Verarbeitung von Daten durch Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung,

Einschränkung, Löschen oder Vernichtung von Daten ausschließlich im Zusammenhang mit den im Hauptvertrag aufgeführten Dienstleistungen, konkret im Zusammenhang mit (bitte entsprechendes auswählen):

- ☐ Erbringung von Hostingdienstleistungen
- ☐ Vermietung von virtuellen (Cloud)-Servern
- ☐ Vermietung von dedizierten physikalischen Servern
- ☐ Registrierung und Verwaltung von Domainnamen
- ☐ Bereitstellung von statischen IP-Adressen
- ☐ Bereitstellung von SSL-Zertifikaten
- ☐ Softwareinstallation oder -updates auf Kundensystemen
- ☐ Entwicklung, Anpassung und Erweiterung von Software, webbasierten Angeboten oder Online-Shops
- ☐ Erbringung von Online-Marketing Dienstleistungen.

Eine Verarbeitung zu anderen Zwecken findet nicht statt.

Hierbei ist zunächst klarzustellen, dass der Hauptvertrag originär nicht die Verarbeitung personenbezogener Daten durch den Auftragnehmer zum Gegenstand hat. Dass der Auftragnehmer im Rahmen von Reparatur- und Wartungsarbeiten oder bestimmten Leistungserbringungen (z. B. Entwicklung, Anpassung und Erweiterung von Software, webbasierten Angeboten oder Online-Shops, Einspielen von Updates, Supportdienstleistungen etc.) mit personenbezogenen Daten in Kontakt kommt, kann jedoch nicht ausgeschlossen werden.

Die vertragsgegenständlichen Dienstleistungen werden seitens des Auftragnehmers selbst ausschließlich im Gebiet der Bundesrepublik Deutschland, in Mitgliedsstaaten der EU oder in einem Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum erbracht. Eine Verlagerung der Dienstleistungen oder Teilarbeiten in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen des Art. 44 ff. DSGVO erfüllt sind und dies zur Erbringung der Dienstleistungen zwingend erforderlich ist (beispielsweise bei bestimmten Toplevel-Domains, siehe auch unten).

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

3. Dauer des Auftrags:
   Der Vertrag beginnt mit der Unterschrift beider Parteien (nicht jedoch vor dem 25. Mai 2018) und endet mit der Wirksamkeit der Kündigung des Hauptvertrages.

4. Umfang, Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung:
   Umfang, Art und Zweck der Zugriffsmöglichkeit des Auftragnehmers auf Daten des Auftraggebers ergeben sich i. d. R. aus dem Hauptvertrag. Auch wenn der Hauptvertrag keine Datenverarbeitung durch den Auftragnehmer zum Gegenstand hat, kann zum Zwecke der Vertragserfüllung ein Zugriff des Auftragnehmers auf die unter I.4.1. und I.4.2. aufgeführten Daten nicht ausgeschlossen werden (z. B. im Rahmen von Wartungen, Reparaturarbeiten, Supportdienstleistungen etc.).

4.1. Art der personenbezogenen Daten:
Die von der Auftragstätigkeit möglicherweise betroffenen Datenkategorien, abhängig von den jeweiligen zu erbringenden Leistungen, lauten wie folgt (bitte entsprechendes auswählen):

☐ Personenstammdaten (z. B. Nachname, Vorname, Geburtsdatum, Adresse)
☐ Kommunikationsdaten (z. B. Telefonnummern, E-Mail-Adressen)
☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse) und sonstige Vertragsdaten
☐ Kundenhistorie
☐ Vertragsabrechnungs- und Zahlungsdaten
☐ Identitätsnachweisdaten
☐ Planungs- und Steuerungsdaten
☐ Auskunftsangaben (von Dritten, z. B. Auskunfteien, oder aus öffentl. Verzeichnissen)
☐ Objektstammdaten
☐ allgemeiner Schriftwechsel
☐ E-Mails
☐ statistische Daten
☐ Rechnungen
☐ Protokolle
☐ Datenbanken
☐ Konfigurationsdaten
☐ Verbindungsdaten und IP-Adressen
☐ Gespeicherte Benutzerkennungen
☐ _____
☐ _____
☐ _____

Es wird klargestellt, dass diese Angaben vom Auftraggeber gemacht wurden und der Auftragnehmer weder Kenntnis noch Einfluss darauf hat, welche Daten auf den Systemen des Auftraggebers tatsächlich gespeichert werden. Der Auftraggeber verpflichtet sich, später hinzukommende Datenkategorien mit dem Auftragnehmer vorab abzustimmen (s. I.2., letzter Absatz).

4.2. Kreis der Betroffenen:
Der Kreis der durch den Umgang mit den Daten im Rahmen dieses Auftrags Betroffenen umfasst (bitte entsprechendes auswählen):

☐ Beschäftigte
☐ Kunden
☐ Abonnenten
☐ Interessenten
☐ Geschäftspartner
☐ Lieferanten

☐ Besucher
☐ Dienstleister
☐ Gläubiger
☐ _____
☐ _____
☐ _____

Es wird klargestellt, dass diese Angaben vom Auftraggeber gemacht wurden und der Auftragnehmer weder Kenntnis noch Einfluss darauf hat, wessen Daten auf den Systemen des Auftraggebers tatsächlich gespeichert werden. Der Auftraggeber verpflichtet sich, später hinzukommende Betroffenenkategorien mit dem Auftragnehmer vorab abzustimmen (s. I.2., letzter Absatz).

**II. Rechte und Pflichten des Auftraggebers**

1. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der Betroffenen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich; er bleibt Verantwortlicher i. S. d. Art. 4 Ziff. 7 DSGVO. Insbesondere obliegt es dem Auftraggeber, sich gegebenenfalls erforderliche Einwilligungen von den datenschutzrechtlich Betroffenen einzuholen oder behördliche Meldepflichten einzuhalten. Gleiches gilt für die Gestaltung eines rechtssicheren Rahmens für ggf. beabsichtigte Übermittlungen von personenbezogenen Daten in Drittstaaten, bei welchen ein angemessenes Datenschutzniveau nicht gewährleistet ist. Gleichwohl ist der Auftragnehmer verpflichtet, alle Anfragen Betroffener, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

2. Der Auftraggeber garantiert die Rechtmäßigkeit der Verarbeitung i. S. d. Art. 6 DSGVO, insbesondere soweit er Daten Dritter oder von Mitarbeitern unter Zuhilfenahme der Systeme des Auftragnehmers verarbeitet. Bezüglich der Registrierung und Verwaltung von Domainnamen, der Bereitstellung von SSL-Zertifikaten sowie von statischen IP-Adressen gilt das Folgende: Der Auftraggeber wird hiermit darüber in Kenntnis gesetzt, dass zur Erfüllung des Vertrages die von ihm für die Registrierung von Domainnamen und Bestellung von SSL-Zertifikaten hinterlegten Daten an die jeweiligen Lieferanten (Registrar, Registry bzw. Certificate Authority) übermittelt und von diesen ggf. veröffentlicht werden. Teilweise sind die übermittelten Daten über Datenbanken (sog. WHOIS-Datenbanken), bzw. bei SSL-Zertifikaten über bestimmte Programme und Browserfunktionen, öffentlich einsehbar; teilweise werden Daten auch an das RIPE NCC in den Niederlanden weitergeleitet, das ebenfalls eine öffentliche Datenbank im Internet unterhält. Vom Auftragnehmer kann keinerlei Gewähr für ein angemessenes Datenschutzniveau bei diesen Stellen, die sich zum Teil in Drittstaaten befinden, übernommen werden. Der Auftraggeber verpflichtet sich, die Betroffenen im Rahmen der Informationspflichten des Art. 13 DSGVO u. a. auch auf diese vertragsnotwendigen Übermittlungen in ausreichend transparenter Weise hinzuweisen. Die vorgenannte Hinweispflicht entfällt nur dann, wenn der Auftraggeber ausschließlich Unternehmensdaten verwendet bzw. keinerlei Datensätze, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Auch die Zuteilung von statischen IP-Adressen kann nach den Bestimmungen des RIPE nur erfolgen, wenn zuvor die Daten des jeweiligen Bestellers an das RIPE übermittelt wurden. Schließlich werden bei einer Registrierung von Domains unterhalb einer generischen Toplevel-Domain (sog. gTLDs, wie z. B. .com, .net, .org, .biz etc.) u. a. die Inhaberdaten an die Internet Corporation for Assigned Names and Numbers (ICANN), Los Angeles, USA, und ggf. an Escrow Unternehmen weitergeleitet. Die genannten Datenübermittlungen sind für Domainregistrierungen bzw. Bestellungen von SSL-Zertifikaten, mithin für die Vertragserfüllung, zwingend erforderlich. Soweit er für Dritte Domains registriert oder SSL-Zertifikate bestellt, garantiert der Auftraggeber ausdrücklich die Rechtmäßigkeit der Verarbeitung i. S. d. Art. 6 DSGVO. Gleiches gilt, sofern er bei den Domainkontakten personenbezogene Daten von Mitarbeitern einträgt.

3. Der Auftraggeber erteilt alle Aufträge oder Teilaufträge schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind nochmals unverzüglich schriftlich oder in einem dokumentierten elektronischen Format durch den Auftraggeber zu bestätigen.

4. Der Auftraggeber hat das Recht, dem Auftragnehmer im Hinblick auf die Verarbeitung von ihm bereitgestellter persönlicher Daten Weisungen in Schriftform zu erteilen.

5. Der Auftraggeber ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen, sowie den Verpflichtungen aus diesem Vertrag zu überzeugen. Der Auftraggeber kann diese Kontrolle auch durch einen Dritten durchführen lassen. Der Auftraggeber verpflichtet sich, die bei dem Auftragnehmer im Rahmen der Ermöglichung von Kontrollen entstehenden Aufwände zu vergüten (siehe auch VI.).

6. Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

7. 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.

**III. Pflichten des Auftragnehmers**

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen des Hauptvertrags, der getroffenen Vereinbarungen, der rechtlichen Grundlagen und nach Weisungen des Auftraggebers im Einklang mit der DSGVO, außer er ist zur Verarbeitung verpflichtet durch das Recht der Europäischen Union oder des Mitgliedsstaates, dem der Auftragsverarbeiter unterliegt (z. B. Ermittlungen von Strafverfolgungs- und Staatsschutzbehörden). Ist dies der Fall, hat der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mitzuteilen, es sei denn eine solche Mitteilung ist wegen wichtigem öffentlichen Interesse durch das betreffende Recht verboten (Art. 28 Abs. 3 S. 2 lit. a DSGVO).

   Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung oder Erfüllung vertraglicher oder gesetzlicher Pflichten erforderlich sind.

2. Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen und zu sperren bzw. deren Verarbeitung einzuschränken, wenn der Auftraggeber dies in der getroffenen Vereinbarung oder einer Weisung verlangt und keine berechtigten Interessen des Auftragnehmers entgegenstehen. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten. Der Auftragnehmer ist berechtigt, entsprechende Änderungen selbst vorzunehmen, wenn der Auftraggeber nicht auf entsprechende Anfragen der Betroffenen reagiert.

3. Der Auftragnehmer verwendet die zur Datenverarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die verarbeiteten Daten von sonstigen Datenbeständen getrennt werden. Die Trennung der Datensätze des Auftraggebers von denen anderer Auftraggeber erfolgt bei dedizierten physikalischen Servern durch Speicherung in physisch getrennten Datenbanken bzw. Verzeichnissen. Bei virtuellen (Cloud-)Server-Umgebungen erfolgt eine logisch getrennte Speicherung.

4. Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

5. Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber – nach Terminvereinbarung – berechtigt ist, die Einhaltung dieser Vereinbarung im erforderlichen Umfang nach Art. 28 DSGVO selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren. Der Auftragnehmer verpflichtet sich, dem Auftraggeber die erforderlichen Auskünfte zu erteilen, und die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen. Der Auftraggeber verpflichtet sich, die bei dem Auftragnehmer im Rahmen der Ermöglichung von Kontrollen entstehenden Aufwände zu vergüten (siehe auch VI.).

6. Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz gelangten Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen, sofern dem nicht ein gesetzlicher oder tatsächlicher Grund entgegensteht.

7. Sofern gem. DSGVO beim Auftragnehmer ein Datenschutzbeauftragter notwendig ist, wird dieser vom Auftragnehmer bestellt und kann seine Tätigkeit gemäß Art. 37, 38 DSGVO ausüben. Er ist dann per E-Mail zu erreichen unter: datenschutz@weber-ebusiness.de. Dessen weitere Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme auf Anforderung mitgeteilt. Ein nach dieser Mitteilung eintretender Wechsel des Datenschutzbeauftragten ist dem Auftraggeber wiederum unverzüglich mitzuteilen.

8. Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind und er seine entsprechenden Pflichten einhält.

9. Der Auftragnehmer verpflichtet sich, die Vertraulichkeit bei der Verarbeitung der personenbezogenen Daten des Auftraggebers zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

10. 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 sie sowohl für die Zeit ihrer Tätigkeit, als auch nach Beendigung des Beschäftigungsverhältnisses zur Verschwiegenheit verpflichtet. Der Auftragnehmer überwacht die Einhaltung der hier angegebenen datenschutzrechtlichen Vorschriften in seinem Betrieb.

11. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder schriftlicher Zustimmung durch den Auftraggeber erteilen, oder soweit diese Auskunft aufgrund gesetzlicher Verpflichtungen erfolgt.

**IV. Subunternehmen**

1. Der Auftragnehmer stellt dem Auftraggeber im Service-Center unter https://service.weber-ebusiness.de eine Liste der aktuell für den Auftragnehmer tätigen Subunternehmen mit Namen und Auftragsinhalt zur Verfügung, die unter bestimmten Umständen möglicherweise Zugriff auf personenbezogene Daten erhalten könnten. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden. Der Auftragnehmer informiert den Auftraggeber im Service-Center stets über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Der Einspruch hat schriftlich zu erfolgen. Erhebt der Auftraggeber Einspruch gegen die Hinzuziehung eines neuen oder die Ersetzung eines bisherigen Subunternehmers, dessen Leistung jedoch für ein bestimmtes Produkt erforderlich ist, ist der Auftragnehmer berechtigt, das jeweilige Produkt dem Auftraggeber nicht mehr anzubieten. Bezieht der Auftraggeber bereits das betreffende Produkt, steht dem Auftragnehmer im Falle des Einspruchs diesbezüglich ein Sonderkündigungsrecht zu, das vom Auftragnehmer innerhalb von vier Wochen ab Zugang des Einspruchs ausgeübt werden kann.

2. Die Beauftragung von Subunternehmern zur Verarbeitung von Daten wie Registrierungsstellen, Registraren und Data Escrow-Anbietern ist aufgrund der Besonderheiten des Vorganges der Verwaltung und Registrierung von Domainnamen, statischen IP-Adressen und SSL-Zertifikaten zugelassen und bedarf keiner weiteren Zustimmung, soweit die Verwendung dieser Subunternehmer für eine Auftragserfüllung im Rahmen das Hauptvertrages erforderlich ist. Die nach Art. 28 Abs. 2 und Abs. 9 DSGVO erforderliche Genehmigung wird hiermit erteilt.

3. Der Auftragnehmer trägt dafür Sorge, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig ausgewählt hat.

4. Subunternehmen in Drittstaaten dürfen nur beauftragt werden, wenn die besonderen Voraussetzungen der Art. 44 ff DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln), oder sofern deren Beauftragung für die

Erbringung der Dienstleistung durch den Auftragnehmer zwingend erforderlich ist (z. B. bei bestimmten Toplevel-Domains).

5. Der Auftragnehmer hat dafür Sorge zu tragen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer – soweit möglich – auch gegenüber Subunternehmern gelten. Er wird die Einhaltung der Pflichten des/der Subunternehmer(s) regelmäßig überprüfen.

6. 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.

**V. Technische und organisatorische Maßnahmen**

1. Der Auftragnehmer gewährleistet ein für die konkrete Auftragsverarbeitung dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau. Dazu werden mindestens die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität 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. Das vom Auftragnehmer genutzte Datenschutzkonzept hat seine technischen und organisatorischen Maßnahmen unter Berücksichtigung der Schutzziele nach dem Stand der Technik und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer umgesetzt.

3. Der Auftragnehmer beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung. Er gewährleistet die vertraglich vereinbarten und gesetzlich vorgeschriebenen Datensicherheitsmaßnahmen.

4. Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftragnehmer setzt Verfahren zur regelmäßigen Überprüfung, Evaluierung und Bewertung der Wirksamkeit der getroffenen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung ein. Wesentliche Änderungen wird der Auftragnehmer dem Auftraggeber in dokumentierter Form mitteilen.

5. 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 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen.

## VI. Vergütung

1. Erteilt der Auftraggeber Einzelweisungen (s. II.3.), die über den vereinbarten Leistungsumfang des Hauptvertrags hinausgehen, sind die dadurch begründeten Kosten grundsätzlich vom Auftraggeber zu tragen.

2. Der Auftragnehmer behält sich vor, für die Erfüllung von Auskunftspflichten gegenüber Betroffenen, sowie von sonstigen Pflichten, die nach der Datenschutzgrundverordnung oder dem Bundesdatenschutzgesetz dem Auftraggeber obliegen, und die nicht vom Hauptvertrag umfasst sind, vom Auftraggeber eine angemessene Vergütung zu verlangen. Gleiches gilt für besondere Löschungs- und Vernichtungsaufträge des Auftraggebers.

3. Auch für die Ermöglichung von Kontrollen durch den Auftraggeber i. S. von III.5., ob schriftlich oder durch Vor-Ort-Termine, behält sich der Auftragnehmer die Geltendmachung von Vergütungsansprüchen vor.

4. Im Übrigen wird für die Einhaltung der in diesem Vertrag geregelten Verpflichtungen keine gesonderte Vergütung fällig. Insbesondere wird klargestellt, dass für Betroffene aus der Geltendmachung ihrer Rechte, sowohl gegenüber dem Auftraggeber als auch gegenüber dem Auftragnehmer, keinerlei Kosten entstehen.

## VII. Haftung / Nichterfüllung

1. Für den Ersatz von Schäden, die ein Betroffener wegen einer Vorschrift für den Datenschutz unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, ist der Auftraggeber gegenüber dem Betroffenen verantwortlich. Der Rückgriff des Auftragsgebers für derartige Schäden Dritter beim Auftragnehmer ist nur zulässig, wenn dieser grob fahrlässig oder vorsätzlich gegen diesen Vertrag verstoßen hat.

   Soweit es sich beim Auftraggeber um ein Unternehmen handelt, das die Leistungen des Auftragnehmers nutzt, um sie Dritten anzubieten bzw. weiterzuverkaufen, stellt der Auftraggeber den Auftragnehmer von sämtlichen Schadensersatz-, Aufwendungsersatz- und sonstigen Haftungsansprüchen Dritter sowie von Rechtsanwaltskosten frei, die durch die Verletzung der in diesem Vertrag vereinbarten oder unmittelbar gem. DSGVO geltenden Pflichten durch den Auftraggeber im Zusammenhang mit der Nutzung/Weiterveräußerung der Produkte/Leistungen des Auftragnehmers verursacht werden. Art. 82 DSGVO sowie sonstige zwingende Vorschriften bleiben im Übrigen unberührt.

2. Kann der Auftragnehmer die vereinbarte Leistung wegen höherer Gewalt, Krieg, Aufruhr, Streik, Aussperrung oder Stromausfall nicht oder nicht rechtzeitig erfüllen, so ist er von der Leistung frei. Die Beweislast hierfür obliegt dem Auftragnehmer. Der Auftraggeber hat in diesem Falle keinen Anspruch auf Schadenersatz. Er hat jedoch das Recht, ein anderes Dienstleistungsunternehmen mit der Auftragsausführung zu beauftragen.

3. Im Übrigen sind die Haftungsregelungen zu den einzelnen Leistungen des Auftragnehmers im Hauptvertrag vereinbart.

**VIII. Sonderkündigungsrecht**

1. Bei schwerwiegenden Verstößen gegen die Abmachungen dieses Vertrages, insbesondere gegen die Einhaltung anwendbarer datenschutzrechtlicher Vorschriften, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt. Weitergehende Sanktionen, insbesondere Vertragsstrafen, sind ausgeschlossen.

2. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in diesem Vertrag bestimmten Pflichten in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

3. Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung, wie in diesem Abschnitt beschrieben, berechtigt.

**IX. Sonstiges**

1. Frühere Vereinbarungen bzw. Verträge zur Auftragsdatenverarbeitung oder Auftragsverarbeitung werden mit Abschluss dieses Vertrages durch ihn ersetzt.

2. Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

3. Mündliche Nebenabreden bestehen nicht. Änderungen oder Ergänzungen bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für eine Abänderung dieses Formerfordernisses.

4. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definitionen in der EUDatenschutz-Grundverordnung zu verstehen.

5. Gerichtsstand für sämtliche sich aus diesem Auftragsverarbeitungsvertrag ergebende Streitigkeiten ist, sofern der Kunde Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtlichen Sondervermögens oder im Inland ohne Gerichtsstand ist, Balingen.

**X. Wirksamkeit des Vertrags**

1. Sollten einzelne Teile dieses Vertrags unwirksam oder undurchführbar sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht. An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirksamkeit der wirtschaftlichen Zielsetzung am nächsten kommen, die die Parteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben.

2. Für einen wirksamen Vertragsschluss und zur Dokumentation des Vertragsschlusses ist dieser mit Ort, Datum, Unterschrift, Name und Position versehene Vertrag am Tage der Unterzeichnung seitens des Auftraggebers an datenschutz@weber-ebusiness.de zu senden. Zudem sind die Seiten 1-4 auszufüllen. Der Eingang des Vertrags zur Auftragsvereinbarung wird dann seitens Weber eBusiness Services per E-Mail bestätigt.

| _____ | _____ | _____ |
|---|---|---|
| Ort, Datum | (Unterschrift Auftraggeber) | (Name und Position des Unterzeichnenden in Blockbuchstaben) |

***Dieses Dokument wurde von Weber eBusiness Services GmbH elektronisch erstellt und ist somit ohne Unterschrift der Weber eBusiness Services GmbH gültig.***

# Anhang 1 zum Vertrag zur Auftragsverarbeitung

**Technische und organisatorische Sicherheitsmaßnahmen gem. Art. 32 DSGVO**

Für die beauftragte Erhebung und/oder Verarbeitung von personenbezogenen Daten werden folgende Maßnahmen vereinbart:

**I. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)**

1. Zutrittskontrolle: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z. B.: Magnet- oder Chipkarten, Schlüsselregelung, Alarmanlage, Videoüberwachung des Rechenzentrums bei Bewegungserkennung

2. Zugangskontrolle: Keine unbefugte Systembenutzung, z. B.: Authentifizierung per Benutzername und/oder Kennwort, Bildschirmsperre mit Passwortaktivierung, Protokollierung des Zugangs, manuelle und teils automatische Sperrmechanismen, Ausweisleser an zentralen Zugangstüren

3. Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z. B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte für IT-Systeme, Regelungen zur Löschung bzw. Vernichtung von Datenträgern

4. Trennungskontrolle: Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z. B. getrennte Ordnerstrukturen, Mandantenfähigkeit, Sandboxing

5. Pseudonymisierung: Es werden Maßnahmen der Pseudonymisierung personenbezogener Daten durchgeführt, welche ein aktuelles Schutzniveau gewährleisten

**II. Integrität (Art. 32 Abs. 1 lit. b DSGVO)**

1. Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z. B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur

2. Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z. B.: Protokollierung

**III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)**

1. Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z. B.: Datensicherungskonzept und Umsetzung, Laufwerksspiegelung (RAID o. ä.), unterbrechungsfreie Stromversorgung (USV), Klimatisierung, teilweise Redundanz der Stromversorgungen und Kommunikationsverbindungen, Firewall

2. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO): Datensicherungskonzept und Umsetzung

**IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DSGVO)**

1. Datenschutz-Management

2. Incident-Response-Management

3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

4. Auftragskontrolle: Es findet keine Auftragsverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers statt