# Ergänzende AGBs zur Auftragsdatenverarbeitung

von easyinttel.de nach Art. 28 Abs. 3 DSGVO mit dem Stand vom 01.03.2023.

Die nachstehenden ‚Ergänzende AGBs zur Auftragsdatenverarbeitung' gelten gegenüber den Kunden (nachfolgend auch „Auftraggeber") von easyinttel.de, Patrick Badent, Goethestraße 2, 88281 Schlier (nachfolgend „easyinttel.de" bzw. auch „Auftragnehmer") in allen Fällen.

Aufgrund des Umstandes, dass die easyinttel.de nach ihrem Geschäftsmodell für fast jeden Kunden auch Daten im Auftrag verarbeitet, schließen wir mit jedem Kunden einen Auftragsverarbeitungsvertrag. Daher beziehen wir die ‚Ergänzende AGBs zur Auftragsdatenverarbeitung' in jeden Hauptvertrag mit ein.

Um diesen Vorgang zu erleichtern, haben wir die nachfolgenden ‚Ergänzende AGBs zur Auftragsdatenverarbeitung' so formuliert, dass diese wie unsere AGBs in den Hauptvertrag miteinbezogen werden können und eine separate Vereinbarung nicht notwendig ist.

## 1 Präambel

easyinttel.de bietet Internet im Festnetz, professionelle Telefonie- und Cloud-Lösungen mit allem was dazu gehört: Strategie, Planung, Umsetzung und Support sowie dauerhaft preiswerte Tarife mit fairen Verträgen.

Der Auftragnehmer erbringt gegenüber dem Auftraggeber im Rahmen eines gesonderten, auf Grundlage des Angebots des Auftragnehmers schriftlich oder in elektronischer Form geschlossenen Vertrages sowie in diesen einbezogener Allgemeiner Geschäftsbedingungen (im Folgenden insgesamt als „Hauptvertrag" bezeichnet) verschiedene Dienstleistungen (nachfolgend als „Leistungen" bezeichnet).

Unser Auftragsverarbeitungsvertrag orientiert sich an einer entsprechenden Vorlage der Aufsichtsbehörde Baden-Württembergs und entspricht somit den "offiziellen" Vorgaben der für easyinttel.de zuständigen Aufsichtsbehörde.

## 2 Gegenstand und Dauer

Der Auftragnehmer verarbeitet im Rahmen der Erbringung der von ihm aufgrund des Hauptvertrages geschuldeten Leistungen personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO.

Gegenstand und Dauer der Verarbeitung der Daten ergeben sich aus dem Hauptvertrag, soweit sich aus den Bestimmungen dieses Vertrages nicht darüberhinausgehende Verpflichtungen ergeben.

Dieser Vertrag regelt die Verarbeitung der personenbezogenen Daten, die der Auftragnehmer im Rahmen der Erfüllung des Hauptvertrages für den Auftraggeber verarbeitet („Daten").

Die Laufzeit dieses Vertrags entspricht der Laufzeit des Hauptvertrages.

# 3 Konkretisierung des Auftragsinhalts

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich aus dem Hauptvertrag.

Gegenstand der Verarbeitung personenbezogener Daten sind
- Personenstammdaten,
- Kommunikationsdaten (z.B. Telefon, E-Mail),
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse),
- die vom Kunden im System gespeicherten Daten sowie
- automatisch generierte Abrechnungs-, Verbindungs- und sonstige Daten.

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen Mitarbeiter, weiteren Nutzer des Kunden und alle Personen zu denen der Kunde Daten im System speichert oder ein speichern erforderlich ist.

Die vertraglich vereinbarten Leistungen werden ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Leistungen 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).

# 4 Rechte und Pflichten des Auftraggebers

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. Der Auftragnehmer wird solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterleiten.

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

Die Weisungen des Auftraggebers werden anfänglich durch diese Vereinbarung sowie den Hauptvertrag festgelegt. Danach kann der Auftraggeber einzelne Weisungen schriftlich oder in einem dokumentierten elektronischen Format ändern, ergänzen oder ersetzen. In Eilfällen können mündliche Weisungen erteilt werden. Diese sind vom Auftraggeber unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen. Geht der Inhalt von Weisungen des Auftraggebers über dasjenige hinaus, was der Auftragnehmer dem Auftraggeber nach dem Hauptvertrag schuldet, hat der Auftraggeber die entsprechenden Leistungen dem Auftragnehmer gesondert zu vergüten. Ist eine Weisung nur mit unverhältnismäßig hohem Aufwand umsetzbar, steht dem Auftragnehmer ein Recht zur außerordentlichen Kündigung des Hauptvertrages und dieses Vertrages zu.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 6 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

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

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 Pflichten des Auftragnehmers

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 Auftragnehmer unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber 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).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten 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 für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen zumindest logisch getrennt gespeichert werden. Der Auftragnehmer hat die Einhaltung seiner Pflichten aus diesem Vertrag mindestens einmal in jedem Kalenderjahr zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

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 den Auftraggeber im Rahmen seiner Möglichkeiten zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO). Für hierfür entstehenden Mehraufwand steht dem Auftragnehmer eine zusätzliche Vergütung zu.

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.

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. Die vorstehenden Löschungspflichten gelten nicht für Datenkopien, die in regelmäßig erstellten Sicherungskopien von umfassenden Datenbeständen des Auftragnehmers enthalten sind, deren isolierte Löschung für den Auftragnehmer einen erheblichen Aufwand bedeuten würde und die im Rahmen des vom Auftragnehmer angewandten Sicherungs-Zyklus spätestens nach einem Jahr automatisch gelöscht oder überschrieben werden. Die Wiederherstellung und jede sonstige Nutzung solcher Kopien bis zu ihrer automatischen

Löschung bzw. Überschreibung ist nach Vertragsbeendigung unzulässig. Der Auftraggeber kann vom Auftragnehmer auch die sofortige Löschung solcher Sicherungskopien verlangen, wenn der Auftraggeber dem Auftragnehmer die hierdurch verursachten Kosten erstattet; dies umfasst auch eine Aufwandsentschädigung für die Arbeitszeit des vom Auftragnehmer beanspruchten Personals.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen, soweit der Auftraggeber nicht gesetzlich zur Auftragserteilung verpflichtet ist.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber – außer aus dringlichen, vom Auftraggeber zu dokumentierenden Gründen – nach Terminvereinbarung zu den üblichen Geschäftszeiten des Auftragnehmers ohne Störung des Betriebsablaufs und nicht häufiger als alle 12 Monate berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der zugehörigen vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). Sollte der durch den Auftraggeber beauftragte Dritte in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Für hierfür entstehenden Mehraufwand steht dem Auftragnehmer eine zusätzliche Vergütung zu.

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

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.

## 6 Mitteilungspflichten des Auftragnehmers bei Störungen bei Verletzungen des Schutzes personenbezogener Daten

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).

# 7 Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

Als Unterauftragsverhältnis im Sinne dieses Vertrages sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Leistungen aus dem Hauptvertrag beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post- und Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software der Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der personenbezogenen Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessen und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer allgemein gestattet, Art. 28 Abs. 2 DSGVO. Der Auftragnehmer informiert den Auftraggeber immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Der Auftragnehmer muss dafür Sorge tragen, dass er Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt.

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).

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. Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO). Sofern dem Vertrag mit einem Subunternehmer dessen eigene Vertragsbedingungen zugrunde liegen, müssen diese Vertragsbedingungen entweder vom Auftragnehmer genehmigt oder mindestens das Schutzniveau des vorliegenden Vertrages erreichen. Der Auftraggeber hat das Recht, auf Verlangen Einsicht in die relevanten Vertragsbedingungen zu nehmen.

Die Weiterleitung von Daten an einen Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Die zurzeit für den Auftragnehmer mit der Verarbeitung von personenbezogenen Daten beschäftigten Subunternehmer ergeben sich aus der Tabelle im Anhang 1.

Grundlage der Beauftragung dieser Subunternehmer sind ihre jeweiligen Standardbedingungen (einschließlich ihrer Standard-Maßnahmen zum technischen und organisatorischen Schutz der jeweils verarbeiteten Daten), die auf den o.g. Websites veröffentlicht sind. Mit der Beauftragung dieser Subunternehmer sowie deren jeweiligen Standardbedingungen erklärt sich der Auftraggeber einverstanden.

# 8 Technische und organisatorische Maßnahmen (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

Es wird für die konkrete Auftragsverarbeitung 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.

Das als Anhang beigefügte Datenschutzkonzept des Auftragnehmers stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

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).

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

# 9 Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags (Art. 28 Abs. 3 Satz 2 lit. g DSGVO)

Nach Vertragsbeendigung hat der Auftragnehmer sämtliche in Besitz des Auftragnehmers sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, zu löschen. Bis zur Vertragsbeendigung kann der Auftraggeber die Daten über die auf Auftragnehmer bereitgestellten Standard-Schnittstellen selbst über das Internet abrufen und bei sich speichern. Der Auftraggeber kann vom Auftragnehmer auch die Bereitstellung der Daten in anderer Form verlangen, wenn der Auftraggeber dem Auftragnehmer die hierdurch verursachten Kosten erstattet; dies umfasst auch eine Aufwandsentschädigung für die Arbeitszeit des vom Auftragnehmer beanspruchten Personals.

# 10 Schlussbestimmung

Nebenabreden, Änderungen und Ergänzungen eines Vertragsverhältnisses bedürfen für ihre Wirksamkeit der Textform. Abweichende Allgemeine Geschäftsbedingungen des Kunden, denen easyinttel.de nicht ausdrücklich schriftlich zugestimmt hat, gelten nicht.

Auf diesen Auftragsverarbeitungsvertrag und alle hierunter abgeschlossenen Verträge findet das Recht der Bundesrepublik Deutschland zur Geltung, wie es zwischen inländischen Personen unter Ausschluss des UN-Kaufrechts gilt, sofern nicht zwingendes Recht die Anwendbarkeit einer anderen Rechtsordnung vorschreibt.

Sollte eine Bestimmung dieses Vertrages unwirksam oder undurchführbar sein oder werden, so wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Für den Fall einer unwirksamen Bestimmung treffen die Partien stattdessen eine Regelung, die der unwirksamen Bestimmung in rechtlicher, wirtschaftlicher und tatsächlicher Hinsicht möglichst nahekommt. Dies gilt in gleicher Weise, sofern sich in diesen AGB eine Regelungslücke herausstellt.

Sollten die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Der Gerichtsstand ist der Hauptsitz von easyinttel.de, soweit der Kunde Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist.

# Anhang 1 – Subunternehmer des Auftragnehmers

Als Unterauftragsverhältnisse im Sinne dieser AGB sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer in Anspruch nimmt, z.B. Telekommunikationsleistungen, Post-/Transportdienstleistungen, Reinigungsleistungen oder Bewachungsdienstleistungen. Wartungs- und Prüfleistungen stellen dann ein Unterauftragsverhältnis dar, wenn sie für IT-Systeme erbracht werden, die im Zusammenhang mit einer Leistung des Auftragnehmers erbracht werden. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen bzw. Verpflichtungen abzugeben sowie Kontrollmaßnahmen zu ergreifen.

Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Der Auftraggeber stimmt der Beauftragung folgender Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO bzw. eines anderen Rechtsinstruments nach dem Unionsrecht mit dem Unterauftragnehmer mit Einbeziehung dieser AGB zu:

- Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland
- netcup GmbH, Daimlerstraße 25, 76185 Karlsruhe, Deutschland
- easybell GmbH, Brückenstraße 5a, 10179 Berlin
- Google Germany GmbH, ABC-Straße 19, 20354 Hamburg, Deutschland
- Microsoft Germany GmbH, Walter-Gropius-Straße 5, 80807 München, Deutschland

Auf schriftlichen Wunsch des Auftraggebers verzichtet der Auftragnehmer Google Germany als Unterauftragnehmer einzubinden. Entsprechende von Google bereitgestellte Dienste oder Services können dann nicht angeboten werden. Details hierzu finden sich in der Servicebeschreibung.

Der Wechsel der Unterauftragnehmers ist zulässig, soweit der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber in einer angemessenen Zeit, die 14 Tage nicht unterschreiten darf, vorab schriftlich oder in Textform anzeigt und der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und eine vertragliche Vereinbarung oder eines anderen Rechtsinstruments nach dem Unionsrecht nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

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

Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

# Anhang 2 – Technische und organisatorische Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrechtzuerhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

## A2.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

**Zutrittskontrolle:** Unbefugten wird von dem Auftragsverarbeiter der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt. Folgende Maßnahmen verhindern, dass unbefugte Personen Zutritt zu Datenverarbeitungsanlagen haben:

- Festlegung von Sicherheitsbereichen
- Realisierung eines wirksamen Zutrittsschutzes, Festlegung zutrittsberechtigter Personen
- Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen über den gesamten Lebenszyklus
- Begleitung von Besuchern und Fremdpersonal
- Überwachung der Räume außerhalb der Schließzeiten, Protokollierung des Zutritts

**Zugangskontrolle:** Unbefugten wird von dem Auftragsverarbeiter die unbefugte Nutzung von Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt. Folgende Maßnahmen verhindern, dass unbefugte Dritte Zugang zu Datenverarbeitungsanlagen haben:

- Zugangsschutz (Authentisierung)
- Einfache Authentisierung der Mitarbeiter (per Benutzername/Passwort) bei hohem Schutzniveau
- Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk, Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen
- Verbot Speicherfunktion für Passwörter und/oder Formulareingaben
- Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen
- Protokollierung des Zugangs, automatische und manuelle Zugangssperre

**Zugriffskontrolle:** Der Auftragsverarbeiter gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Folgende Maßnahmen stellen sicher, dass unbefugte Dritte keinen Zugriff auf Daten haben:

- Erstellen eines Berechtigungskonzepts
- Umsetzen von Zugriffsbeschränkungen
- Vergabe minimaler Berechtigungen
- Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen
- Vermeidung der Konzentration von Funktionen
- Protokollierung des Datenzugriffs

**Trennungskontrolle:** Der Auftragsverarbeiter gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten in seinen Systemen getrennt verarbeitet werden können. Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Speicherung der Datensätze in physikalisch getrennten Datenbanken
- Verarbeitung auf mindestens logisch getrennten Systemen
- Zugriffsberechtigungen nach funktioneller Zuständigkeit
- Getrennte Datenverarbeitung durch differenzierende Zugriffsregelungen

**Pseudonymisierung** (Art 32 Abs. 1 lit a DSGVO): Die Verarbeitung personenbezogener Daten finden in einer Weise statt, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.

## A2.2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

**Weitergabekontrolle:** Ziel der Weitergabekontrolle ist es, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Es existieren folgende Maßnahmen zur Weitergabekontrolle:

- Protokollierungen jeder Übermittlung oder einer repräsentativen Auswahl
- Rechtmäßigkeit der Weitergabe ins Ausland
- Sichere Datenübertragung zwischen Server und Client, Sicherung der Übertragung im Backend, Sicherung der Übertragung zu externen Systemen, Risikominimierung durch Netzseparierung
- Implementation von Sicherheitsgateways an den Netzübergabepunkten
- Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder, Sichere, verschlüsselte Ablage von Daten
- Verhinderung von Zugriffen auf lokale Zwischenspeicher
- Sichere Datenträgeraufbewahrung, Prozess zur Sammlung und Entsorgung
- Datenschutzgerechtes Lösch-/ Zerstörungsverfahren

**Eingabekontrolle:** Ziel der Eingabekontrolle ist es, mithilfe geeigneter Maßnahmen sicherzustellen, dass nachträglich die näheren Umstände der Dateneingabe überprüft und festgestellt werden können. Es existieren folgende Maßnahmen zur Eingabekontrolle:

- Dokumentation der Anmeldungen am System
- Dokumentation der Eingabeberechtigungen

## A2.3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

**Verfügbarkeitskontrolle und Belastbarkeitskontrolle:** Der Auftragsverarbeiter gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Folgende Maßnahmen stellen sicher, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Datensicherungskonzept, welches 2 verschiedene Verfahren beinhaltet
- Recvoery-Plan mit 4 verschiedenen Optionen
- Regelmäßige Prüfung der Wiederherstellung

**Rasche Wiederherstellbarkeit:** Der Auftragsverarbeiter gewährleistet, dass die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall durch regelmäßige Datensicherungen (Backups) rasch wiederherzustellen. Um diese Anforderung der Datensicherheit zu erfüllen, hat der Auftragsverarbeiter ein Notfallmanagement erstellt und testet die Wiederherstellbarkeit der Daten regelmäßig. Dazu gehört insbesondere die regelmäßige Prüfung, dass die erstellten Datensicherungen zur Wiederherstellung verlorener Daten genutzt werden können (Notfallplan).

## A2.4 Weisungskontrolle und Auftragskontrolle

Der Auftragsverarbeiter gewährleistet durch folgende eingerichtete Maßnahmen die regelmäßige Kontrolle und den Stand seiner technischen und organisatorischen Maßnahmen entsprechend der Vorgaben der DSGVO:

- Protokollierung der Auftragsausführung durch den Auftragnehmer
- Beschränkung der Auftragsausführung

## A2.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

**Datenschutz-Management:** Organisationsstruktur und Prozesse, um nachvollziehbaren Schutz von Daten zu ermöglichen.

- Dokumentation der Prozesse im Verarbeitungsverzeichnis
- Regelmäßig Überprüfung, ob die hier dargelegte Maßnahmen ihre Zwecke noch erfüllen
- Regelmäßig Überprüfung, ob der technische Fortschritt oder neu entstandene Risiken neue oder abgeänderte Maßnahmen erfordern.

**Incident-Response-Management:** Prozesse, um die rasche und zielgerichtete Behandlung von (Datenschutz-) Vorfällen zu ermöglichen. Dies umfasst insbesondere das Melden von Datenschutzverstößen.

- Dokumentation des Incident-Prozesses
- Verpflichtung aller Mitarbeiter, Datenverstöße unverzüglich an die Geschäftsführung zu melden

**Datenschutzfreundliche Voreinstellungen** (Art. 25 Abs. 2 DS-GVO)**:** Technische und organisatorische Maßnahmen, um die Datenschutzgrundsätze (gemäß Art. 5 DS-GVO) wirksam umzusetzen.

- Maßnahmen zur Datenminimierung
- Anonymisierung / Pseudonymisierung

**Auftragskontrolle:** Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

- Sicherstellung, dass personenbezogenen Daten nur für den jeweiligen bestimmten Verarbeitungszweck unbedingt erforderlich sind, verarbeitet werden
- Keine Verwendung der Daten zu eigenen Zwecken