AGB (Allgemeine Geschäftsbedingungen) der IT-HAUS GmbH zur Auftragsverarbeitung gemäß Art. 28 DSGVO einschließlich Darstellung der getroffenen technischen und organisatorischen Maßnahmen

Einleitung

Die IT-HAUS GmbH (im Folgenden kurz: „ITH“ oder „Auftragnehmer“ oder „wir“) ist eines der Top System- und Handelshäuser in Deutschland. Als Anbieter nationaler und internationaler IT-Lösungen und Services bietet ITH umfangreiche Full-Service-Konzepte aus einer Hand. Ein starkes und flächendeckendes Netzwerk weltweit, 25 bundesweite Standorte, ein internationaler Standort in Luxembourg sowie über 260 Mitarbeiter machen ITH zu einem der führenden Anbieter im B2B-Bereich. Die Experten des Unternehmens beraten und betreuen die Kunden bei allen IT-Fragen und entwickeln innovative, intelligente und zukunftsorientierte Konzepte. Von der einfachen Anwendung bis zur umfassenden Komplettlösung.

1. Allgemeines, Geltungsbereich

(1) Die vorliegenden AGB finden Anwendung auf alle Tätigkeiten, die nach dem individuellen Kundenvertrag (im Folgenden: „Hauptvertrag“) geschuldet sind oder die mit dem Hauptvertrag im Zusammenhang stehen und bei denen wir, unsere Beschäftigten oder durch uns Beauftragte personenbezogene Daten des Auftraggebers verarbeiten (im Folgenden: „Auftragsverarbeitung“ oder „AV“). Diese AGB enthalten daher die vertraglich vereinbarten Regeln zur Auftragsverarbeitung nach Art. 28 DSGVO durch ITH für den jeweiligen Auftraggeber. Sie gelten, soweit die von ITH zu erbringenden Leistungen die Verarbeitung von personenbezogenen Daten im Auftrag umfassen bzw. erfordern, insbesondere für Leistungen von ITH wie

IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel.: +49 6502 9208-0 | Fax: +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

- das Outsourcing personenbezogener Datenverarbeitungen im Rahmen von Cloud-Computing, ohne dass ein inhaltlicher Datenzugriff von ITH als Cloud-Betreiber erforderlich ist;
- die Auslagerung von Backup-Sicherheitsspeicherungen und anderer Archivierungen;
- die Datenträgerentsorgung;
- die Prüfung oder Wartung (z.B. Fernwartung, externer Support) automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann;
- die Prüfung oder Wartung (z.B. Fernwartung, Wartung vor Ort, externer Support) von Geräten mit integriertem Speichermedium, wenn bei diesen Tätigkeiten ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann;

(2) Diese AGB gelten nur, wenn der Auftraggeber Unternehmer (§ 14 BGB), eine juristische Person des öffentlichen Rechts oder ein öffentlich-rechtliches Sondervermögen ist.

(3) Sofern nichts anderes vereinbart ist, gelten diese AGB in der zum Zeitpunkt der Bestellung des Auftraggebers gültigen bzw. jedenfalls in der ihm zuletzt in Textform mitgeteilten Fassung als Rahmenvereinbarung auch für gleichartige künftige Verträge, ohne dass wir in jedem Einzelfall wieder auf sie hinweisen müssten.

(4) Diese AGB gelten ausschließlich. Abweichende, entgegenstehende oder ergänzende Allgemeine Geschäftsbedingungen des Auftraggebers werden nur dann und insoweit AV-Vertragsbestandteil, als wir ihrer Geltung ausdrücklich zugestimmt haben. Dieses Zustimmungserfordernis gilt in jedem Fall, beispielsweise auch dann, wenn wir in Kenntnis der AGB des Auftraggebers die Leistung an ihn vorbehaltlos ausführen.

(5) Im Einzelfall getroffene, individuelle Vereinbarungen mit dem Auftraggeber (einschließlich Nebenabreden, Ergänzungen und Änderungen) haben in jedem Fall Vorrang vor diesen AGB. Die Verarbeitungsdetails werden durch den individuellen Hauptvertrag definiert.

(6) Hinweise auf die Geltung gesetzlicher Vorschriften haben nur klarstellende Bedeutung. Auch ohne eine derartige Klarstellung gelten daher die gesetzlichen Vorschriften, soweit sie in diesen AGB nicht unmittelbar abgeändert oder ausdrücklich ausgeschlossen werden.

IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel.: +49 6502 9208-0 | Fax: +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

2. Gegenstand und Dauer

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich Lieferungen, Leistungen und Services im IT-Bereich des Auftraggebers. Im Übrigen gelten die Regelungen des Hauptvertrags.

(2) Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses AV-Vertrages.

(3) Die AV-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).

(4) Dieser AV-Vertrag wird auf unbestimmte Zeit geschlossen. Er kann von beiden Parteien mit einer Frist von einem Monat zum Monatsende gekündigt werden. Bei einem bestehenden Hauptvertrag ist eine gesonderte Beendigung dieser Vereinbarung ohne gleichzeitige Beendigung des Hauptvertrags ausgeschlossen; es gelten hierfür dann einheitlich die Kündigungsfristen und Kündigungstermine des Hauptvertrags.

(5) Der Auftraggeber kann den AV-Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses AV-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 AV-Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel.: +49 6502 9208-0 | Fax: +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

3. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

(1) Art und Zweck der Verarbeitung:
Verarbeitung von Daten zur Sicherstellung von Lieferungen, Leistungen und Services im IT- Bereich des Auftraggebers. Art und Zweck der Verarbeitung ergeben sich im Übrigen aus dem Hauptvertrag und dem Umfang der individuellen Verarbeitungen des Auftraggebers.

(2) Art der personenbezogenen Daten:
Die Art der im Rahmen der Datenverarbeitung verarbeiteten personenbezogenen Daten wird vom Auftraggeber selbst bestimmt. Beispiele für verarbeitete Daten sind: Name, Vorname, Adresse, Telefonnummer, E-Mailadresse, Geburtsdatum, Abrechnungsdaten.

(3) Kategorien betroffener Personen:
Der Kreis der von der Verarbeitung Betroffenen besteht aus Mitarbeitern, Lieferanten/Herstellern und/oder Kunden. Die Kategorien betroffener Personen ergeben sich im Übrigen aus dem Hauptvertrag und den konkreten Datenverarbeitungsprozessen 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) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

(3) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen nicht mündlich, sondern schriftlich oder in einem dokumentierten elektronischen Format. Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren.

IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel.: +49 6502 9208-0 | Fax: +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

(4) 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 AV-Vertrag festgelegten Verpflichtungen zu überzeugen.

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

(6) Der Auftraggeber ist verpflichtet, alle im Rahmen des AV-Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses AV-Vertrages bestehen.

5. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

(1) Der Auftraggeber teilt dem Auftragnehmer seine im Rahmen dieses AV-Vertrags weisungsbefugten Personen mit (Name, Funktion, Telefonnummer, E-Mailadresse). Weisungsempfänger beim Auftragnehmer sind die dortigen individuellen Ansprechpartner.

(2) Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem AV-Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. 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 Auftragnehmer unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragnehmer dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit,

IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel.: +49 6502 9208-0 | Fax: +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

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. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die AV-Vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

(4) Der Auftragnehmer hat über die gesamte Abwicklung der Dienstleistung für den Auftraggeber insbesondere folgende Überprüfungen in seinem Bereich durchzuführen:

- Sicherheitsüberprüfungen auf Infrastruktur- und Applikationsebene;
- Verfügbarkeitskontrolle der Daten durch regelmäßige Datensicherung

Das Ergebnis der Kontrollen ist zu dokumentieren.

(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). Der Auftraggeber trägt die dem Auftragnehmer hierdurch entstehenden Kosten, sofern nicht anders vereinbart (z.B. im Hauptvertrag oder Auftrag).

(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

IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel.: +49 6502 9208-0 | Fax: +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

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 aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

(9) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der AV-Vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs.3 Satz 2 lit. h DSGVO).

(10) Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt. Hierzu wird bis auf weiteres folgendes vereinbart: Ein vom Auftraggeber beauftragter Dritter darf nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören. Sofern nicht anders vereinbart (im Hauptvertrag, Auftrag u.a.), trägt der Auftraggeber die dem Auftragnehmer entstehenden Kosten der Vor- Ort- Kontrolle.

(11) Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers AV-vertraglich sicher zu stellen. 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. Er

IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel.: +49 6502 9208-0 | Fax: +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

verpflichtet sich, die für den Auftrag relevanten Geheimnisschutzregeln zu beachten, denen der Auftraggeber unterliegt.

(13) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des AV-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.

(15) Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz Frau Tamara Mai, IT-HAUS GmbH, 06502-9208-223, datenschutz@it-haus.com, bestellt. Ein Wechsel des/der Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

7. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und 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). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 5 dieses AV-Vertrages durchführen.

IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel.: +49 6502 9208-0 | Fax: +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

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

(1) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DSGVO, welche auf einem der o. g. Kommunikationswege (Ziff. 5) erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

(2) 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).

(3) 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. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

(4) 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).

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

(6) Der Auftragnehmer hat die Einhaltung der Pflichten der / des Subunternehmer(s) regelmäßig zu prüfen.

IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel.: +49 6502 9208-0 | Fax: +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

(7) 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.

(8) Die Subunternehmer, die IT-HAUS mit der Verarbeitung von personenbezogenen Daten beschäftigt, kann der Auftraggeber bei dem persönlichen Ansprechpartner anfragen oder unter info@it-haus.com. Mit der Beauftragung dieser Subunternehmer erklärt sich der Auftraggeber im Rahmen der Bestimmungen des Hauptvertrags und der hiernach vom Auftragnehmer geschuldeten Tätigkeiten einverstanden.

(9) Der Auftragsverarbeiter informiert den Verantwortlichen immer 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 (§ 28 Abs. 2 Satz 2 DSGVO).

(10) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

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

(1) 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

IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel.: +49 6502 9208-0 | Fax: +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

(2) Für die auftragsgemäße Verarbeitung personenbezogener Daten wird eine angemessene und nachvollziehbare Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten Betroffener berücksichtigt.

(3) Das nachstehend beschriebene Datenschutzkonzept 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; das nachstehend beschriebene Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der datenschutzkonformen Verarbeitung wird als verbindlich festgelegt:

a) **Zutrittskontrolle**

Technische bzw. organisatorische Maßnahmen zur Zutrittskontrolle, insbesondere auch zur Legitimation der Berechtigten:

→ Werkschutz, Pförtner
→ Zutrittskontrollsystem,
→ Anmeldesystem der Zutrittberechtigten, Ausweiskontrolle
→ Türsicherung (elektrische Türöffner)
→ Überwachungseinrichtung Alarmanlage, Video- / Fernsehmonitor

b) **Zugangskontrolle**

Technische (Kennwort- / Passwortschutz) und organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung

→ Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
→ Automatische Sperrung (Kennwort / Pausenschaltung)
→ Einrichtung eines Benutzerstammsatzes pro User
→ Verschlüsselung von Datenträgern

IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel.: +49 6502 9208-0 | Fax: +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

c) **Zugriffskontrolle**

Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung:

→ Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
→ Auswertungen
→ Kenntnisnahme
→ Veränderung
→ Löschung

d) **Weitergabekontrolle**

Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung:

→ Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network)
→ Protokollierung
→ Transportsicherung

e) **Eingabekontrolle**

Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind:
Beispiel: Protokollierungs- und Protokollauswertungssysteme

f) **Auftragskontrolle**

Maßnahmen (technisch / organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer:

- AV-Vertragsgestaltung
- Formalisierte Auftragserteilung (Auftragsformular/Mail/bestimmter Personenkreis auf Seitendes Auftraggebers und -nehmers)
- Kontrolle der AV-Vertragsausführung

g) **Verfügbarkeit und Belastbarkeit**

Maßnahmen zur Datensicherung (physikalisch / logisch):

- Backup-Verfahren (Backup to Disk to Tape [B2D2T])
- Spiegeln von Festplatten, z.B. RAID-Verfahren
- Unterbrechungsfreie Stromversorgung (USV)
- Virenschutz / Firewall
- Notfallplan

IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel.: +49 6502 9208-0 | Fax: +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

h) **Trennungskontrolle**

Maßnahmen zur getrennten Verarbeitung von Daten mit unterschiedlichen Zwecken:

- "Interne Mandantenfähigkeit" / Zweckbindung
- Funktionstrennung /Produktion / Test

i) **Pseudonymisierung**

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

j) **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

→ Incident-Response-Management;

→ Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

→ Datenschutz-Management:

Es muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung des Datenschutzes und der Wirksamkeit der festgelegten technischen und organisatorischen Maßnahmen implementiert sein.

Bei dem Datenschutz-Managementsystem (DSMS) verfolgt der Auftragnehmer den prozessorientierten Ansatz, d.h. die Prozesse des Auftragnehmers stehen im Vordergrund und nicht die Aufbauorganisation. Die allgemeine Vorgehensweise bei der Einführung des DSMS ist der Deming-Kreis, auch bekannt als PDCA-Methodik (Plan-Do-Check-Act), der auch beim Qualitätsmanagementsystemen verwendet wird. Diese Methodik ermöglicht es, sich auf ändernde Ereignisse einzustellen und das System verbessern zu können.

- Plan: In der Planungsphase wurden/werden Ziele, die Strategien, Prozesse, Budgets und Zeitvorgaben erstellt. Dies geschieht bei dem aufzusetzenden DSMS und wenn Anpassungen des DSMS nach der Act-Phase erfolgen. U.a: Datenschutzrichtlinie/-leitlinie, Einbindung des Datenschutzbeauftragten, Verzeichnis von Verarbeitungstätigkeiten, AV-Vertragsmanagement, Verpflichtung auf das Datengeheimnis, Datenschutzschulung/-en, Prozesse zur Wahrnehmung von Betroffenenrechten, Meldung von Datenschutzverstößen, Nachweis der Datensicherheit.

IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel.: +49 6502 9208-0 | Fax: +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

- Do: In der Umsetzungs- und Durchführungsphase wird das DSMS gemäß der erstellten Planung umgesetzt. Z.B. Umgang mit Auskunftsverlangen, Meldung von Datenschutzverletzungen, Löschverlangen usw.

- Check: Die Phase der Überwachung und Überprüfung soll zur Messung und Aufrechterhaltung des DSMS dienen und Hinweise für Verbesserungen bzw. Anpassungen liefern. U.a. Erstellung von regelmäßigen DSMS- Bewertungen. Darüber hinaus müssen die Risikoeinschätzungen in regelmäßigen Zeitabständen hinsichtlich Veränderungen der Organisation, von Prozessen, Bedrohungen etc. überprüft werden.

- Act: In der Verbesserungsphase werden die Erkenntnisse aus der Check-Phase verarbeitet und damit das DSMS verbessert. Die identifizierten Verbesserungen sind umzusetzen, Korrekturmaßnahmen und Vorbeugemaßnahmen aus Sicherheitsvorfällen zu ziehen und es ist sicherzustellen, dass die Verbesserungen auch tatsächlich die vorgenommenen Ziele erreichen. Nach dieser Phase startet der Prozess wieder mit der Planungsphase. Ziel ist, dass sich das DSMS ständig optimiert und weiter verbessert. Das DSMS ist ständigen neuen Einflüssen und Gefährdungen ausgesetzt, auf die der Auftragnehmer reagieren muss.

  Beim Auftragnehmer umgesetzte Maßnahmen u.a.:
  - Löschen nicht mehr benötigter Daten (z. B. veraltete Daten, Testumgebungen)
  - Sichere Entsorgung defekter/nicht mehr benötigter Hardware
  - Sichere Entsorgung von Dokumenten (z. B. Aktenvernichter, Reisswolf)
  - Sichere Aufbewahrung von Dokumenten (z.B. abschließbare Aktenschränke)

(4) 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 samt

IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel.: +49 6502 9208-0 | Fax: +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

vollständigem Auditbericht ist dem Auftraggeber auf dessen Wunsch hin vom Auftragnehmer mitzuteilen.

(5) Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.

(6) Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

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

(8) Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Ob die hierdurch entstehenden Kosten vom Auftraggeber dem Auftragnehmer zu erstatten sind, folgt aus den übrigen Vereinbarungen (Hauptvertrag, Auftrag u.a.) der Parteien. Die Abstimmungen sind für die Dauer dieses AV-Vertrages aufzubewahren.

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 auszuhändigen oder auf schriftliche (Textform ist ausreichend) Anweisung des Auftraggebers hin datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen. In diesem Fall ist der Auftragnehmer verpflichtet, organisatorisch sicherzustellen, dass die Daten des Auftraggebers auch tatsächlich gelöscht bzw. vernichtet werden können; der Auftragnehmer hat sämtliche Beschäftigten über diese Löschpflichten zu informieren.

(2) Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel.: +49 6502 9208-0 | Fax: +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

11. Haftung

(1) Auf Art. 82 DSGVO wird verwiesen

(2) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber gegenüber dem Betroffenen verantwortlich.

12. Sonstiges

(1) Diese Vereinbarung unterliegt dem Recht der Bundesrepublik Deutschland. Gerichtsstand für alle Streitigkeiten aus dem AV-Vertragsverhältnis zwischen Auftraggeber und Auftragnehmer ist der Sitz des Auftragnehmers.

(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) Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

(4) 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.

(5) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(6) Die vorliegende Vereinbarung enthält für die Auftragsverarbeitung alle Angaben nach Art. 30 DSG- VO für das Verzeichnis von Verarbeitungstätigkeiten.

(7) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel.: +49 6502 9208-0 | Fax: +49 6502 9208-850 | www.it-haus.com | info@it-haus.com

Geschäftsführer: Ingo Burggraf, Stefan Sicken, Dr. Thomas Simon

Handelsregister: Amtsgericht Wittlich, HRB 3983 USt-IdNr.: DE 192 270 896

Anschrift: IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Deutschland / Germany

IT-HAUS GmbH | Europa-Allee 26/28 | 54343 Föhren | Tel.: +49 6502 9208-0 | Fax: +49 6502 9208-850 | www.it-haus.com | info@it-haus.com