PROJEKT **PRO**

AUFTRAGSVERARBEITUNGSVERTRAG

Zwischen

.....

.....

.....

.....

- Verantwortlicher im Sinne der DS-GVO, nachfolgend 'Auftraggeber' genannt -

und

PROJEKT PRO GmbH
vertr. d. d. Geschäftsführer Harald Mair
Kampenwandstraße 77c
83229 Aschau i. Ch.

- Auftragsverarbeiter im Sinne der DS-GVO, nachfolgend 'Auftragnehmer' genannt -

PROJEKT PRO GmbH
Bürosoftware für Architekten und Ingenieure

Kampenwandstraße 77c
D-83229 Aschau im Chiemgau
Telefon **+49 8052 95179-0**
Telefax **+49 8052 95179-79**
E-Mail **info@projektpro.com**
www.**projektpro.com**

Geschäftsführer **Harald Mair**
Amtsgericht Traunstein HRB 15475

§ 1 Gegenstand des Auftrags

Der Auftragnehmer verarbeitet personenbezogene Daten gem. Art. 4 Ziff. 1 DS-GVO im Auftrag des Auftraggebers nach Art. 5 DS-GVO. Dies umfasst Tätigkeiten, die in den zwischen den Parteien geschlossenen Software-Pflegeverträgen oder Serviceaufträgen enthaltenen Leistungsbeschreibungen konkretisiert sind.

§ 2 Verantwortlichkeit

(1) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie die Rechtmäßigkeit der Datenverantwortung verantwortlich ('Verantwortlicher' im Sinne des Art. 4 Ziff. 7 DS-GVO).

(2) Auftraggeber sowie Auftragnehmer müssen gewährleisten, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Dazu müssen alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, auf das Datengeheimnis verpflichtet und über ihre Datenschutzpflichten belehrt werden. Dabei ist jede Partei für die Verpflichtung des eigenen Personals zuständig. Ferner müssen die eingesetzten Personen darauf hingewiesen werden, dass das Datengeheimnis auch nach Beendigung der Tätigkeit fortbesteht.

(3) Der Auftragnehmer und der Auftraggeber sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

§ 3 Dauer des Auftrags

(1) Der Vertrag wird mit der Unterzeichnung wirksam und korrespondiert mit den zwischen den Parteien geschlossenen Software-Pflegeverträgen oder Serviceaufträgen. Jede Partei ist berechtigt, den Vertrag mit einer Frist von vier Wochen zum Monatsende zu kündigen.

(2) Es ist den Vertragspartnern bewusst, dass ohne Vorliegen eines gültigen AV-Vertrages, z. B. bei Beendigung des vorliegenden Vertragsverhältnisses, keine (weitere) Auftragsverarbeitung durchgeführt werden darf.

(3) Das Recht zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt.

(4) Kündigungen bedürfen zu ihrer Wirksamkeit der Schriftform.

§ 4 Weisungsbefugnis des Auftraggebers

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Auftraggebers. Ausgenommen hiervon sind Sachverhalte, in denen dem Auftragnehmer eine Verarbeitung aus zwingenden rechtlichen Gründen auferlegt wird. Der Auftragnehmer unterrichtet, soweit ihm möglich, in derartigen Situationen den Auftraggeber vor Beginn der Verarbeitung über die entsprechenden rechtlichen Anforderungen. Der Auftraggeber behält sich ein im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann.

(2) Die Weisungen des Auftraggebers werden vom Auftragnehmer dokumentiert und dem Auftraggeber unmittelbar nach erfolgter Dokumentation als unterschriebene Kopie zur Verfügung gestellt.

§ 5 Leistungsort

(1) Der Auftragnehmer wird die vertraglichen Leistungen in der Europäischen Union (EU) oder im Europäischen Wirtschaftsraum (EWR) oder einem sicheren Drittland erbringen. Dies gilt in gleicher Weise für etwaige Unterauftragnehmer. Erfolgt eine Leistungserbringung in einem Drittland, garantiert der Auftragnehmer die Einhaltung der diesbezüglichen Vorgaben der DS-GVO und weist dies auf Verlangen nach.

(2) Der Auftraggeber stimmt einer Verlagerung des Ortes der Leistungserbringung innerhalb des Leistungslandes, für das eine Zustimmung besteht, zu, wenn dort nachweislich ein gleiches Sicherheitsniveau gegeben ist und keine für den Auftraggeber geltenden gesetzlichen Bestimmungen gegen diese Verlagerung sprechen. Die Nachweispflicht hierzu liegt beim Auftragnehmer.

(3) Bei einer Verlagerung des Ortes der Leistungserbringung in Länder, die Mitglied der EU / EWR sind und über ein diesem Vertrag genügendes und verifiziertes Datenschutzniveau verfügen, wird der Auftraggeber schriftlich informiert.

(4) Sofern der Auftragnehmer vom Auftraggeber nicht innerhalb einer Frist von vier Wochen nach Zugang der Mitteilung gemäß Abs. 3 über Gründe informiert wird, die eine Verlagerung nicht zulassen, gilt die Zustimmung zu dieser Verlagerung seitens des Auftraggebers als erteilt.

(5) Wenn der Auftragnehmer die geschuldeten Leistungen ganz oder teilweise von einem Standort außerhalb der EU/EWR in einem sog. sicheren 'Drittland' erbringen möchte bzw. die Leistungserbringung dorthin zu verlagern plant, wird der Auftragnehmer zuvor die schriftliche Zustimmung durch den Auftraggeber einholen.

(6) Sofern die Leistungsverlagerung in ein anderes Land nach den vorstehenden Regelungen möglich ist, gilt dies entsprechend für jeglichen Zugriff bzw. jegliche Sicht auf die Daten durch den Auftragnehmer, z. B. im Rahmen von internen Kontrollen oder zu Zwecken der Entwicklung, der Durchführung von Tests, der Administration oder der Wartung.

(7) Sofern die Datenverarbeitung nach dieser Vereinbarung und den gesetzlichen Vorgaben zur Verarbeitung personenbezogener Daten im Auftrag bzw. zur Übermittlung personenbezogener Daten ins Ausland zulässig außerhalb Deutschlands erbracht werden darf, wird der Auftragnehmer für die Einhaltung und Umsetzung der gesetzlichen Erfordernisse zur Sicherstellung eines adäquaten Datenschutzniveaus bei Standortverlagerungen und bei grenzüberschreitendem Datenverkehr Sorge tragen.

§ 6 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten nur im Rahmen des Auftrages und der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Anforderungen der entsprechenden datenschutzrechtlichen Bestimmungen entsprechen; diese Maßnahmen muss der Auftragnehmer auf Anfrage dem Auftraggeber und ggfs. der Aufsichtsbehörde gegenüber nachweisen. Dieser Nachweis beinhaltet insbesondere die Umsetzung der aus Art. 32 DS-GVO resultierenden Maßnahmen.

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative, nachweislich adäquate Maßnahmen umzusetzen. Dabei muss sichergestellt sein, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren. Eine Darstellung dieser technischen und organisatorischen Maßnahmen erfolgt in Anlage 1 zu diesem Vertrag.

(3) Der Auftragnehmer selbst führt für die Verarbeitung ein Verzeichnis der bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 DS-GVO. Er stellt auf Anforderung dem Auftraggeber die für die Übersicht nach Art. 30 DS-GVO notwendigen Angaben zur Verfügung. Des Weiteren stellt er das Verzeichnis auf Anfrage der Aufsichtsbehörde zur Verfügung.

(4) Der Auftragnehmer unterstützt den Auftraggeber bei etwaigen erforderlichen Datenschutz-Folgenabschätzungen mit allen ihm zur Verfügung stehenden Informationen. Im Falle der Notwendigkeit einer vorherigen Konsultation der zuständigen Aufsichtsbehörde unterstützt der Auftragnehmer den Auftraggeber auch hierbei.

(5) Als Datenschutzbeauftragter ist beim Auftragnehmer derzeit Enzo Berger, c/o PROJEKT PRO GmbH, Kampenwandstraße 77 c, 83229 Aschau im Chiemgau, datenschutz@projektpro.com benannt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich mitzuteilen. Der Auftragnehmer gewährleistet, dass die Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß Art. 38 DS-GVO erfüllt werden. Sofern kein Datenschutzbeauftragter beim Auftragnehmer benannt ist, benennt der Auftragnehmer dem Auftraggeber einen Ansprechpartner.

(6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich bei Verstößen des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen. Er trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die Betroffenen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung der Informationspflichten gegenüber der jeweils zuständigen Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen nach Art. 33, 34 DS-GVO.

(7) Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(8) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind.

(9) Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer betroffenen Person verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereitzustellen, vorausgesetzt der Auftraggeber hat den Auftragnehmer hierzu schriftlich aufgefordert.

(10) Der Auftragnehmer informiert den Auftraggeber unverzüglich über Kontrollen und Maßnahmen durch die Aufsichtsbehörden oder falls eine Aufsichtsbehörde bei dem Auftragnehmer ermittelt.

(11) 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 Auftraggeber bestätigt oder geändert wird.

(12) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichen im Sinne der DS-GVO liegen.

(13) Der Auftragnehmer verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung und setzt auch keine Mittel zur Verarbeitung ein, die nicht vom Auftraggeber zuvor genehmigt wurden.

(14) Der Auftragnehmer speichert keine Daten, die einer besonderen Verschwiegenheit unterliegen, auf Systemen, die außerhalb der Verfügungsgewalt des Auftraggebers liegen bzw. die nicht dem Beschlagnahmeschutz unterliegen.

(15) Sofern der Auftragnehmer durch das Recht der Union oder Mitgliedstaaten verpflichtet ist, die Daten auch auf andere Weise zu verarbeiten, teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(16) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren, zu dokumentieren und in geeigneter Weise gegenüber dem Auftraggeber auf Anforderung nachzuweisen.

§ 7 Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Der Auftraggeber wird in seinem Verantwortungsbereich dafür Sorge tragen, dass die gesetzlich notwendigen Voraussetzungen (z. B. durch Einholung von Einwilligungserklärungen für die Verarbeitung der Daten) geschaffen werden, damit der Auftragnehmer die vereinbarten Leistungen rechtsverletzungsfrei erbringen kann.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Der Auftraggeber ist hinsichtlich der vom Auftragnehmer eingesetzten und vom Auftraggeber genehmigten Verfahren zur automatisierten Verarbeitung personenbezogener Daten datenschutzrechtlich verantwortlich und hat – neben der eigenen Verpflichtung des Auftragnehmers – ebenfalls die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten.

(4) Dem Auftraggeber obliegen die aus Art. 33, 34 DS-GVO resultierenden Informationspflichten gegenüber der Aufsichtsbehörde bzw. den von einer Verletzung des Schutzes personenbezogener Daten Betroffenen.

(5) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.

(6) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Betriebsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

(7) Der Auftraggeber stellt sicher, dass die aus Art. 32 DS-GVO resultierenden Anforderungen bzgl. der Sicherheit der Verarbeitung seinerseits eingehalten werden. Insbesondere gilt dies für Fernzugriffe des Auftragnehmers auf die Datenbestände des Auftraggebers.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unter dem Aspekt ausgewählt, dass dieser hinreichend Garantien dafür bietet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Er dokumentiert das Ergebnis seiner Auswahl.

Hierfür kann er beispielsweise

- datenschutzspezifische Zertifizierungen oder Datenschutzsiegel und –prüfzeichen berücksichtigen
- schriftliche Selbstauskünfte des Auftragnehmers einholen
- sich ein Testat eines Sachverständigen vorlegen lassen
- sich nach rechtzeitiger Anmeldung zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs persönlich oder durch einen sachkundigen Dritten, der nicht in einem Wettbewerbsverhältnis zum Auftragnehmer stehen darf, von der Einhaltung der vereinbarten Regelungen überzeugen.

(2) Liegt ein Verstoß des Auftragnehmers oder der bei ihm im Rahmen des Auftrags beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder der im Vertrag getroffenen Festlegungen vor, so kann eine darauf bezogene Prüfung auch ohne rechtzeitige Anmeldung vorgenommen werden. Eine Störung des Betriebsablaufs beim Auftragnehmer sollte auch hierbei weitestgehend vermieden werden. Die Durchführung der Auftragskontrolle mittels regelmäßiger Prüfungen durch den Auftraggeber im Hinblick auf die Vertragsausführung bzw. -erfüllung, insbesondere Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung des Auftrags wird vom Auftragnehmer unterstützt. Insbesondere verpflichtet sich der Auftragnehmer, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind.

§ 9 Berichtigung und Beschränkung bei Verarbeitung, Löschung und Rückgabe von Datenträgern

(1) Während der laufenden Beauftragung berichtigt, löscht oder sperrt der Auftragnehmer die vertragsgegenständlichen Daten nur auf Anweisung des Auftraggebers.

(2) Sofern eine Vernichtung von Datenträgern und sonstiger Materialien während der laufenden Beauftragung vorzunehmen ist, übernimmt der Auftragnehmer die nachweislich datenschutzkonforme Vernichtung nur aufgrund entsprechender Einzelbeauftragung durch den Auftraggeber. Dies gilt nicht, sofern im Hauptvertrag bereits eine entsprechende Regelung getroffen worden ist.

(3) In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.

(4) Nach Abschluss der Erbringung der Verarbeitungsleistungen muss der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder löschen oder diesem zurückgeben, sofern nicht nach dem Unionsrecht oder dem für den Auftragnehmer geltenden nationalen Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Gleiches gilt für alle Daten, die Betriebs- oder Geschäftsgeheimnisse des Auftraggebers beinhalten. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(5) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

(6) Der Auftraggeber kann jederzeit, d. h. sowohl während der Laufzeit als auch nach Beendigung des Vertrages, die Berichtigung, Löschung, Verarbeitungseinschränkung (Sperrung) und Herausgabe von Daten durch den Auftragnehmer verlangen, solange der Auftragnehmer die Möglichkeit hat, diesem Verlangen zu entsprechen.

(7) Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist. Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragnehmer aufgrund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Einzelfall etwas anderes vereinbart ist. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(8) Sollte dem Auftraggeber eine Rücknahme der Daten nicht möglich sein, wird er den Auftragnehmer rechtzeitig schriftlich informieren. Der Auftragnehmer ist dann berechtigt, personenbezogene Daten im Auftrag des Auftraggebers zu löschen.

§ 10 Unterauftragnehmer

(1) Der Auftragnehmer ist nur mit ausdrücklicher vorheriger Zustimmung des Auftraggebers zur Einschaltung von Unterauftragnehmern berechtigt.

(2) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht. Hierbei muss jedoch jeder Unterauftragnehmer (verbundenes Unternehmen) vor Beauftragung dem Auftraggeber schriftlich angezeigt werden, sodass der Auftraggeber bei Vorliegen wichtiger Gründe die Beauftragung untersagen kann.

§ 11 Haftung

(1) Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der DS-GVO entsprechende Verarbeitung verursacht wird, gemeinsam im Außenverhältnis gegenüber der jeweiligen betroffenen Person.

(2) Der Auftragnehmer haftet ausschließlich für Schäden, die auf einer von ihm durchgeführten Verarbeitung beruhen, bei der

- er den aus der DS-GVO resultierenden und speziell für Auftragsverarbeiter auferlegten Pflichten nicht nachgekommen ist, oder
- er unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers handelte, oder
- er gegen die rechtmäßig erteilten Anweisungen des Auftraggebers gehandelt hat, oder
- er gegen ihm aus dem vorliegenden Vertrag obliegenden Pflichten verstoßen hat.

(3) Soweit der Auftraggeber zum Schadensersatz gegenüber dem Betroffenen verpflichtet ist, bleibt ihm der Rückgriff auf den Auftragnehmer vorbehalten.

(4) Im Innenverhältnis zwischen Auftraggeber und Auftragnehmer haftet der Auftragnehmer für den durch eine Verarbeitung verursachten Schaden jedoch nur, wenn er

a) seinen ihm speziell durch die DS-GVO auferlegten Pflichten nicht nachgekommen ist oder

b) unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des Auftraggebers oder gegen diese Anweisungen gehandelt hat.

(5) Weitergehende Haftungsansprüche nach den allgemeinen Gesetzen bleiben unberührt.

§ 12 Sonstiges

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

(2) Für Nebenabreden ist die Schriftform erforderlich.

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

(4) Es gilt deutsches Recht. Gerichtsstand ist der Sitz der PROJEKT PRO GmbH.

Ort, Datum

Auftraggeber

Ort, Datum

Auftragnehmer

Anlage 1

UMSETZUNG TECHNISCHER UND ORGANISATORISCHER MASSNAHMEN BEIM AUFTRAGNEHMER

Diese Gliederung ist angelehnt an die Informationssicherheit nach ISO 27001.

Informationssicherheitsrichtlinien

Der Auftragnehmer verfügt über eine Informationssicherheitsleitlinie, die allen Mitarbeitern bekannt ist.

Organisation und Informationssicherheit

Für die Informationssicherheit ist die Geschäftsführung des Auftragnehmers verantwortlich.

Es gibt eine Leitlinie für die mobilen Endgeräte, diese müssen verschlüsselt und mit Passwort gesichert werden.

Personalsicherheit

Im Arbeitsvertrag und einer ergänzenden Verpflichtungserklärung zum Datenschutz ist die Verpflichtung zur Informationssicherheit mit den Mitarbeitern geregelt. Die Teilnahme an regelmäßigen Schulungen zum Datenschutz und zur Informationssicherheit ist verpflichtend und wird dokumentiert. Bei Abwesenheit werden die Schulungen per Videoaufzeichnung zur Verfügung gestellt. Es gibt eine Leitlinie für On- und Offboarding von Mitarbeitern.

Verwaltung der Werte

Die Verwaltung von Werten ist durch ein Inventarverzeichnis mit Personenzuordnung und einem Verzeichnis der Verarbeitungstätigkeiten sichergestellt. Informationen werden entsprechend von Werten und Risiken klassifiziert, um einen angemessenen Schutz sicher zu stellen. Zum Beispiel sind mobile Datenträger verschlüsselt, andere mobile Medien werden nicht verwendet.

Zugangssteuerung

Ein Zugang zu den Netzwerken und Netzwerkdiensten des Auftragnehmers ist nur via VPN oder anderen verschlüsselten Verbindungen möglich. Interne Anwendungen wie Fileserver, PROJEKT PRO und weitere Netzwerkdienste erfordern eine Authentifizierung. Die Benutzerkonten sind von Administratorenkonten getrennt. Vertrauliche Informationen oder personenbezogene Daten werden in verschlüsselten Datenbanken oder in gesicherten Bereichen am Fileserver gespeichert. Der Zugriff auf Informationen und Applikationen wird durch Rollen und Zugriffsrechte geregelt.

Kryptographie

Es gibt eine Leitlinie für die Verwendung von Verschlüsselung und zur Verwaltung der Schlüssel.

Physische und umgebungsbezogene Sicherheit

Die Büroräume sowie der Zutritt zum Empfang sind versperrt und die Mitarbeiter sind angewiesen, betriebsfremden Personen keinen Zutritt zu gewähren. Die Übergabe der Büroschlüssel ist dokumentiert. Die IT-Infrastruktur ist versperrt und nur für autorisierte Personen zugänglich. Die Büroräume und die Infrastruktur sind vor Überspannung gesichert. USV, Brandschutzkonzept mit Brandmeldeanlage und Feuerlöscher sind vorhanden. Interne Brandschutz- und Sicherheitsbeauftragte überwachen die Einhaltung der Vorschriften.

Eine Leitlinie für Werteanschaffung definiert die hohe Qualität der Ausstattung, sichert die regelmäßige Instandhaltung und gewährt eine sichere Entsorgung. Waren werden beim Eingang kontrolliert und auf Versiegelung geprüft. Bei Geräten mit Windows oder macOS wird eine Neuinstallation des Betriebssystems durchgeführt.

Betriebssicherheit

In der Software-Entwicklung wird das Changemanagement durch Tickets und Anforderungen dokumentiert. Die Entwicklungs-, Test- und Produktivumgebung sind voneinander getrennt. Für einen umfangreichen Schutz gegen Schadsoftware sorgen Antivirensoftware und Firewalls. Der Auftragnehmer hat eine Backupleitlinie in der die regelmäßigen Backups und Prüfung der Wiederherstellung definiert sind. Die Firewall besitzt ein umfangreiches Logging. Bei Fehlfunktionen der Infrastruktur ergeht eine Alarmmeldung an die zuständigen Personen. Administratoren dokumentieren relevante durchgeführte Arbeitstätigkeiten und Veränderungen an den Systemen. Informationssysteme werden durch Monitoring-Software überwacht.

Kommunikationssicherheit

Die Netzwerke werden verwaltet und kontrolliert, um Informationen in Systemen und Anwendungen zu schützen und bei Ausfall mit redundanten Komponenten den Betrieb wiederherzustellen. Kalkulierte Ausfallzeiten sind im Risikomanagement berücksichtigt und über redundante Komponenten und Notfallpläne geregelt. Eine Netzwerksegmentierung ist vorhanden. Die Verwendung von Diensten zum Informationsaustausch ist geregelt. Beim Informationsaustausch mit Dritten werden Geheimhaltungsvereinbarungen geschlossen.

Anschaffung, Entwicklung und Instandhaltung von Systemen

Die Anforderungen an die Beschaffung von Informationssystemen ist durch die zentrale Freigabe durch die Geschäftsführung sichergestellt. Die Sicherheit im Software-Entwicklungsprozess wird durch die Software-Qualitätssicherung abgedeckt. Für die Softwaretests werden ausschließlich fiktive Daten verwendet.

Lieferantenbeziehung

Sicherung der langfristigen Geschäftsbeziehung durch regelmäßige Kontakte und vertrauensvolle Zusammenarbeit. Die erbrachten Leistungen der Lieferanten werden nach der vorhandenen Leitlinie überprüft.

Handhabung von Informationssicherheitsvorfällen

Berichtswesen für Vorfälle in der Informationssicherheit (Incident Management) ist vorhanden.