PROJEKT **PRO**

Auftragsverarbeitungsvertrag

PROJEKT PRO GmbH Software
für Architekt:innen und Ingenieur:innen

Georg-Wiesböck-Ring 9
D-83115 Neubeuern

Telefon + 49 8035 94608-0

E-Mail info@projektpro.com
www.projektpro.com

Geschäftsführer **Manfred Scholz, Matthias Werner**
Amtsgericht Traunstein HRB 15475

Zwischen

Dem „Verantwortlichen" im Sinne dieses Vertrages ist dies das Unternehmen, das Softwarelösungen der PROJEKT PRO GmbH in Anspruch nimmt und im Sinne von Art. 4 Nr. 7 DSGVO über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet.

- nachfolgend 'Auftraggeber' genannt –

und

PROJEKT PRO GmbH vertr. d. d. Geschäftsführer Manfred Scholz, Matthias Werner, Georg-Wiesböck-Ring 9 in 83115 Neubeuern

- Auftragsverarbeiter im Sinne der DSGVO, nachfolgend ‚Auftragnehmer' genannt -

§ 1 Gegenstand des Auftrags

Der Auftragnehmer verarbeitet personenbezogene Daten gem. Art. 4 Ziff. 1 DSGVO im Auftrag des Auftraggebers nach Art. 5 DSGVO. Dies umfasst Tätigkeiten, die in dem zwischen den Parteien geschlossenen Hauptvertrag und den zugehörigen Leistungsbeschreibungen konkretisiert sind. Die Einzelheiten zu den Arten der verarbeiteten Daten sowie die Datenkategorien ergeben sich aus Anlage 1.

§ 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 DSGVO).

(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; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Ausgenommen hiervon sind Sachverhalte, in denen der Auftragnehmer zu einer weiteren Verarbeitung durch das Recht der Europäischen Union oder des Mitgliedstaats, dem er unterliegt, verpflichtet 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, welches er durch Einzelweisungen konkretisieren kann.

(2) Weisungen des Auftraggebers an den Auftragnehmer sind zu dokumentieren. Die Textform (§ 126b BGB) ist hierfür ausreichend.

§ 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 DSGVO, insbesondere Kapitel 5 Art. 44-50 DSGVO, und weist dies auf Verlangen nach.

(2) 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 wird, 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 DSGVO 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 2 zu diesem Vertrag.

(3) Der Auftragnehmer selbst führt für die Verarbeitung ein Verzeichnis der bei ihm stattfindenden Verarbeitungstätigkeiten im Sinne des Art. 30 DSGVO. Er stellt auf Anforderung dem Auftraggeber die für die Übersicht nach Art. 30 DSGVO notwendigen Angaben 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) PROJEKT PRO GmbH hat einen Datenschutzbeauftragten bestellt. Dieser ist unter datenschutz@projektpro.com erreichbar. Der Auftragnehmer gewährleistet, dass die Anforderungen an den Datenschutzbeauftragten und seine Tätigkeit gemäß Art. 38 DSGVO erfüllt werden.

(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 DSGVO.

(7) Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Betroffenenanfragen wie der 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 so lange 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 DSGVO 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 DSGVO 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 Datensicherheits-maßnahmen des Auftragnehmers vertraulich zu behandeln.

(7) Der Auftraggeber stellt sicher, dass die aus Art. 32 DSGVO 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 DSGVO 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

(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) 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.

(6) 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 darf zur Erbringung der vertraglich vereinbarten Leistungen Unterauftragnehmer (Subdienstleister) einsetzen. Der Auftraggeber erteilt seine Zustimmung zu den bereits eingesetzten Unterauftragnehmern. Eine Übersicht der aktuell eingesetzten Unterauftragsnehmern ist unter: www.projektpro.com/impressum#avv zu finden.

(2) Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine Genehmigung zum Einsatz weiterer oder zur Ersetzung bestehender Unterauftragnehmer. Der Auftragnehmer informiert den Auftraggeber mindestens 14 Tage vor der geplanten Beauftragung über jede beabsichtigte Änderung (Hinzunahme oder Austausch eines Unterauftragnehmers).

(3) Der Auftraggeber kann der Änderung aus wichtigem Grund widersprechen, insbesondere wenn: der neue Unterauftragnehmer die Anforderungen an Datenschutz und Datensicherheit offensichtlich nicht erfüllt oder berechtigte Zweifel an der Zuverlässigkeit oder Eignung bestehen.

(4) Erfolgt innerhalb von 14 Tagen nach Mitteilung kein Widerspruch, gilt die Zustimmung des Auftraggebers als erteilt.

(5) Übt der Auftraggeber sein Widerspruchsrecht aus, kann er den Vertrag aus wichtigem Grund mit angemessener Frist kündigen, sofern keine einvernehmliche Lösung gefunden wird.

(6) Der Auftragnehmer stellt sicher, dass jeder Unterauftragnehmer mindestens denselben Datenschutz- und Datensicherheitsanforderungen unterliegt wie der Auftragnehmer selbst. Dies umfasst insbesondere die in diesem Vertrag festgelegten Pflichten, die Anforderungen des Art. 28 DSGVO sowie die Umsetzung angemessener technischer und organisatorischer Maßnahmen gemäß Art. 32 DSGVO, die dem Risiko der jeweiligen Verarbeitung angemessen sind.

(7) Der Auftragnehmer bleibt für die Erfüllung der Pflichten der Unterauftragnehmer gegenüber dem Auftraggeber verantwortlich.

§ 11 Haftung

(1) Auftraggeber und Auftragnehmer haften für den Schaden, der durch eine nicht der DSGVO 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 DSGVO 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 seinen ihm speziell durch die DSGVO auferlegten Pflichten nicht nachgekommen ist oderunter

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) Änderungen und Ergänzungen dieses Vertrags erfolgen in Textform (§ 126b BGB). Die Textform kann auch durch elektronische Zustimmung, z. B. per Klick im Administrationsbereich der Software, erfüllt werden. Dies gilt ebenso für die Aufhebung dieser Formvorgabe.

(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.

(5) Diese Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO ersetzt alle zuvor geschlossenen Vereinbarungen zur Auftragsverarbeitung.

Anlage 1

ARTEN UND KATEGORIEN DER DATEN

§ 1 Gegenstand des Auftrages

(1) Gegenstand dieses Auftrags ist die Verarbeitung personenbezogener Daten des Auftraggebers im Rahmen der Bereitstellung und Nutzung der Softwarelösung von PROJEKT PRO GmbH für Architektur- und Ingenieurbüros.

(2) Im Zusammenhang mit der Erfüllung der vertraglichen Pflichten aus dem zwischen den Parteien bestehenden Hauptauftrag. Als Hauptauftrag gilt entweder

- ein zwischen den Parteien geschlossener Subscriptionsvertrag,
- oder ein zwischen den Parteien geschlossener Support-/Pflegevertrag,

je nachdem, welcher der Verträge abgeschlossen wurde. Die nachfolgenden Bestimmungen zur Art und zum Umfang der Datenverarbeitung beziehen sich jeweils nur auf den konkret bestehenden Vertrag.

(3) Im Rahmen eines Subscriptionsvertrags stellt der Dienstleister eine umfassende Softwarelösung für Architekt:innen und Ingenieur:innen zur Verfügung, die sämtliche Anforderungen im Bereich der Projektplanung, -entwurfs und -kalkulation abdeckt. Die Lösung basiert auf einem cloud- oder hybridbasierten Bereitstellungsmodell: Je nach individueller Auswahl des Auftraggebers werden bestimmte Module entweder beim Auftraggeber (on-premise) betrieben oder durch den Auftragnehmer gehostet.

(4) Sofern zusätzlich ein Support-/Pflegevertrag abgeschlossen wurde, beinhaltet dieser insbesondere die Installation und Betreuung eines Servers beim Auftraggeber. Der Auftragnehmer erhält ausschließlich zu Supportzwecken Zugriff auf das System, um Wartungs- und Unterstützungsleistungen erbringen zu können. Auch hierbei erfolgt die Verarbeitung personenbezogener Daten ausschließlich im Rahmen der vertraglich vereinbarten Leistungen.

(5) Die Softeware dient dem projektbezogenen Controlling sowie dem operativen Management und untersützt insbesondere die folgenden Aufgaben:

Controlling

- Projektplanung und -verfolgung
- Zeiterfassung und Projektabrechnung
- Analyse von Projektkennzahlen
- Dokumentation arbeitszeitbezogener Abwesenheiten (z.B. Urlaubstage)
- Auswertung und Management von Ausgaben, Liquidität und Ressourcen
- Angebots- und Auftragsverwaltung
- Verwaltung von Mitarbeitenden im Kontext projektbezogener Daten

Management

- Kommunikation und Verwaltung von E-Mails (über IMAP-Schnittstelle)
- Projektbezogene Aufgabensteuerung, Dokumentation und operative Maßnahmen
- Planung und Dokumentation von Aktionen im Projektalltag

Basic

- Pflege von Kontaktdaten (Benutzer, Kunden, Lieferanten, Auftraggeber, Projektbeteiligte)
- Tägliche Aufgabenverwaltung („Daily Actions")
- Interne Mitteilungen über das digitale Schwarze Brett („Noticeboard")

§ 2 Kategorien betroffener Personen und personenbezogener Daten

(1) Je nach gebuchter Lizenz und freigeschalteten Modulen werden personenbezogene Daten folgender Kategorien von betroffenen Personen verarbeitet:

Mitarbeiter des Auftraggebers (Architektur-/Ingenieurbüro)

Verarbeitet werden insbesondere:

- Vor- und Nachname
- E-Mail-Adresse, Telefonnummer
- Jubiläen und Geburtstage
- Arbeitszeitdaten (Zeiterfassung, Projektzeiten, Zeitkonto)

- Abwesenheiten (Urlaub, projektrelevante Krankheitstage ohne Angabe der Diagnose)
- Zugeordnete Projekte, Rollen, Stundensätze
- Benutzerkennungen und Zugriffsrechte
- Kommunikation über integrierte E-Mail-Funktion (IMAP-Client)

Besondere Kategorien (Art. 9 DSGVO):

Es kann dokumentiert werden, dass eine Abwesenheit krankheitsbedingt ist (z.B. "Krankheit" als Auswahlgrund).

Kunden des Auftraggebers (z.B. Projektpartner, Bauherren)

Verarbeitet werden insbesondere:

- Vor- und Nachname von Ansprechpartnern
- E-Mail-Adresse, Telefonnummer
- Projektbezogene Informationen (z.B. Angebots- oder Rechnungsdaten)
- Kontakthistorie und Kommunikationsdaten
- Jubiläen und Geburtstage
- Zuweisung zu Projekten und Aktionen

Lieferanten und Dienstleister des Auftraggebers

Verarbeitet werden insbesondere:

- Vor- und Nachname von Ansprechpartnern
- E-Mail-Adresse, Telefonnummer
- Informationen zu Lieferungen, Leistungen, Abrechnungsdaten
- Projektbezogene Zuordnungen

(2) Die Software ist modular aufgebaut. Die konkret verarbeiteten Daten hängen von der jeweiligen Lizenzart und den genutzten Funktionen ab. Je nach Lizenz können nur Teilbereiche der genannten Datenverarbeitung stattfinden.

Anlage 2

UMSETZUNG TECHNISCHER UND ORGANISATORISCHER MASSNAHMEN BEIM AUFTRAGNEHMER

Die hier dargestellten Technisch und Organisatorischen Maßnahmen (TOM) bilden die hausintern umgesetzten Schutzmaßnahmen des Unternehmens ab. Diese internen Maßnahmen werden durch den gezielten Einsatz externer Subdienstleister (z.B. im Bereich Hosting oder Rechenzentrum) ergänzt und gestärkt. Dabei werden die deren TOM im Rahmen des Datenschutz- und Informationssicherheitsmanagements berücksichtigt.

Organisatorische Maßnahmen

1. Leitlinien & Zuständigkeiten

· Datenschutz- und Informationssicherheitsleitlinie sind vorhanden und allen Mitarbeitenden bekannt.

· Thematische Richtlinien regeln adressatengerecht spezifische Anforderungen und werden den Mitarbeitenden bedarfsgerecht zur Verfügung gestellt.

· Mitarbeitende werden zur Einhaltung aller Datenschutz- und Sicherheitsvorgaben verpflichtet.

· Aufgaben und Zuständigkeiten im Bereich Datenschutz und Informationssicherheit sind definiert.

· Zuständige Behörden (z.B. Datenschutzaufsicht) sind identifiziert, Kontaktinformationen dokumentiert, feste Ansprechpersonen benannt.

2. Informationssicherheitsmanagement

· Gefährdungen der Daten- und Informationssicherheit werden erfasst, analysiert und bewertet (z.B. durch Monitoring).

· Relevante Sicherheitsanforderungen werden projektbezogen berücksichtigt (Einbindung in Projektmanagement).

· Ein Inventar von Informationswerten und zugehörigen Verantwortlichkeiten wird zentral gepflegt.

3. Datenklassifikation & Umgang mit Informationen

· Datenklassifikation legt Schutzbedarf (Vertraulichkeit, Integrität, Verfügbarkeit) fest und bestimmt den Umgang mit Informationen.

· Vorgaben für Erhebung, Verarbeitung, Speicherung und Übermittlung klassifizierter Daten sind dokumentiert.

· Mitarbeitende werden zur Behandlung unterschiedlicher Schutzklassen sensibilisiert.

4. Zugriffs- und Identitätsmanagement

· Physische und logische Zugriffskontrollen sind umgesetzt:

  o Zugriff erfolgt nach dem Need-to-know- und Least-Privilege Prinzip.

  o Physischer Schutz sensibler Bereiche durch Zugangskontrollmaßnahmen.

  o Logische Zugriffe über personenbezogene Konten, sichere Authentifizierung und rollenbasierte Berechtigungen.

· Identitätsmanagement ist zentral organisiert:

  o Keine Sammelkonten (eindeutige Zuordnung zu Personen).

  o Kontenerstellung, Änderungen und Löschung erfolgen kontrolliert bei Eintritt, Rollenwechsel oder Austritt.

· Zugriffsrechte werden im Rahmen des Onboarding-Prozesses vergeben:

  o Rollenbasiert und nach dem Prinzip der minimalen Rechtevergabe.

  o Zuständigkeiten für Beantragung, Freigabe und Umsetzung sind klar geregelt.

  o Rechte werden bei Rollenwechsel oder Austritt zeitnah angepasst oder entzogen.

5. Sicherer Einsatz externer Dienste (Lieferanten & Cloud)

· Risiken bei der Nutzung externer Produkte und Dienste (z.B. Cloud, Tools) werden durch Prozesse gesteuert:

  o Lieferantenmanagementprozess stellt sicherheitsrelevante Anforderungen sicher.

  o Anforderungen an Informationssicherheit werden je nach Lieferantenbeziehung festgelegt und vertraglich vereinbart.

  o Lieferanten-TOM werden schutzbedarfsgerecht geprüft, Sicherheitspraktiken regelmäßig bewertet.

· Nutzung von Clouddiensten ist geregelt (IT-Tools, Entwicklung):

  o Sicherheits- und Risikoanalyse erfolgt vor Einsatz neuer Dienste.

  o Verantwortlichkeiten für Auswahl, Nutzung und Überwachung sind festgelegt.

  o Einsatz erfolgt auf Basis zentraler Sicherheitsvorgaben.

6. Management von Informationssicherheitsvorfällen

· Richtlinie zum Umgang mit Datenschutzverletzungen ist vorhanden.

· Rollen, Zuständigkeiten und Meldewege sind klar definiert.

· Risikobewertung, Dokumentation und Maßnahmen zur Vorbeugung sind Bestandteil des Prozesses.

· Erkenntnisse aus Vorfällen fließen in die Weiterentwicklung der Sicherheitsmaßnahmen ein.

7. Verfügbarkeit und Wiederherstellung

· Maßnahmen zur raschen Wiederherstellung der Verfügbarkeit sind umgesetzt.

· Dazu zählen regelmäßige Backups, Ausfallsicherungen und Maßnahmen zur Notfallbewältigung.

8. Datenschutz und rechtliche Anforderungen

· Gesetzliche, behördliche und vertragliche Anforderungen im Bereich Informationssicherheit und Datenschutz werden berücksichtigt und umgesetzt.

· Prozesse zur Wahrung der Betroffenenrechte und zum Umgang mit personenbezogenen Daten sind etabliert.

· Die Umsetzung der Informationssicherheitsmaßnahmen und die Einhaltung relevanter Richtlinien, Regeln und Standards werden regelmäßig überprüft.

· Die Prüfungen erfolgen unabhängig, unter Einbindung des externen Datenschutzbeauftragten.

· Ergebnisse fließen in die kontinuierliche Verbesserung der Sicherheitsmaßnahmen ein.

Personelle Maßnahmen

1. Vertraulichkeit und arbeitsvertragliche Verpflichtung

· Arbeitsverträge enthalten Klauseln zur Vertraulichkeit und zur Wahrung der Informationssicherheit.

· Vertraulichkeits- bzw. Geheimhaltungsklauseln sind vertraglich für interne und externe Mitarbeitende geregelt.

· Mitarbeitende werden auf ihre Pflichten zur Informationssicherheit und zum Datenschutz verpflichtet.

2. Sensibilisierung und Schulung

- Mitarbeitende und relevante Dritte werden im Rahmen des Onboarding-Prozesses zu Datenschutz und Informationssicherheit geschult.
- Regelmäßige Wiederholungsschulungen sind vorgesehen.
- Ein Schulungskonzept legt Inhalte, Zielgruppen und Formate fest.
- Personen mit erhöhtem Informationssicherheitsbezug erhalten vertiefende Schulungen oder Awarenessmaßnahmen.
- Schulungen sensibilisieren auch für den richtigen Umgang mit Datenschutzverletzungen und Betroffenenrechten.

3. Meldung von Informationssicherheitsereignissen

- Mitarbeitende können beobachtete oder vermutete Informationssicherheitsereignisse über interne Meldewege an den Datenschutzkoordinator melden.
- Die Meldewege sind in der entsprechenden Richtlinie dokumentiert und bekannt gemacht.

4. Disziplinarmaßnahmen bei Verstößen

- Verstöße gegen Vertraulichkeit und Geheimhaltung sind arbeitsvertraglich geregelt.
- Die arbeitsvertragliche Regelung ermöglicht disziplinarische Maßnahmen bei Pflichtverletzungen im Umgang mit vertraulichen Informationen.

5. Pflichten bei Beschäftigungsende (Offboarding)

- Vertraulichkeitsverpflichtungen gelten vertraglich über das Beschäftigungsende hinaus.
- Die Rückgabe firmeneigener Werte erfolgt über einen geregelten Offboarding-Prozess.
- Eine Offboarding-Checkliste stellt sicher, dass Zugriffe entzogen und Assets vollständig zurückgegeben werden.

6. Sicheres Arbeiten außerhalb der Organisation

- Mitarbeitende erhalten Zugriff auf Informationen außerhalb der Organisation nur über gesicherte Verbindungen.
- Der Zugriff erfolgt ausschließlich über VPN in Kombination mit Zwei-Faktor-Authentifizierung (2FA).
- So wird die Vertraulichkeit und Integrität der Daten bei externem Zugriff sichergestellt.

Physische Maßnahmen

1. Sicherheitszonen und Zutrittskontrolle

· Bereiche mit schützenswerten Informationen oder Systemen (z.B. Serverraum, Archiv, Bürozugang) sind als Sicherheitszonen definiert.

· Sicherheitszonen sind durch bauliche oder technische Maßnahmen geschützt (z.B. abschließbare Türen, Fensterverriegelungen, Tür- und Schrankschlösser).

· Zutritt ist auf autorisierte Personen beschränkt.

· Berechtigungen werden regelmäßig überprüft und bei Bedarf angepasst.

· Zutrittspunkte sind auf das notwendige Maß begrenzt und technisch gesichert.

· Besucher werden in sicherheitsrelevanten Bereichen durch autorisierte Mitarbeitende begleitet.

· Räume mit sensiblen Informationen oder Systemen werden außerhalb der Servicezeiten zusätzlich abgesperrt.

2. Schutz von Büroräumen und Arbeitsbereichen

· Büros, Arbeitsbereiche und Einrichtungen sind durch geeignete physische Maßnahmen geschützt.

· Zutritt zu sensiblen Bereichen ist eingeschränkt und nur mit Berechtigung möglich.

· Der Zugang zu Büroräumen ist ausschließlich mit einem Schlüssel möglich.

· Sicherheitsmaßnahmen werden regelmäßig überprüft und bei Bedarf angepasst.

3. Schutz vor physischen und umgebungsbezogenen Gefährdungen

· Maßnahmen zum Schutz vor physischen Bedrohungen (z.B. Brand) sind umgesetzt.

· Brandschutz ist baulich berücksichtigt.

· Brandschutzhelfer sind benannt und entsprechend geschult.

4. Clean Desk & Gerätesperre

· Am Arbeitsplatz gelten verbindliche Regeln zum „Clean Desk" und zur Gerätesperre.

· Vertrauliche Papiere und mobile Speichermedien werden außerhalb der Arbeitszeiten sicher verwahrt.

· Bildschirme und Geräte sind bei Verlassen des Arbeitsplatzes zu sperren.

· Die Vorgaben sind in einer internen Richtlinie dokumentiert und den Mitarbeitenden bekannt.

· Die Einhaltung wird stichprobenartig durch die IT kontrolliert und bei Bedarf nachgeschärft.

5. Betriebsmittel und Geräte

· Betriebsmittel werden so aufgestellt, dass unbefugter Zugriff, Diebstahl oder unbeabsichtigte Schäden vermieden werden.

· Die Platzierung berücksichtigt Sicherheitsaspekte und Anforderungen an das Betriebsumfeld.

6. Schutz von Assets außerhalb der Organisation

· IT-Geräte und andere Assets, die im Homeoffice oder auf Reisen genutzt werden, sind durch geeignete Maßnahmen geschützt (z. B. verschlüsselte Festplatten, VPN, Gerätesperre).

· Mitarbeitende sind über den sicheren Umgang mit Geräten und Daten außerhalb der Organisation informiert.

· Verlust oder Diebstahl ist umgehend zu melden.

· Die Verantwortung für den Schutz liegt auch außerhalb der Betriebsstätte beim jeweiligen Nutzer.

7. Speichermedienmanagement

· Speichermedien werden über ihren gesamten Lebenszyklus hinweg sicher verwaltet.

· Die Handhabung erfolgt gemäß dem internen Klassifizierungsschema und den definierten Schutzanforderungen.

· Schutzmaßnahmen gelten insbesondere für Speicherung, Transport, Weitergabe und sichere Löschung von Datenträgern.

8. Schutz vor Versorgungsstörungen

· Informationsverarbeitende Systeme sind durch unterbrechungsfreie Stromversorgung (USV) gegen Stromausfälle und Spannungsstörungen geschützt.

· So wird die Verfügbarkeit und Integrität der Systeme auch bei kurzfristigen Ausfällen sichergestellt.

9. Schutz von Kabeln und Leitungen

· Kabel für Stromversorgung, Datenübertragung und Netzwerkverbindungen sind vor Abhören, Manipulation und Beschädigung geschützt.

· Die Verlegung erfolgt so, dass physischer Zugriff erschwert und versehentliche Beschädigungen vermieden werden.

Technische Maßnahmen

1. Zugriffsschutz & Authentifizierung

· Rollenbasiertes Berechtigungskonzept mit Zugriffsprofilen je Modul.

· Trennung administrativer und regulärer Benutzerrechte.

· Der Zugriff auf Systeme und Informationen erfolgt rollenbasiert und über gesicherte Verbindungen (VPN).

· Sichere Authentifizierung wird durch Passwortmanager, komplexe Passwortregeln, Schlüsselbund und VPN-Zugangsschutz gewährleistet.

· Gäste-WLAN ist strikt vom internen Netz getrennt.

· Zugänge mit privilegierten Rechten werden zentral über Bitwarden verwaltet (rollenbasiert).

· Sicherheitsgruppen im Domain Controller (DC) trennen Dienste, Nutzer und Systeme voneinander.

2. Gerätesicherheit & Endpoint Protection

· Anwender-Endgeräte sind durch FileVault-Verschlüsselung, Passwortmanager, Virenschutz und MDM-Richtlinien abgesichert.

· Schutz vor Schadsoftware erfolgt durch Virenscanner, automatische Updates und Awareness zu E-Mail-Anhängen.

· Maßnahmen zur Vermeidung von Datenabfluss: Verbot von USB-Sticks, Device Control über TrendMicro, Netzwerksegmentierung.

3. Verschlüsselung & Kryptographie

· FileVault-Festplattenverschlüsselung schützt gespeicherte Daten (auch als Datenmaskierung).

· Kommunikation wird durch SSL-Zertifikate mit zentraler Verwaltung und jährlichem Austausch gesichert.

4. Netzwerk- und Systemschutz

· Netzwerke sind segmentiert in LAN, Server, Client, WLAN, DMZ.

- Netzdienste werden durch Webfilter und Firewall kontrolliert.
- Zugriff auf externe Webseiten wird durch Firewall/Webfilter eingeschränkt.
- Logs zu Aktivitäten und Fehlern werden durch TrendMicro gespeichert und ausgewertet.
- Anomalien werden über Firewall-Logs erkannt.
- Systemzeiten sind über Windows Server und Apple-Zeitquellen synchronisiert.
- Ressourcenüberwachung erfolgt durch Server-Hardening und regelmäßige Sicherheitsscans/Penetrationstests.
- Technische Schwachstellen werden regelmäßig mit OpenVAS gescannt und bewertet.
- Sicherheitskonfigurationen von Hardware, Software und Netzwerken sind dokumentiert, umgesetzt und werden durch Firewall-Updates gepflegt.
- Informationsverarbeitende Systeme sind ohne Hochverfügbarkeitsarchitektur, aber grundsätzlich abgesichert.

5. Software-Management & Installation

- Die Installation von Software wird durch die IT zentral gesteuert.
- Änderungen an Systemen und Anwendungen durchlaufen einen einfachen Change-Management-Prozess (MS Planner).

6. Backup & Datenlöschung

- Regelmäßige Backups sichern Systeme, Software und Daten gemäß Backup-Richtlinie.
- Daten werden nach Ausscheiden oder Nichtnutzung mittels Datei-Shredder sicher gelöscht.

7. Softwareentwicklung & Secure Coding

- Sichere Entwicklung ist in den Produktmanagement-, Entwicklungs-, QA- und Releasing-Prozessen verankert.
- Sicherheitsanforderungen werden dokumentiert und über Stories/Epics definiert.
- Sicherheitstests erfolgen automatisiert (Cloud) oder intern (z.B. FileMaker-Systeme).
- Sichere Programmierung ist Teil der Entwicklungsstandards.
- Grundsätze sicherer Entwicklung sind teilweise dokumentiert; Umsetzung durch erfahrenes Fachpersonal und moderne Sicherheitstools.

· Entwicklungs-, Test- und Produktivsysteme sind getrennt und gesichert.

· Externe Entwickler sind vollständig in Prozesse, Tools und Teams integriert.

8. Testdatenmanagement

· Testdaten werden mit Kundenerlaubnis verwendet, verschlüsselt gespeichert und sicher übertragen.

· Anonymisierung erfolgt nicht, regelmäßige Löschung erfolgt nicht systematisch.

· Eine regelmäßige Prüfung des Testdaten-Umgangs findet derzeit nicht statt.