Zwischen

_____

_____

_____

- Auftraggeber -

und

Volker Baron
Baron Consult EDV-Beratung und -Service
Haydnstraße 2
80336 München
- Auftragnehmer -

wird folgende Datenschutzvereinbarung für die Wartung und Pflege von IT-Systemen getroffen.

❑ Zwischen den Parteien besteht ein Vertragsverhältnis über die Wartung und Pflege von IT-Systemen mit Datum vom _____ .

❑ Diese Vereinbarung wird für künftige Beauftragungen des Auftragnehmers geschlossen.

Sie stellt eine ergänzende Regelung zur Einhaltung der datenschutzrechtlichen Vorgaben insbesondere nach Art. 28 der EU-DSGVO und § 62 BDSG (neu) dar.

Präambel

Der Auftragnehmer führt im Auftrag des Auftraggebers Wartungs- und/oder Pflegearbeiten an IT-Systemen des Auftraggebers durch. In diesem Zusammenhang ist nicht ausgeschlossen, dass der Auftragnehmer personenbezogene Daten verarbeitet, um die Wartung und Pflege von IT-Systemen durchzuführen oder durchführen zu können.

...

1. Laufzeit der Vereinbarung

Der Auftragnehmer führt für den Auftraggeber Leistungen (Wartung und/oder Pflege von IT-Systemen) durch. Zwischen den Parteien besteht diesbezüglich ein Vertragsverhältnis („Hauptvertrag“), das entweder auf individuellen vertraglichen Vereinbarungen, allgemeinen Geschäftsbedingungen oder auf gesetzlichen Regelungen (z. B. BGB) basiert.

Bei einem bestehenden Vertragsverhältnis (Hauptvertrag) gilt diese Vereinbarung ab Unterzeichnung durch beide Parteien für die Dauer des jeweiligen Hauptvertrages.

Bezieht sich diese Vereinbarung auf Einzelbeauftragungen, ohne dass ein dauerhaftes Vertragsverhältnis besteht, so gilt sie auch für alle künftigen Beauftragungen, bis sie von einer der Vertragsparteien gekündigt wird.

Ein außerordentliches Kündigungsrecht jeder Partei bleibt unberührt.

2. Gegenstand des Auftrags

Bezieht sich die Vereinbarung auf einen Hauptvertrag, so wird der Gegenstand des Auftrags durch diesen festgelegt.

Bezieht sich die Vereinbarung auf Einzelbeauftragungen, so wird der Gegenstand der Beauftragung darin festgelegt.

3. Kategorien von Betroffenen

Bei den Betroffenen kann es sich um folgende Personengruppen handeln:

Beschäftigte des Auftraggebers
Kunden des Auftraggebers
Lieferanten des Auftraggebers

weitere: _____

4. Ort der Datenverarbeitung

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. EU-DSGVO erfüllt sind.

...

5. Technisch-organisatorische Maßnahmen

Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 c, 32 EU-DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 EU-DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 EU-DSGVO zu berücksichtigen [Einzelheiten in Anlage TOM].

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

6. Berichtigung, Einschränkung und Löschung von Daten

Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

7. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 EU-DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

...

a) Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird benannt:

   Volker Baron
   Haydnstraße 2
   80336 München
   E-Mail: volker.baron@baron-consult.de

b) Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 b, 29, 32 Abs. 4 EU-DSGVO: Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 c, 32 EU-DSGVO [Einzelheiten in Anlage TOM].
d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
e) Unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer bei Geltendmachung seiner Rechte zu unterstützen. Der Auftragnehmer erhält hierfür eine Vergütung entsprechend den entstandenen Aufwendungen.
g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
j) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

8. Unterauftragsverhältnisse

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post- / Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

...

Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Zur Vertragserfüllung bedient sich der Auftragnehmer folgender Unterauftragsverhältnisse:

- keine -

Der Auftragnehmer darf weitere Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

Der Wechsel des bestehenden Unterauftragnehmers ist zulässig, soweit
- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 EU-DSGVO zugrunde gelegt wird.

Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

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

9. Kontrollrechte des Auftraggebers

Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 EU-DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

10. Fernwartung

Sofern der Auftragnehmer die Wartung und/oder Pflege der IT-Systeme auch im Wege der Fernwartung durchführt, ist der Auftragnehmer verpflichtet, dem Auftraggeber eine wirksame Kontrolle der Fernwartungsarbeiten zu ermöglichen. Dies kann z. B. durch Einsatz einer Technologie erfolgen, die dem Auftraggeber ermöglicht, die vom Auftragnehmer durchgeführten Arbeiten auf einem Monitor o. ä. Gerät zu verfolgen.

Für den Fall, dass der Auftraggeber einer Berufsgeheimnispflicht i. S. d. § 203 StGB unterliegt, hat dieser Sorge dafür zu tragen, dass eine unbefugte Offenbarung urch die Fernwartung nicht erfolgt. Der Auftragnehmer ist diesbezüglich verpflichtet, Technologien einzusetzen, die nicht nur ein Verfolgen der Tätigkeit auf dem Bildschirm ermöglicht, sondern dem Auftraggeber auch eine Möglichkeit gibt, die Fernwartungsarbeiten jederzeit zu unterbinden.

Wenn der Auftraggeber bei Fernwartungsarbeiten nicht wünscht, die Tätigkeiten an einem Monitor o. ä. Gerät zu beobachten, wird der Auftragnehmer die von ihm durchgeführten Arbeiten in geeigneter Weise dokumentieren.

11. Mitteilung bei Verstößen des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 EU-DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u. a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen
b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden
c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen
d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung
e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

12. Weisungsbefugnis des Auftraggebers

Mündliche Weisungen bestätigt der Auftraggeber unverzüglich mindestens in Textform.

...

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

13. Löschung und Rückgabe von personenbezogenen Daten

Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

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.

_____, den _____ München, den _____

_____ _____

Unterschrift Auftraggeber Unterschrift Auftragnehmer

Anlage – Technisch-organisatorische Maßnahmen (TOM)

1. Vertraulichkeit (Art. 32 Abs. 1 b EU-DSGVO)

Zutrittskontrolle	Der Auftragnehmer hat seine Büro- und Geschäftsräume grundsätzlich außerhalb der Büro- und Geschäftszeiten geschlossen zu halten. Während der Büro- und Geschäftszeiten ist sichergestellt, dass Besucher oder sonstige Dritte sich nicht alleine in Räumen bewegen können, in denen sie Zugang zu personenbezogenen Daten erhalten könnten. Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt. Videoüberwachung im Eingangsbereich.
Zugangskontrolle	Um Zugang zu IT-Systemen zu erhalten, müssen der Auftragnehmer und seine Beschäftigten über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen vom Administrator vergeben. Remote-Zugriffe auf IT-Systeme des Auftragnehmers erfolgen stets über verschlüsselte Verbindungen. Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, wobei das Passwort auf Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss. Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen. Passwörter, die der Auftragnehmer vom Auftraggeber erhält oder für dessen IT-Systeme verwendet, werden grundsätzlich verschlüsselt gespeichert und sind nur den Beschäftigten zugänglich zu machen, die konkret mit der Erbringung von Leistungen für den Auftraggeber betraut sind.
Zugriffskontrolle	Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems (Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte)
Trennungskontrolle	Soweit der Auftragnehmer personenbezogene Daten vom Auftraggeber im Zusammenhang mit der Auftragsverarbeitung erhält, wird er diese getrennt von Daten anderer Kunden verarbeiten.
Pseudonymisierung (Art. 32 Abs. 1 a EU-DSGVO; Art. 25 Abs. 1 EU-DSGVO)	Ein administrativer Zugriff auf IT-Systeme des Auftraggebers erfolgt grundsätzlich über verschlüsselte Verbindungen, soweit dieser nicht innerhalb der Räumlichkeiten des Auftraggebers erfolgt.

2. Integrität (Art. 32 Abs. 1 b EU-DSGVO)

Weitergabekontrolle	Eine Weitergabe von personenbezogenen Daten, die im Auftrag des Auftraggebers erfolgt, darf jeweils nur in dem Umfang erfolgen, wie und soweit dies mit dem Auftraggeber abgestimmt ist. Die Nutzung von privaten Datenträgern ist dem Auftragnehmer im Zusammenhang mit der Auftragsverarbeitung für den Auftraggeber untersagt.
Eingabekontrolle	Der Auftragnehmer wird Eingaben, Änderungen oder Löschungen von personenbezogenen Daten, die er im Auftrag des Auftraggebers durchführt, in geeigneter Weise dokumentieren, sofern nicht sichergestellt ist, dass das jeweilige IT-System selbst eine Protokollierung entsprechender Aktivitäten durchführt.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 b EU-DSGVO)

Verfügbarkeitskontrolle	Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust (Backup-Strategie, unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Notfallpläne)
Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 c EU-DSGVO)	Soweit der Auftragnehmer personenbezogene Daten oder Zugangsdaten für den Auftraggeber speichert oder verwaltet, trägt er Sorge dafür, dass diese Daten mindestens täglich inkrementell und wöchentlich „voll“ gesichert werden. Es gibt ein Datensicherungskonzept, dass auch das erfolgreiche Testen der Wiederherstellung von Daten beinhaltet.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 d EU-DSGVO; Art. 25 Abs. 1 EU-DSGVO)

Der Auftragnehmer trägt durch Richtlinien und/oder Anweisungen an die Beschäftigten dazu bei, dass eine Verarbeitung personenbezogener Daten in einer Weise gewährleistet ist, die den Anforderungen der DSGVO entspricht. Dies beinhaltet insbesondere eine regelmäßige Überprüfung der Wirksamkeit der getroffenen Maßnahmen zum Schutz personenbezogener Daten und ggf. der Anpassung.

Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Beschäftigten erkannt und unverzüglich dem Auftraggeber gemeldet werden, wenn dies Daten betrifft, die im Rahmen der Auftragsverarbeitung für den Auftraggeber verarbeitet werden.

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 EU-DSGVO) werden nicht durch solche minderer Sicherheit ersetzt.

Auftragskontrolle	Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben des jeweils anzuwendenden Datenschutzrechts ein Auftragsverarbeitungsvertrag abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert. Die Auftragsverarbeitung im Sinne von Art. 28 EU-DSGVO erfolgt ausschließlich nach entsprechender Weisung des Auftraggebers.