

**Vereinbarung zur Auftragsverarbeitung
gemäß Art. 28 DS-GVO
zwischen**

**München Klinik gGmbH, Thalkirchner Str. 48, 80337 München
(im Folgenden „Auftraggeber“)
und**

**[Name des Auftragnehmers, Adresse],
(im Folgenden „Auftragnehmer“)**

1. Gegenstand und Dauer des Auftrags

- (1) Der Auftragnehmer übernimmt Planungsleistungen für den Auftraggeber. Der Gegenstand des Auftrags ergibt sich im Einzelnen aus dem zwischen den Parteien abgeschlossenen Vertrag (nachfolgend „**Vertrag**“). Die vorliegende Vereinbarung findet Anwendung auf alle Verarbeitungen personenbezogener oder personenbeziehbarer Daten im Sinne der einschlägigen datenschutzrechtlichen Bestimmungen (nachfolgend „**Daten**“) durch den Auftragnehmer oder durch von dem Auftragnehmer beauftragte Dritte, die mit dem Vertrag in Zusammenhang stehen. Die Tätigkeiten des Auftragnehmers auf Grundlage dieser Vereinbarung werden durch die im Vertrag vereinbarte Vergütung abgegolten. Eine gesonderte Vergütung erfolgt nicht.
- (2) Die Dauer dieser Vereinbarung (Laufzeit) entspricht der Laufzeit des Vertrages. Bestimmte, gekennzeichnete Verpflichtungen dieser Vereinbarung überdauern dabei die Laufzeit des Vertrags (insb. Vertraulichkeitsregelungen).

2. Konkretisierung des Auftragsinhalts

- (1) Art und Zweck der vorgesehenen Verarbeitung der Daten:

Eine Verarbeitung von Daten erfolgt ausschließlich zur Durchführung der nach dem Vertrag vom Auftragnehmer geschuldeten baubetrieblichen Beratungsleistungen.

Der Auftragnehmer verpflichtet sich, die ihm im Verlauf oder anlässlich der Zusammenarbeit erhobenen Daten, bekannt gewordenen Betriebsgeheimnisse oder sonstige ihrer Natur nach schutzwürdigen Angelegenheiten nur zur rechtmäßigen

Aufgabenerfüllung im Sinn der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten sowie die Art der Daten und den Kreis der Betroffenen nur für vertragliche Zwecke zu verwenden und im Übrigen geheim zu halten. Dies gilt über das Vertragsende hinaus.

Der Auftragnehmer verwendet Daten, die ihm im Rahmen der vertraglichen Erfüllung bekannt geworden sind, nur für die vorgesehenen Zwecke. Kopien oder Duplikate dürfen ohne Wissen und Zustimmung des Auftraggebers nicht erstellt werden.

Auskünfte an Dritte darf der Auftragnehmer, außer in gesetzlich zwingend vorgesehenen Fällen, nicht erteilen.

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Personenstammdaten (Nachname, Vorname von Mitarbeitern des Auftraggebers; Position der Mitarbeiter beim Auftraggeber);
- Kontaktdaten/Kommunikationsdaten (z.B. Telefonnummer, E-Mail-Adresse, Fax-Nummer, Handy-Nummer, Geschäftsadresse von Mitarbeitern des Auftraggebers, von Bauunternehmen, Planungsbüros und Projektsteuerungsbüros (nachfolgend „**Unternehmen**“) sowie von im Zusammenhang mit der Leistungserbringung zusätzlich Beauftragten (dies können beispielsweise sein: Rechtsanwälte, Wirtschaftsprüfer, Steuerberater, Sachverständige sowie andere Berater));
- Vertragsstammdaten von Unternehmen;
- Zahlungsbedingungen / Rechnungsdaten von Unternehmen;
- Planungs- und Steuerungsdaten.

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Beschäftigte und Erfüllungsgehilfen des Auftraggebers;
- Ansprechpartner;
- Unternehmen;
- sonstige Vertragspartner des Auftraggebers.

3. Technische und organisatorische Maßnahmen

- (1) 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.
- (2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 DS-GVO zu berücksichtigen. Einzelheiten ergeben sich aus dem **Anhang** „Technische und organisatorische Maßnahmen“ zu dieser Vereinbarung zur Auftragsverarbeitung.
- (3) Die in dem **Anhang** zu dieser Auftragsverarbeitung festgehaltenen vereinbarten technischen und organisatorischen Maßnahmen berücksichtigen zum Zeitpunkt des Abschlusses dieser Vereinbarung den Stand der Technik und unterliegen während der Laufzeit der Vereinbarung dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der in dem **Anhang** festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind von dem Auftraggeber zu genehmigen und im Anschluss zu dokumentieren.

4. Weisung des Auftraggebers

- (1) Der Auftragnehmer darf die personenbezogenen Daten nur auf dokumentierte Weisung des Auftraggebers verarbeiten (vgl. Art. 28 Abs. 3 S. 2 lit. a DS-GVO), sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der

Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

- (2) Eine „**Weisung**“ ist jede an den Normadressaten gerichtete Anordnung, die sich auf den Gegenstand und die Art des Umgangs mit Daten und der darauf bezogenen technischen und organisatorischen Maßnahmen bezieht.
- (3) Mündliche Weisungen bestätigt der Auftraggeber schriftlich (mind. Textform).
- (4) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Auffassung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

5. Berichtigung, Löschung und Einschränkung der Verarbeitung

- (1) 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.
- (2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

6. Verschwiegenheitsverpflichtung

- (1) Der Auftragnehmer ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von personenbezogenen Daten, Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftraggebers vertraulich zu behandeln und hierüber Stillschweigen zu bewahren.
- (2) Die in dieser Ziffer 6 geregelte Pflicht zur Verschwiegenheit besteht auch nach Ende des Vertragsverhältnisses zeitlich unbeschränkt weiter fort.
- (3) Der Auftragnehmer ist verpflichtet, seine Beschäftigten und Erfüllungsgehilfen auf die Verschwiegenheit zu verpflichten und zu belehren. Hierzu hat der Auftragnehmer entsprechende Verpflichtungserklärungen von seinen Beschäftigten und Erfüllungsgehilfen einzuholen und dem Auftraggeber auf Verlangen nachzuweisen.

- (4) Soweit zwischen den Parteien eine Verschwiegenheitsvereinbarung im Vertrag (sofern vorhanden) oder an anderer Stelle bereits getroffen worden ist, gelten die Bestimmungen zur Verschwiegenheit aus dieser Ziffer 6 ergänzend zu jener Verschwiegenheitsvereinbarung. Im Falle eines Widerspruchs in Bezug auf einen bestimmten Lebenssachverhalt gilt für den Auftragnehmer die jeweils strengere Bestimmung.

7. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

- (1) ☐ Der Auftragnehmer hat einen Datenschutzbeauftragten schriftlich bestellt, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.
- ☐ Dessen Kontaktdaten werden dem Auftraggeber zum Zweck der direkten Kontaktaufnahme mitgeteilt. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt.
 - ☐ Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr/Frau *Vorname, Name, Organisationseinheit, Telefon, E-Mail* bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.
 - ☐ Dessen jeweils aktuelle Kontaktdaten sind auf der Homepage des Auftragnehmers leicht zugänglich hinterlegt.
- ☐ Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Als Ansprechpartner beim Auftragnehmer wird Herr/Frau *Vorname, Name, Organisationseinheit, Telefon, E-Mail* benannt.
- (2) Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:
- a) Die Wahrung der Vertraulichkeit bzw. der angemessenen Verschwiegenheitspflicht gemäß Art. 28 Abs. 3 S. 2 lit. b), 29 DS-GVO, Art. 32 Abs. 1 BayDSG herzustellen. Der Auftragnehmer wird darauf hingewiesen, dass die Verletzung personenbezogener Daten eine Ordnungswidrigkeit oder Straftat nach §§ 41, 42 des Bundesdatenschutzgesetzes (BDSG) bedeuten kann. Er ist verpflichtet, hierüber ebenfalls die von ihm Beschäftigten oder sonst vertraglich Verpflichteten zu belehren. Der Auftragnehmer setzt bei der Durchführung des Auftrags nur Beschäftigte ein, die auf die Vertraulichkeit bzw. Verschwiegenheit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz betraut gemacht wurden. Sie sind über die sich aus dieser Vereinbarung ergebenden

- besonderen Datenschutzpflichten zu informieren sowie über die bestehende Weisungs- bzw. Zweckbindung zu belehren. Dies ist schriftlich zu dokumentieren und dem Auftraggeber auf Verlangen durch Vorlage der unterzeichneten Vertraulichkeitsverpflichtungserklärungen nachzuweisen.
- b) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit c), 32 DS-GVO und Art. 32 BayDSG ist zu gewährleisten. Dies insbesondere, damit der Auftraggeber die Rechte der betroffenen Personen nach Kapitel III der DS-GVO innerhalb der gesetzlichen Fristen jederzeit erfüllen kann (vergl. Art. 28 Abs. 3 S. 2 lit e DS-GVO).
 - c) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
 - d) Der Auftragnehmer hat die Pflicht, den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde zu informieren, soweit sie sich auf diesen Auftrag beziehen (vergl. Art. 31, 51 ff. DS-GVO). 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 (vergl. Art. 83, 84 DS-GVO).
 - e) 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 nach besten Kräften zu unterstützen (vergl. Art. 28 Abs. 3 S. 2 lit f DS-GVO).
 - f) 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.
 - g) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 3 und 8 dieser Vereinbarung.
- (3) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO sowie Art. 13, 14, 32, 33, 36 BayDSG genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen 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 von Vorschriften zum Schutz personenbezogener Daten unverzüglich an den Auftraggeber zu melden,
- c) die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen unverzüglich zur Verfügung zu stellen,
- d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung,
- e) die Unterstützung des Auftraggebers bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der Rechte der betroffenen Personen,
- f) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

8. Unterauftragsverhältnisse

- (1) Die Einschaltung von Unterauftragnehmern, die für den Auftragnehmer unmittelbar Daten des Auftraggebers nutzen, ist dem Auftragnehmer nur nach schriftlicher Zustimmung des Auftraggebers gestattet. Für die im Angebot des Auftragnehmers benannten Unterauftragnehmer gilt die Zustimmung des Auftraggebers als erteilt.
- (2) Der Auftragnehmer ist verpflichtet, eine Liste mit allen Unterauftragnehmern zu führen, deren Einschaltung der Auftraggeber zugestimmt hat. Der Auftragnehmer hat diese Liste fortlaufend zu aktualisieren.
- (3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die Einhaltung der Voraussetzungen durch den Unterauftragnehmer wird vom Auftragnehmer regelmäßig überprüft.
- (4) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Auftraggebers (mind. Textform); sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

- (5) Bezüglich der Unterauftragnehmer sind dem Auftraggeber erforderliche Kontroll- und Überprüfungsrechte entsprechend Ziffer 11 dieser Vereinbarung einzuräumen.

9. Internationale Datentransfers

Die Datenverarbeitung findet ausschließlich in der Bundesrepublik Deutschland statt. Jede Übermittlung personenbezogener Daten in ein anderes Land ist unzulässig.

10. Kontrollrechte des Auftraggebers

- (1) Der Auftragnehmer räumt dem Auftraggeber Kontrollrechte nach Art. 28 Abs. 3 lit. S. 2 h DS-GVO nach Maßgabe dieser Ziffer 11 ein.
- (2) Der Auftragnehmer ermöglicht dem Auftraggeber, dessen Rechts- oder Fachaufsicht oder einem vom Auftraggeber beauftragten Prüfer, Kontrollen zu den üblichen Geschäftszeiten nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit gemeinsam mit dem Auftragnehmer durchzuführen. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit von ca. fünf Werktagen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer oder dem Unterauftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.
- (3) Der Auftragnehmer wird dem Auftraggeber auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte geben und die entsprechenden Nachweise verfügbar machen. Hierzu wird der Auftragnehmer dem Auftraggeber alle erforderlichen Informationen, insbesondere gegebenenfalls erstellte Protokolle, zum Nachweis der Einhaltung der Pflichten zur Verfügung stellen.
- (4) Aufgrund der Kontrollverpflichtung des Auftraggebers gemäß Art. 28 DS-GVO vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann.
- (5) Der Auftraggeber kann sich zu Prüfzwecken in den Betriebsstätten des Auftragnehmers zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und

organisatorischen Erfordernisse der für die Auftragsdatenverarbeitung einschlägigen Datenschutzgesetze überzeugen.

- (6) Der Auftraggeber ist berechtigt, die vorgenannten Kontrollen auch unter Hinzuziehung Dritter durchzuführen (insbesondere solcher, die gegenüber dem Auftraggeber zur Kontrolle berechtigt sind, wie z.B. Auftraggeber des Auftraggebers und Aufsichtsbehörden)
- (7) Der Auftragnehmer ist verpflichtet, die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO und Art. 32 BayDSG sowie die Durchführung der regelmäßig durchgeführten Risikobewertung nachzuweisen. Der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann dabei auch durch Vorlage eines aktuellen Testats oder von Berichten unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren) oder einer geeigneten Zertifizierung gemäß Art. 42 DS-GVO durch IT-Sicherheits- oder Datenschutzaudit erbracht werden.

11. Löschung oder Rückgabe von personenbezogenen Daten

- (1) 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.
- (2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Vertrages – 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, sofern keine gesetzlichen Speicherfristen vorliegen. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.
- (3) 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.

12. Haftung

- (1) Werden im Zusammenhang mit den unter diesen Vertrag fallenden Verarbeitungsvorgängen gegenüber einer Partei Schadenersatzansprüche i.S.v. Art. 82 DS-GVO, Geldbußen i.S.v. Art. 83 DS-GVO und/oder andere Sanktionen i.S.v. Art. 84 DS-GVO angedroht oder geltend gemacht, so informiert diese Partei die andere Partei hierüber unverzüglich in Textform. Auftraggeber und Auftragnehmer sind verpflichtet, sich bei der Abwehr solcher Ansprüche gegenseitig zu unterstützen.
- (2) Der Auftraggeber und der Auftragnehmer haften nach den einschlägigen Gesetzen.

13. Kündigung

- (1) Ergänzend zum Vertrag wird geregelt, dass ein schwerwiegender Verstoß des Auftragnehmers gegen gesetzliche oder vertragliche Datenschutzbestimmungen stets ein wichtiger Grund für den Auftraggeber ist, das im Vertrag vorbehaltene Recht zur außerordentlichen Kündigung auszuüben. In diesem Zusammenhang kann der Auftraggeber den Vertrag aus wichtigem Grunde ohne Einhaltung einer Frist kündigen.
- (2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in diesem Vertrag bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

14. Zurückbehaltungsrecht

Die Einrede des Zurückbehaltungsrechts, gleich aus welchem Rechtsgrund, an den vertragsgegenständlichen Daten sowie an vorhandenen Datenträgern wird ausgeschlossen.

Anhang zur Vereinbarung zur Auftragsverarbeitung – „Technische und organisatorische Maßnahmen“

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

Der Auftragnehmer verpflichtet sich, technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit (Zutrittskontrolle, Zugangskontrolle, Zugrisskontrolle, Trennungskontrolle und Pseudonymisierung) von Daten garantieren. Beispielhaft kann dies die Umsetzung folgender Maßnahmen bedeuten:

- **Zutrittskontrolle**
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, sichergestellt durch
 - ☐ Magnet- oder Chipkarten
 - ☐ Schlüssel
 - ☐ elektrische Türöffner
 - ☐ Werkschutz bzw. Pförtner
 - ☐ Alarmanlagen
 - ☐ Videoanlagen
 - ☐ Sonstiges: *Sonstiges*

- **Zugangskontrolle**
Keine unbefugte Systembenutzung, sichergestellt durch
 - ☐ (sichere) Kennwörter
 - ☐ automatische Sperrmechanismen
 - ☐ Zwei-Faktor-Authentifizierung
 - ☐ Verschlüsselung von Datenträgern
 - ☐ Sonstiges: *Sonstiges*

- **Zugriffskontrolle**
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, sichergestellt durch
 - ☐ Berechtigungskonzepte
 - ☐ bedarfsgerechte Zugriffsrechte
 - ☐ Protokollierung von Zugriffen
 - ☐ Sonstiges: *Sonstiges*

- Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, sichergestellt durch
 - ☐ Mandantenfähigkeit
 - ☐ Sandboxing
 - ☐ Sonstiges: *Sonstiges*

- Pseudonymisierung (Art. 32 Abs. 1 a) DS-GVO; Art. 25 Abs. 1 DS-GVO)
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 entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

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

Der Auftragnehmer verpflichtet sich, technische und organisatorische Maßnahmen zu treffen, die die Integrität (Weitergabekontrolle, Eingabekontrolle) von Daten garantieren. Beispielhaft kann dies die Umsetzung folgender Maßnahmen bedeuten:

- Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, sichergestellt durch
 - ☐ Verschlüsselung
 - ☐ Virtual Private Networks (VPN)
 - ☐ elektronische Signatur
 - ☐ Sonstiges: *Sonstiges*

- Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, sichergestellt durch
 - ☐ Protokollierung
 - ☐ Dokumentenmanagement
 - ☐ Sonstiges: *Sonstiges*

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

Der Auftragnehmer verpflichtet sich, technische und organisatorische Maßnahmen zu treffen, die die Verfügbarkeit und Belastbarkeit (Verfügbarkeitskontrolle, Wiederherstellbarkeit) von Daten garantieren. Beispielhaft kann dies die Umsetzung folgender Maßnahmen bedeuten:

- Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, sichergestellt durch Backup-Strategie (online/offline; on-site/off-site)
 - ☐ unterbrechungsfreie Stromversorgung (USV)
 - ☐ Virenschutz
 - ☐ Firewall
 - ☐ Meldewege
 - ☐ Notfallpläne
 - ☐ Sonstiges: *Sonstiges*

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 c) DS-GVO).

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

Der Auftragnehmer verpflichtet sich, technische und organisatorische Maßnahmen zu treffen, die Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Datenschutz-Management und Informationssicherheits-Management, Incident-Response-Management, Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO), Auftragskontrolle) von Daten möglich machen. Beispielhaft kann dies die Umsetzung folgender Maßnahmen bedeuten:

- Datenschutz-Management und Informationssicherheits-Management
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)
- Auftragskontrolle
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, sichergestellt durch

-
- ☐ eindeutige Vertragsgestaltung
 - ☐ formalisiertes Auftragsmanagement
 - ☐ strenge Auswahl des Dienstleisters
 - ☐ Vorabüberzeugungspflicht
 - ☐ Nachkontrollen
 - ☐ Sonstiges: *Sonstiges*