Anhang D1

zum

EVB-IT Systemvertrag

(im Folgenden „**Hauptvertrag**“)

Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 Abs. 3 Europäische Datenschutz-Grundverordnung

(im Folgenden „**DSGVO**“)

zwischen

Dachgesellschaft Bauvorhaben

Hochschulmedizin Niedersachsen mbH,

Andreaestraße 7,

30159 Hannover

„**Hauptauftraggeber**“ genannt,

und

Die Hochschulmedizin Hannover Baugesellschaft mbH (HBG),

Podbielskistraße 386,

30659 Hannover

„**Auftraggeber 2**“ genannt,

und

Die Baugesellschaft Universitätsmedizin Göttingen mbH (BauG UMG),

Robert-Koch-Straße 34,

37075 Göttingen

„**Auftraggeber 3**“ genannt,

nachfolgend gemeinschaftlich als „**Auftraggeber** oder **Gesamtauftraggeber**“ genannt

und

[XXX],
[XXX],

„**Auftragnehmer**“ genannt,

jeder für sich eine „**Partei**“, zusammen die „**Parteien**“

1. Gegenstand und Dauer des Auftrags; Ort der Datenverarbeitung

1.1 Der Gegenstand dieser Vereinbarung über die Verarbeitung von personenbezogenen Daten im Auftrag **(„Auftragsverarbeitungsvereinbarung“)** ergibt sich aus dem Hauptvertrag, den EVB-IT System-AGB und seinen Anlagen. Die genauen Details des Leistungsumfangs und der Leistungsbereiche sind in der Leistungsbeschreibung (Dokument: B Leistungsbeschreibung BI-CPM Software) dem Kriterienkatalog (Dokument: C4 Kriterienkatalog BI-CPM Software) sowie in diesem Vertrag festgelegt.

1.2 Die Kategorien von Daten, die Gegenstand der Datenverarbeitung nach Maßgabe dieser Auftragsverarbeitungsvereinbarung sind, werden mitsamt Art und Zweck der Verarbeitung durch den Auftragnehmer für die Auftraggeber in **Anhang 1** zu dieser Auftragsverarbeitungsvereinbarung aufgeführt.

Die Vertragsdauer und die Kündigungsfristen dieser Auftragsverarbeitungsvereinbarung bestimmen sich nach den EVB_IT_System_AGB.

1.3 Die Auftraggeber sind für die Einhaltung der gesetzlichen Bestimmungen im Rahmen der Auftragsdatenverarbeitung, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer, allein verantwortlich („Verantwortlicher“ nach Art. 4 Nr. 7 DSGVO).

1.4 Eine Verarbeitung außerhalb der Geschäftsräume, insbesondere – aber nicht ausschließlich – in Privatwohnungen, ist nur mit ausdrücklicher schriftlicher Zustimmung des Hauptauftraggebers gestattet. Die Maßnahmen nach Artikel 32 DSGVO sind sicherzustellen und der Zutritt zur Wohnung des Beschäftigten zu Kontrollzwecken vertraglich zu vereinbaren.

1.5 Ohne eine ausdrückliche schriftliche Zustimmung des Auftraggebers ist eine Verarbeitung personenbezogener Daten durch den Auftragnehmer außerhalb des Hoheitsgebiets der Länder der Europäischen Union oder einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraums untersagt. Die Zustimmung wird nur erteilt, wenn die Vorgaben der Art. 44 ff. DSGVO eingehalten werden. Klarstellend wird vereinbart, dass auch mit Wirksamwerden des Austritts eines Landes aus der Europäischen Union oder des Europäischen Wirtschaftsraums eine Verarbeitung personenbezogener Daten durch den Auftragnehmer in diesem Land der ausdrücklichen Zustimmung des Auftraggebers bedarf. Der Auftraggeber ist nicht verpflichtet, seine Zustimmung zu erteilen.

2. Pflichten des Auftragnehmers

2.1 Der Auftragnehmer verarbeitet personenbezogene Daten nur im Rahmen des Auftrags der Auftraggeber und der Weisungen des Hauptauftraggebers, außer dass er durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zu einer weitergehenden Verarbeitung verpflichtet ist; in einem solchen Fall teilt der Auftragsnehmer dem Hauptauftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Die Weisungen sind jeweils durch den Auftragnehmer und den Hauptauftraggeber zu dokumentieren. Der Auftragnehmer darf die Daten für keine anderen Zwecke außerhalb dieser Auftragsverarbeitungsvereinbarung und des Hauptvertrags verwenden und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben.

2.2 Sofern erforderlich, unterstützt der Auftragnehmer die Auftraggeber im Rahmen von Datenschutz-Folgenabschätzungen im Sinne von Artikel 35 DSGVO.

2.3 Der Auftragnehmer verarbeitete die personenbezogenen Daten ausschließlich im Rahmen von Weisungen des Hauptauftraggebers. Weisungen des Auftraggeber 2 und Auftraggeber 3 setzt der Auftragnehmer nur nach Zustimmung des Hauptauftraggebers um. Mündliche Weisungen des Hauptauftraggebers bestätigt der Auftragnehmer unverzüglich in Textform (z.B. E-Mail, Fax, o.ä.). Der Auftragnehmer informiert den Hauptauftraggeber unverzüglich, wenn er der Auffassung ist, eine Weisung verstoße gegen anwendbares Recht. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Hauptauftraggeber bestätigt oder abgeändert wird.

2.4 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit und der Wahrung des Datenschutzes verpflichtet haben. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

2.5 Personenbezogene Daten dürfen nur denjenigen Mitarbeitern zugänglich gemacht werden, die von diesen personenbezogenen Daten für die Durchführung der Auftragsverarbeitungsvereinbarung und des Hauptvertrags Kenntnis haben. Personenbezogene Daten dürfen nicht an Dritte weitergegeben werden, sofern es nicht ausdrücklich im Hauptvertrag und in dieser Auftragsverarbeitungsvereinbarung gestattet oder dies durch geltendes Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, vorgeschrieben ist; in diesem Fall wird der Auftragnehmer den Hauptauftraggeber über die erzwungene Offenlegung vorher informieren.

2.6 Der Auftragnehmer unterrichtet den Hauptauftraggeber unverzüglich über jede eingetretene Verletzung des Schutzes personenbezogener Daten oder die in diesem Auftrag getroffenen Festlegungen sowie bei Vorliegen des begründeten Verdachts, dass eine solche Verletzung einzutreten droht. Dies gilt insbesondere im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten der Auftraggeber nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen und spricht sich hierzu unverzüglich mit dem Hauptauftraggeber ab.

2.7 Der Auftragnehmer wird eine Person bestimmen, welche die Informationssicherheit, einschließlich des Betriebs des Auftragnehmers, überwacht, und dem Hauptauftraggeber diese Person unverzüglich mitsamt Kontaktdaten zumindest in Textform und in **Anhang 2** benennen. Anfragen des Hauptauftraggebers im Hinblick auf Dokumentation zur Informationssicherheit der Auftraggeber können an diese Person gerichtet werden. Ändert sich diese Person, hat der Auftragnehmer dies dem Hauptauftraggeber unverzüglich in Textform (z.B. E-Mail, Fax, o.ä.) mitzuteilen.

2.8 Der Auftragnehmer teilt dem Hauptauftraggeber den Namen und die Kontaktdaten des Datenschutzbeauftragten zumindest in Textform und in **Anhang 2** mit. Ändert sich diese Person, hat der Auftragnehmer dies dem Hauptauftraggeber unverzüglich in Textform mitzuteilen. Hat der Auftragnehmer keinen Datenschutzbeauftragten bestellt, teilt er dem Hauptauftraggeber die Gründe mit, warum dies nach den einschlägigen Regelungen des Datenschutzrechts nicht erforderlich ist.

2.9 Der Auftragnehmer wird die Personen bestimmen, welche Weisungen des Hauptauftraggebers im Hinblick auf die Verarbeitung personenbezogener Daten

entgegennimmt und teilt deren Kontaktdaten zumindest in Textform und in **Anhang 2**. Ändern sich diese Personen, hat der Auftragnehmer dies dem Hauptauftraggeber unverzüglich in Textform mitzuteilen.

2.10 Im Falle einer Inanspruchnahme der Auftraggeber durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Artikel 82 DSGVO verpflichtet sich der Auftragnehmer, die Auftraggeber bei der Abwehr des Anspruchs im Rahmen seiner Möglichkeiten zu unterstützen.

3. Rechte und Pflichten der Auftraggeber

3.1 Die Auftraggeber haben den Auftragnehmer zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

3.2 Der Hauptauftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen. Zum Zeitpunkt des Inkrafttretens dieser Auftragsverarbeitungsvereinbarung ist diese Person in **Anhang 2** benannt. Ändert sich diese Person, hat der Hauptauftraggeber dies dem Auftragnehmer unverzüglich in Textform mitzuteilen.

3.3 Weisungsberechtigte Personen im Hinblick auf die Datenverarbeitung nach dieser Auftragsverarbeitungsvereinbarung auf Seiten des Hauptauftraggebers sind in **Anhang 2** benannt. Auftraggeber 2 und Auftraggeber 3 sind nicht weisungsberechtigt.

4. Anfragen betroffener Personen

4.1 Soweit sich eine betroffene Person unmittelbar an den Auftragnehmer mit Anfragen oder Forderungen zur Übertragung, Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Hauptauftraggeber weiterleiten und die betroffene Person darüber informieren, dass die Auftraggeber die Verantwortlichen im Sinne der DSGVO sind. Auskünfte an Dritte oder betroffene Personen dürfen ohne eine entsprechende Weisung des Hauptauftraggebers nicht erteilt werden.

4.2 Der Auftragnehmer unterstützt die Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Artikel 33 bis 36 DSGVO genannten Pflichten.

5. Subunternehmer

5.1 Der Auftragnehmer darf Subunternehmer nur nach vorheriger ausdrücklicher schriftlicher Zustimmung des Hauptauftraggebers beauftragen.

5.2 Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer Dritte mit der vollständigen oder teilweisen Erfüllung der im Hauptvertrag vereinbarten Leistung beauftragt. Hiervon ausgenommen sind Lieferanten und Dienstleister des Auftragnehmers, welche keine Daten, die Gegenstand dieser Auftragsverarbeitungsvereinbarung sind, verarbeiten. Der Verarbeitung von Daten wird die Möglichkeit der Kenntnisnahme gleichgestellt.

5.3 Subunternehmer, die in **Anhang 3** zu dieser Auftragsverarbeitungsvereinbarung aufgeführt sind („**genehmigte Subunternehmer**“), werden mit Unterzeichnung dieser Auftragsverarbeitungsvereinbarung als Subunternehmer genehmigt. Im Falle eines

Austauschs oder Hinzufügens neuer Subunternehmer teilt der Auftragnehmer den neuen Subunternehmer zumindest 12 Wochen vor Beginn der geplanten Aufnahme der Tätigkeit mit. Der Hauptauftraggeber hat in diesem Fall 4 Wochen Zeit, um dem Einsatz des geplanten Subunternehmers zu widersprechen, wobei die Entscheidung begründet werden soll. In einem solchem Fall werden die Parteien versuchen, eine Einigung zu erzielen.

5.4 Der Auftragnehmer wählt sämtliche Subunternehmer sorgfältig aus, insbesondere unter Berücksichtigung der von ihnen umgesetzten technischen und organisatorischen Schutzmaßnahmen und überprüft vor der Beauftragung sowie regelmäßig während des Vertragsverhältnisses die Einhaltung der gesetzlichen und vertraglichen Datenschutzbestimmungen durch den Subunternehmer.

5.5 Subunternehmer werden vom Auftragnehmer auf Grundlage einer schriftlichen Vereinbarung beauftragt, die Bestimmungen zur Vertraulichkeit, zum Datenschutz und Datensicherheit enthalten muss, welche den Anforderungen dieser Auftragsverarbeitungsvereinbarung genügen.

5.6 Der Auftragnehmer verpflichtet sich, Subunternehmer nur dann mit der Verarbeitung personenbezogener Daten zu betrauen, wenn diese sich zuvor schriftlich in gleicher Weise wie der Auftragnehmer zur Einhaltung der Verpflichtungen nach Art. 28 DSGVO verpflichtet.

5.7 Bei der Unterbeauftragung ist sicherzustellen, dass der Auftragnehmer Kontroll- und Überprüfungsrechte entsprechend dieser Auftragsverarbeitungsvereinbarung gegenüber dem Subunternehmer vertraglich vereinbart. Dies umfasst auch das Recht des Hauptauftraggebers, vom Auftragnehmer auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

5.8 Eine weitere Unterbeauftragung durch den Subunternehmer selbst bedarf der vorherigen schriftlichen Zustimmung des Hauptauftraggebers; sämtliche vertraglichen Regelungen mit den Subunternehmern haben den Anforderungen dieser Auftragsverarbeitungsvereinbarung zu genügen.

6. Technische und organisatorische Schutzmaßnahmen

6.1 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. 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 Artikel 32 Abs. 1 DSGVO zu berücksichtigen.

6.2 Die vom Auftragnehmer getroffenen technisch-organisatorischen Maßnahmen sind in **Anhang 4** aufgeführt. Der Auftragnehmer hat die Umsetzung der dargelegten und erforderlichen technischen organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und nachzuweisen sowie dem Hauptauftraggeber zur Prüfung zu übergeben.

6.3 Der Auftragnehmer gewährleistet, seinen Pflichten nach Artikel 32 Abs. 1 lit. d DSGVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

6.4 Der Auftragnehmer ermöglicht eine ordnungsgemäße Kontrolle und Überwachung des Datenschutzes durch den Hauptauftraggeber. Der Auftragnehmer wird insbesondere richtige, vollständige und notwendige Informationen zur Verfügung stellen, Überprüfungen und (Kontroll-)Maßnahmen dulden und Anweisungen des Hauptauftraggebers ausführen. Der Auftragnehmer wird den Hauptauftraggeber unverzüglich informieren, falls eine Datenschutzbehörde Überwachungen oder Kontrollen durchführt und im Rahmen ihrer Kontrolle und Überwachung des Datenschutzes an den Auftragnehmer hinsichtlich der Verarbeitung personenbezogener Daten im Auftrage der Auftraggeber gemäß der Auftragsverarbeitungsvereinbarung herantritt.

6.5 Ungeachtet der Regelung in den vorstehenden Absätzen unterliegen die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist der Auftragnehmer verpflichtet, adäquate Maßnahmen umzusetzen, soweit es für den jeweiligen Schutz erforderlich ist. Weiterhin ist es dem Auftragnehmer gestattet, bestehende Maßnahmen durch anderweitige adäquate Maßnahmen zu ersetzen, wenn dabei sichergestellt ist, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren und dem Hauptauftraggeber in angemessener Zeit, mindestens aber vier (4) Wochen vor deren Einführung mitzuteilen. Ist dies aufgrund der Erforderlichkeit einer sofortigen Umsetzung aus Gründen der Datensicherheit nicht möglich, wird der Auftragnehmer die entsprechenden Informationen unverzüglich zur Verfügung stellen.

7. Kontrollrechte des Hauptauftraggebers

7.1 Der Hauptauftraggeber ist berechtigt, Kontrollen zur Prüfung der Einhaltung der Vorgaben dieses Vertrages im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Der Auftragnehmer wird insbesondere richtige, vollständige und notwendige Informationen zur Verfügung stellen, Überprüfungen und (Kontroll-)Maßnahmen dulden und Anweisungen des Hauptauftraggebers ausführen.

7.2 Nach vorheriger Ankündigung von mindestens sieben (7) Kalendertagen im Voraus darf der Hauptauftraggeber ohne Anlass – bei bestehendem konkreten Anlass nach Ankündigung ohne Einhaltung einer bestimmten Frist – selbst oder durch einen qualifizierten, unabhängigen Prüfer nach Wahl und auf Kosten des Hauptauftraggebers die Verarbeitungsprozesse des Auftragnehmers überprüfen. Die Prüfung ohne konkreten Anlass kann einmal jährlich durchgeführt werden. Sollten im Rahmen einer solchen Prüfung Verstöße gegen die Vorgaben dieser Auftragsverarbeitungsvereinbarung aufgedeckt werden, hat der Auftragnehmer die für die Durchführung der Prüfung entstandenen Kosten zu tragen.

7.3 Die Prüfungen sind während der üblichen Geschäftszeiten und innerhalb einer angemessenen Dauer vorzunehmen und sollen den täglichen Geschäftsbetrieb des Auftragnehmers nicht unangemessen beeinträchtigen.

7.4 Für den Fall der Prüfung durch einen unabhängigen Prüfer ist dieser zur Verschwiegenheit gegenüber Dritten zu verpflichten.

7.5 Der Auftragnehmer unterstützt den Hauptauftraggeber in angemessener Weise bei der Durchführung der Prüfung. Insbesondere erklärt sich der Auftragnehmer dazu bereit,

dem Hauptauftraggeber hinreichende Nachweise und Informationen über seine Datenverarbeitungsanlagen zur Verfügung zu stellen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

8. Rechte hinsichtlich personenbezogener Daten

8.1 Alle Rechte an den personenbezogenen Daten und an allen Kopien hiervon verbleiben im Verhältnis zum Auftragnehmer bei den Auftraggebern.

8.2 Der Auftragnehmer speichert personenbezogene Daten nur solange, wie das Vertragsverhältnis zu den Auftraggebern besteht.

8.3 Kopien/Duplikate dürfen ohne Wissen der Auftraggeber nicht erstellt werden. Der Auftragnehmer darf personenbezogene Daten, Datenträger und Unterlagen nur kopieren, wenn (i) der Hauptauftraggeber vorher ausdrücklich schriftlich zustimmt, (ii) dies ausdrücklich nach dieser Auftragsverarbeitungsvereinbarung erlaubt ist, (iii) dies für die Zwecke dieser Auftragsverarbeitungsvereinbarung oder des Hauptvertrags erforderlich ist oder (iv) dies im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten zwingend erforderlich ist.

8.4 Soweit die Auftraggeber nicht in der Lage sind, personenbezogene Daten zu berichtigen, zu übertragen, zu löschen oder zu sperren, wird der Auftragnehmer einer entsprechenden Aufforderung des Hauptauftraggebers zur Vornahme einer solchen Handlung unentgeltlich nachkommen.

8.5 Nach Beendigung dieser Auftragsverarbeitungsvereinbarung oder nach Aufforderung durch den Hauptauftraggeber wird der Auftragnehmer unverzüglich, spätestens innerhalb von 30 Tagen, und entsprechend den Weisungen des Hauptauftraggebers entweder alle personenbezogenen Daten gemäß den geltenden Datenschutzbestimmungen zurückgeben oder löschen und/oder alle personenbezogenen Daten vernichten. Ebenso sind alle übergebenen Datenträger und Unterlagen nach den Vorgaben von Satz 1 herauszugeben oder zu vernichten. Die Löschung und/oder Vernichtung sind in geeigneter Weise zu dokumentieren und auf Anforderung des Hauptauftraggebers zu bestätigen. Auf Anfrage sind ein Löschprotokoll auszuhändigen und die Löschung nachzuweisen.

9. Haftung und Schadensersatz

Die Auftraggeber und der Auftragnehmer haften gegenüber betroffenen Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung. Im Übrigen gelten die in den EVB-IT System-AGB und dem Hauptvertrag getroffenen Regelungen zur Haftung.

10. Schlussbestimmungen

10.1 Werden personenbezogene Daten, die Gegenstand dieser Auftragsverarbeitungsvereinbarung sind, Gegenstand einer Durchsuchung und Beschlagnahme, einer Zwangsvollstreckung, einer Beschlagnahmung im Rahmen eines Konkurs- oder Insolvenzverfahrens oder ähnlicher Ereignisse oder Maßnahmen Dritter, während sie sich in der Kontrolle des Auftragnehmers befinden, so hat der Auftragnehmer den Hauptauftraggeber unverzüglich hiervon in Kenntnis zu setzen. Der Auftragnehmer hat umgehend alle in eine entsprechende Maßnahme involvierten Parteien darüber zu informieren, dass etwaige betroffene personenbezogene Daten alleiniges Eigentum des jeweiligen Auftraggebers sind und in dessen alleinige

Verantwortung fallen, dass die personenbezogenen Daten der alleinigen Verfügungsbefugnis des jeweiligen Auftraggebers unterliegen und dass der jeweilige Auftraggeber der Verantwortliche im Sinne der DSGVO ist.

10.2 Änderungen an dieser Auftragsverarbeitungsvereinbarung und/oder seinen Bestandteilen – u. a. in Bezug auf etwaige Zusicherungen und Gewährleistungen des Auftragnehmers – sind nur in Schriftform wirksam und bindend und gelten zudem nur, wenn aus der Änderung ausdrücklich hervorgeht, dass diese auf die Bedingungen dieser Auftragsverarbeitungsvereinbarung Anwendung findet. Vorstehendes gilt ebenso für etwaige Verzichtserklärungen oder Änderungen in Bezug auf die vorgeschriebene Schriftform.

10.3 Die Einrede des Zurückbehaltungsrechts i.S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

10.4 Ist oder wird eine Bestimmung oder Teilbestimmung dieser Auftragsverarbeitungsvereinbarung unwirksam oder von einem Gericht gleich aus welchem Grund für unwirksam, nicht durchsetzbar oder rechtswidrig erklärt, bleibt die Wirksamkeit der übrigen Bestimmungen davon unberührt und diese Bestimmung oder Teilbestimmung wird nur insoweit gestrichen oder abgeändert, wie dies notwendig ist, um ihre Wirksamkeit, Durchsetzbarkeit oder Rechtmäßigkeit sicherzustellen.

10.5 Diese Auftragsverarbeitungsvereinbarung unterliegt deutschem Recht, unter Ausschluss des Kollisionsrechts.

_____	_____
Datum, Ort	Datum, Ort
_____	_____
Unterschrift (Hauptauftraggeber)	Unterschrift (Auftragnehmer)
_____	_____
Name, Vorname, Funktion	Name, Vorname, Funktion

_____
Datum, Ort

_____
Unterschrift (Auftraggeber 2)

_____
Name, Vorname, Funktion

_____
Datum, Ort

_____
Unterschrift (Auftraggeber 3)

_____

Name, Vorname, Funktion

Anhang 1

Art und Zweck der Verarbeitung, Kategorien betroffener Personen, Art personenbezogener Daten

Hinweis: Wird nach Abschluss des Hauptvertrages vervollständigt oder ggfs. angepasst, sofern erforderlich

Art und Zweck der Verarbeitung

- Beschaffung, Einführung und Inbetriebnahme einer Business-Intelligence- und Corporate-Planning-Management-Lösung (BI-/CPM-Lösung)
- Installation, Konfiguration
- Workshops, Schulung
- Betriebs-, Support- und Wartungsleistungen
- Service Desk/Hotline

Art der Daten

- Unternehmensdaten, insbesondere zur Verwaltung, Rechnungswesen und Personalkosten
- Mitarbeiterinformationen, z. B. Vorname, Nachname, E-Mail-Adresse etc.
- Informationen zu Kunden, wie z. B. Kontaktdaten

Kreis betroffener Personen

- Mitarbeiter
- Mitarbeiter der Dienstleister des Auftraggebers
- Auftragnehmer
- Kunden

Anhang 2

Kontaktpersonen

Auftragnehmer wird eine Person bestimmen, welche die Informationssicherheit (Nr. 2.7):

[… vom Auftragnehmer zu ergänzen…]

Namen und die Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers (Nr. 2.8):

[… vom Auftragnehmer zu ergänzen…]

Weisungsempfänger des Auftragnehmers (Nr. 2.9)

[… vom Auftragnehmer zu ergänzen…]

Ansprechpartner für Datenschutzfragen beim Hauptauftraggeber (Nr. 3.2):

- *[Wird nach Abschluss des Hauptvertrages bekannt gegeben]*

Weisungsberechtigte Personen des Hauptauftraggebers (Nr. 3.3):

- …

Anhang 3

Genehmigte Subunternehmer

Hinweis: vom Auftragnehmer zu ergänzen

Unternehmen mit Namen, Rechtsform, Kontaktdaten und ladungsfähiger Anschrift	Ort(e) der Datenverarbeitung	Umfang und Zweck des Unterauftrags
[XXX]	[XXX]	[XXX]

Anhang 4

Technische und organisatorische Maßnahmen

Hinweis: Wird ggfs. nach Abschluss des Hauptvertrages vervollständigt

Der Auftragnehmer trifft geeignete technische und organisatorische Datenschutzmaßnahmen gemäß Ziffer 6 der Auftragsverarbeitungsvereinbarung. Die folgenden Maßnahmen sind Mindestanforderungen und zu jeder Zeit vom Auftragnehmer einzuhalten:

C.1 Schutzziel Vertraulichkeit

Es ist sicherzustellen, dass keine Person – sowohl Mitarbeiter als auch Dritte - personenbezogene Daten unbefugt zur Kenntnis nimmt.

C.1.1 Zutrittskontrolle

Kontrolle des räumlichen Zutritts zu Datenverarbeitungsanlagen (DV-Anlage) durch Unbefugte. Durch die Zutrittskontrolle soll verhindert werden, dass Personen, die dazu nicht befugt sind, in die Nähe einer DV-Anlage gelangen können.
Zur DV-Anlage gehören neben der Zentraleinheit einschließlich der integrierten Laufwerke auch die angeschlossenen Peripherieeinheiten wie Terminals, PCs, Drucker, Plotter und Bandeinheiten usw. Eine Zutrittskontrolle zu PCs innerhalb von Büroräumen wird z.B. dadurch sichergestellt, dass Maßnahmen ergriffen werden, die verhindern, dass Betriebsfremde in die Nähe von PCs gelangen bzw. den Bildschirm einsehen können.

Maßnahmen
Zutrittsregelung für **betriebsfremde Personen**; die Umsetzung erfolgt i.d.R. durch folgende Punkte:
• Zentraler Empfangsbereich vorhanden und verschlossene Außentür
• Aufenthalt von Fremden im gesamten Unternehmensgebäude nur in Anwesenheit von Mitarbeitern
• Sichtbar zu tragender Gastausweis
• Vermerk von Zu- und Abgang von betriebsfremden Personen am Empfang
Zutrittsregelung für **betriebsangehörige Personen**; die Umsetzung erfolgt i.d.R. durch folgende Punkte:
• Chipkarte mit Protokollierung & Einsatz Transponder
• Rücknahme von Zugangsmitteln nach Ablauf der Berechtigung
Festlegung der zutrittsberechtigten Personen für Rechner-/Serverraum
Maßnahmen, damit nur Befugte Zutritt zum Rechner-/Serverraum erhalten, i.d.R.:
• Protokollierung der Zu- und Abgänge der Serverräume
• Schlüsselregelung (verschlossene Türen; Schlüsselausgabe nur an Befugte; Aufbewahrung und Verwendung eines Generalschlüssels)
• Maßnahmen der Objektsicherung (wie Absicherung von Schächten und Fenstern; Geländeüberwachung, Bewegungsmelder)

C.1.2 Zugangskontrolle

Die Benutzung von DV-Anlagen durch unbefugte Personen (nicht befugte Mitarbeiter oder Externe) soll verhindert werden. Bei der Zugangskontrolle geht es um die Frage der Identifikation und anschließender Authentifikation. Die Zugangskontrolle umfasst auch das Ziel, dass kein externer Zugang (z.B. aus dem Internet) auf DV-Anlagen erfolgen kann (Hackerschutz).

Maßnahmen
Authentisierung der Benutzer gegenüber dem Datenverarbeitungssystem. d.h. Identifikation durch Benutzernamen und Passwort, biometrisches Verfahren oder ssh-Key
Regelungen zur Passwortvergabe • Persönliches Passwort • Mindestens 8 Zeichen, darunter auch Sonderzeichen/Zahlen • Vergabe durch Nutzer selbst • Verfall nach vorgegebener Zeit (spätestens nach 4 Monaten) • Automatisierte temporäre Zugangssperre nach drei Fehlversuchen • Keine Weitergabe an Dritte • Regelung für Fall der Abwesenheit (Urlaub, Krankheit etc.)
Umgehende Sperrung von Berechtigungen beim Ausscheiden von Mitarbeitern
Regelmäßige Kontrolle der Gültigkeit und einen möglichen Ablauf von Berechtigungen (mindestens jährlich)
Sicherung der Bildschirmarbeitsplätze bei Abwesenheit und laufendem System (Passwortschutz für Bildschirmschoner nach 5 Min. bis 15 Min, je nach Risiko des Missbrauchs)
Abschottung interner Netze gegen Zugriffe von außen (Firewall, Verschlüsselung VPN)
Regelmäßige Überprüfung der Firewall-Regeln
Verschlüsselung der Festplatten ausgegebener Notebooks, die außerhalb des Betriebsgeländes eingesetzt werden
Verwendung verschiedener Passwörter für eingesetzte VMware Hosts

C.1.3 Zugriffskontrolle

Ziel der Zugriffskontrolle ist es, dass Mitarbeiter und befugte Dritte nur im Rahmen ihrer Zugriffsberechtigung auf Daten zugreifen können. Darüber hinaus soll sichergestellt werden, dass beim Umgang mit personenbezogenen Daten diese nicht unbefugt gelesen, kopiert, verändert oder entfernt (gelöscht) werden können. Dies gilt sowohl für Daten, die in DV-Systemen gespeichert sind, als auch für solche, die sich auf maschinell lesbaren Datenträgern oder auf Papier befinden.

Maßnahmen
Erstellung eines Benutzerprofils, d.h. Festlegung von Zugriffsberechtigungen hinsichtlich personenbezogener Daten von Nutzern
Differenzierte Berechtigungen für Lesen, Verändern oder Löschen von Daten
Erstellung eines Berechtigungskonzeptes • Einrichtung von Administrationsrechten • Verwaltung der Zugriffsrechte durch Systemadministrator
Regelmäßige Überprüfung vergebener Berechtigungen mit Entzug nicht mehr benötigter Zugriffsrechte

Trennung von Test- und Produktionsbetrieb
Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger und von Makulatur (beispielsweise Fehldrucke von Arbeitslisten, Anschreiben etc.)
Schriftliche Regelung zum Kopieren und Ausdrucken von vertraulichen Daten

C.1.4 Trennungskontrolle

Gemäß dem Trennungsgebot sind Daten, die zu unterschiedlichen Zwecken erhoben wurden, auch getrennt zu verarbeiten. Dadurch soll gewährleistet werden, dass die Zweckbindung personenbezogener Daten durch organisatorische und technische Maßnahmen umgesetzt wird. Besondere Bedeutung hat das Trennungsgebot im Rahmen der Auftragsverarbeitung, wenn z.B. Daten mehrerer Auftraggeber auf einem System gespeichert sind. Sofern das Trennungsgebot nicht durch technische Maßnahmen, wie z.B. eine Zugriffs-Kontroll-Software, erreicht werden kann, ist eine getrennte Speicherung notwendig.

Maßnahmen
Berechtigungskonzept mit Festlegung der Zugriffsrechte
Umsetzung des Trennungsgebotes auf Datenbankebene durch Mandantentrennung bzw. logische Trennung anhand verschiedener Buchungskreise

C. 2 Schutzziel: Integrität

Es ist sicherzustellen, dass informationstechnische Prozesse und Systeme die festgelegten Spezifikationen kontinuierlich einhalten, so dass die mit ihnen zu verarbeitenden Daten unversehrt, vollständig und aktuell bleiben.

C. 2.1 Weitergabekontrolle

Umfasst sind alle Varianten der Weitergabe von personenbezogenen Daten mittels Datenträgern oder Kommunikationsnetz. Die Weitergabekontrolle soll verhindern, dass Daten bei deren Weitergabe unbefugt verwendet (gelesen, kopiert, verändert oder entfernt/gelöscht) werden können. Der Begriff der Weitergabe umfasst sowohl die Übermittlung an Dritte als auch die Weitergabe im Rahmen der Auftragsverarbeitung zwischen Auftraggeber und Auftragnehmer und an den Betroffenen.

Maßnahmen
Bei Weitergabe auf physischen Datenträgern: Dokumentation von Datenempfänger sowie der Transport-/Übermittlungswege
Soweit technisch möglich, eine elektronische Übermittlung auf gesicherten Übertragungswegen
Patch Management, das ein zeitnahes Einspielen sicherheitskritischer Patches gewährleistet
Härtung der besonders schützenswerten Systeme
Patch Management mit rechtzeitiger Mitigation von Applikationen und Servern, zu denen vom Hersteller keine Sicherheitspatches mehr bereit gestellt werden
Einsatz eines täglich upgedateten Malwareschutzes

C. 2.2 Eingabekontrolle

Durch die Eingabekontrolle soll dokumentiert werden, wer für eine unzulässige oder fehlerhafte Dateneingabe verantwortlich ist. Ziel ist die Revisionsfähigkeit der Eingabe von personenbezogenen Daten in das DV-System, zu welchem auch nicht vernetzte Einzelarbeitsplätze wie z.B. PCs gehören. Die zu kontrollierende Dateneingabe umfasst sowohl das erstmalige Speichern als auch die Veränderung und Löschung (Entfernung) von Daten.

Maßnahmen
Führung revisionssicherer (dokumentierter, nachvollziehbarer) Zugriffsberechtigungen
Protokollierung von Eingabe, Veränderungen oder Löschung personenbezogener Daten
Regelung zu Zugriffsbefugnissen auf erstellte Protokolldaten
Löschungsregelung für Protokolldaten

C. 3 Schutzziel: Verfügbarkeit

C. 3.1 Verfügbarkeitskontrolle

Schutz der Daten gegen zufällige Zerstörung oder Verlust. Mögliche Gefahren sind z.B. Wasserschäden, Blitzschlag, Stromausfall, Brand, Sabotage oder Diebstahl.

Maßnahmen
formalisiertes Freigabeverfahren für neue DV-Verfahren und bei wesentlichen Änderungen in Alt-Verfahren
Unterbrechungsfreie Stromversorgung (USV)
Automatische Feuer- und Rauchmeldeanlagen mit Signalweiterleitung
Feuerlöschgerät im Serverraum
Sicherung der Datenbestände • Erstellung eines Backup-Konzeptes • Spiegelung der Daten je nach SLAs • Aufbewahrung der Sicherungskopien an einem sicheren Ort (Auslagerung bzw. Ablage in einem anderen Brandabschnitt) • Erstellung von Sicherungskopien nach dem Generationenprinzip in geeigneten zeitlichen Abständen
Rekonstruktion von Datenbeständen • Test der Rekonstruktion von Datenbeständen
Redundanz von Hard- und Software sowie Infrastruktur je nach SLAs
Vertretungsregelungen für Mitarbeiter
keine betriebsunnötige Brandlast im Serverraum
Ausreichende Wandstärke von Serverräumen und ausreichend widerstandsfähige Türen für Zutritt zu Serverräumen

C.4 Schutzziel: Belastbarkeit

C.4.1 Auftragskontrolle

Gewährleistung der weisungsgemäßen Auftragsverarbeitung. Der Auftragnehmer hat die ihm erteilten Weisungen einzuhalten, während der Auftraggeber Sorge dafür zu tragen hat, dass seine Weisungen klar und eindeutig sind und befolgt werden.

Maßnahmen
Kontrolle der Einhaltung von Datensicherheitsbestimmungen durch Auftragnehmer und Meldung, wenn Verstöße vorliegen oder der Verdacht besteht, dass die Datensicherheitsvorgaben unzureichend sind.
Verpflichtung der Mitarbeiter des Auftragnehmers zur Wahrung der datenschutzrelevanten Vorgaben
Schriftliche Vereinbarung eines Vertrages zur Auftragsverarbeitung

C.4.2 Verfahren zur regelmäßigen Überprüfung

Ständige Gewährleistung der Einhaltung der Vorgaben an Datenschutz und IT-Sicherheit. Der Auftragnehmer hat regelmäßig zu überprüfen und dokumentieren, dass die vertraglich geschuldeten Vorgaben eingehalten werden.

Maßnahmen
Betrieb eines Systems zur Rechenschaftspflicht und IT-Governance
Meldung von Sicherheitsvorfällen, die im laufenden Betrieb festgestellt werden
Kontrolle der Wirksamkeit der durchgeführten Maßnahmen mindestens einmal pro Jahr