Datenschutz-Grundverordnung

Vertrag zur Auftragsverarbeitung
gem. Art. 28 DSGVO

zwischen der

_____

_____

_____

Verantwortlicher gem. Art. 4 Abs. 7 DSGVO, nachstehend **Auftraggeber** genannt

und der

Venturis IT GmbH

Auf der Krautweide 32

65812 Bad Soden

Auftragsverarbeiter gem. Art. 4 Abs. 8 DSGVO, nachstehend **Auftragnehmer** genannt

1 Gegenstand und Dauer des Auftrags

1.1 Gegenstand

Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

_____

_____

_____

_____

(Definition der Aufgaben)

1.2 Dauer und Kündigung

Der Auftrag wird zur einmaligen Ausführung erteilt.

2 Konkretisierung des Auftragsinhalts

2.1 Art und Zweck der Verarbeitung

Bei der Durchführung von Service- und Wartungsarbeiten kann ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden.
Ein Mitarbeiter des Auftraggebers sollte während der Fernwartungssitzung am Arbeitsplatz bleiben.

2.2 Ort der Datenverarbeitung

2.2.1 Erbringung

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. DS-GVO erfüllt sind.

2.3 Art der Daten

Gegenstand der Verarbeitung sind folgende Arten personenbezogener Daten:
Alle Arten personenbezogener Daten des Auftraggebers.

2.4 Kategorien betroffener Personen

Die Kategorien der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags betroffenen Personen umfassen

Alle Kategorien personenbezogener Daten des Auftraggebers.

3 Technisch-organisatorische Maßnahmen / Sicherheit der Verarbeitung

3.1

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.

3.2

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 in **Anlage 1,** Anlage 1 wird somit Vertragsbestandteil]

3.3

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.

4 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.

5 Qualitätssicherung, Kontrollen und sonstige Pflichten des Auftragnehmers

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:

Schriftliche Bestellung eines Datenschutzbeauftragten, 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.
Datenschutzbeauftragter des Auftragnehmers zum Zeitpunkt des Vertragsschlusses ist:
(Name und Kontaktdaten, bei externen auch Anschrift und ggf. Unternehmen)
Koppenhöfer & Werner Beratungsgesellschaft mbH

Boris Koppenhöfer

Nikolausstraße 11 D-65343 Eltville

+49 6123 9213-61

datenschutz@venturisit.de

Datenschutz-Grundverordnung

- Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit und rechtmäßige Datenverarbeitung 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.
- 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 [Einzelheiten in **Anlage 1**].
- Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- Die 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.
- 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.
- 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.
- Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse gem. Ziffer 7 dieses Vertrages.

6 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.

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

> Der Auftraggeber stimmt der Beauftragung der in **Anlage 2** aufgeführten Unterauftragnehmern unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zu. Anlage 2 wird insoweit Vertragsbestandteil.

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 Satz 2 dieser Ziffer eingesetzt werden sollen.

Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform) sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer im Wortlaut oder sinngemäß aufzuerlegen.

7 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 Kontrollen, 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 gem. Art. 28 DS-GVO 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.

8 Mitteilung bei Verstößen

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u. 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,
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden,
- 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,
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung,
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

9 Weisungsbefugnis des Auftraggebers gegenüber dem Auftragnehmer

Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. 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.

10 Löschung von 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 jedoch 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.

11 Pfändung, Beschlagnahmung der Daten beim Auftragnehmer

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 Ebenso wird der Auftragnehmer alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Datenhoheit beim Auftraggeber liegt.

12 Haftung

Auftraggeber und Auftragnehmer haften im Außenverhältnis gem. Art. 82 Abs. 1 DSGVO für materielle und immaterielle Schaden, die eine Person wegen eines Verstoßes gegen die DSGVO erleidet. Sind sowohl der Auftraggeber als auch der Auftragnehmer für einen solchen Schaden gem. Art. 82 Abs. 2 DSGVO verantwortlich, haften die Parteien im Innenverhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine Person in einem solchen Fall eine Partei ganz oder überwiegend auf Schadenersatz in Anspruch, so kann diese von der jeweils anderen Partei Freistellung oder Schadloshaltung verlangen, soweit dies ihrem Anteil an der Verantwortung entspricht.

Der Auftragnehmer ist zum Zweck der Enthaftung gem. Art. 82 Abs. 3 DSGVO dazu befugt, Details zu Weisungen des Auftraggebers und zur erfolgten Datenverarbeitung offenzulegen. Der Auftraggeber ist dazu verpflichtet, den Auftragnehmer bestmöglich zu unterstützen, damit sich der Auftragnehmer gegenüber der geschädigten Person gem. Art. 82 Abs. 3 DSGVO enthaften kann.

13 Schlussbestimmungen

13.1 Schriftformerfordernis

Änderungen und Ergänzungen dieser Vereinbarung und ihrer Bestandteile, einschließlich etwaiger Zusicherungen des Auftragnehmers, bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung, bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

13.2 Salvatorische Klausel

Sollten einzelne Bestimmungen dieses Vertrages unwirksam oder nicht durchsetzbar sein oder werden, so berührt dies nicht die übrigen Vertragsbestandteile. Die Vertragsparteien vereinbaren, diese Bestimmung durch eine Bestimmung zu ersetzen, die dem Zweck des Vertrages am nächsten kommt. Dies gilt auch für Regelungslücken.

13.3 Inkrafttreten

Diese Datenschutzvereinbarung tritt mit Unterzeichnung beider Parteien in Kraft.

13.4 Recht

Es gilt deutsches Recht.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Auftraggeber	Auftragnehmer
_____	_____
Name Unterzeichner in Druckbuchstaben	Name Unterzeichner in Druckbuchstaben

Anlage 1

Technisch-organisatorische Maßnahmen

Einleitung

Die VenturisIT GmbH führt Aufträge als Dienstleistung für ihre Kunden durch. Hierbei ist ein Zugriff auf personenbezogene Daten der Kunden zur Durchführung des Auftrags entweder notwendig oder kann mitunter nicht ausgeschlossen werden.

Dies erfordert besondere technische und organisatorische Maßnahmen zur Einhaltung der datenschutzrelevanten Rechtsvorschriften.

Dieses Dokument beschreibt die grundsätzlich vorgenommenen Maßnahmen sowie die verwendeten Sicherheitseinrichtungen und Regelungen.

1 Zutrittskontrolle

1.1 Die Eingangstüren aller Gebäude, in denen die Datenverarbeitung erfolgt, sind mit einer manuellen Schließanlage versehen.

1.2 Die Dokumentation der Zutrittsberechtigungen vorgenannter Schließanlage erfolgt namensscharf. Ebenso die Ausgabe und Rücknahme der vergebenen Schlüssel.

1.3 Betriebsfremde Personen wie Gäste und Besucher erhalten nur in Begleitung von Betriebspersonal Zutritt.

1.4 Die Zutrittsberechtigungen von Reinigungs- und Wartungspersonal erfolgen namensscharf. Der Zutritt zu Räumen, in denen besonders kritische Daten verarbeitet werden, erfolgt in Begleitung und unter Aufsicht von Betriebspersonal oder wird namensscharf protokolliert.

1.5 Die Räume der zentralen Datenhaltung (Serverräume etc.), sowie die Büros der IT-Abteilung gehören einem separaten Schließkreis an. Hier erfolgt der Zutritt von betriebsfremden Personen ausschließlich unter Aufsicht von besonders geschultem Betriebspersonal.

1.6 Bei Beendigung des Arbeitsverhältnisses unterlaufen alle Zutrittsberechtigungen einem Standardprozess. Hier werden nicht mehr benötigte oder nicht mehr gewünschte Berechtigungen entzogen und nachgehalten.

2 Zugangskontrolle

2.1 Das gesamte Unternehmensnetzwerk ist durch ein geschlossenes Firewall-System gesichert. Alle Verbindungen zu den Unternehmensstandorten erfolgen einheitlich durch ein gesichertes virtuelles LAN. Alle Firewalls erfahren regelmäßige Sicherheitsupdates.

2.2 An sämtlichen Übergängen zum Unternehmensnetz werden Virenscanner eingesetzt. Ein- und ausgehende E-Mails werden gescannt. Dateiaustausch per FTP-Protokoll wird gescannt. Der Zugriff auf das Web per Webbrowser wird gescannt. Alle Virenscanner werden automatisiert aktuell gehalten. Die Aktualisierungen werden regelmäßig geprüft.

2.3 Auf allen genutzten Servern und Einzelplatzrechnern werden Virenscanner eingesetzt. Alle Virenscanner werden automatisiert aktuell gehalten. Die Aktualisierungen werden regelmäßig geprüft.

2.4 Auf allen genutzten Servern und Einzelplatzrechnern werden regelmäßig und automatisiert Sicherheitsupdates für Betriebssysteme und relevante Software installiert.

2.5 Die Mitarbeiter werden auf die aktuelle Passwort-Richtlinie verpflichtet. Soweit technisch möglich, erfolgt die Umsetzung der Passwort-Richtlinie als Systemvorgabe.

3 Zugriffskontrolle

3.1 Für alle relevanten Zugriffe auf EDV-Systeme sind Berechtigungskonzepte vorhanden und der Einsatz wird dokumentiert.

3.2 Das jeweilige Recht zur Rechtevergabe ist in einem Organisationskonzept namensscharf dokumentiert.

3.3 Die Vergabe der Zugriffsberechtigungen wird namensscharf dokumentiert.

3.4 Die Administratoren, die Datenbestände des Auftraggebers ganz oder in großen Mengen kopieren oder extrahieren dürfen, sind in einem gesonderten Administratorenkonzept dokumentiert und werden explizit vom Datenschutzbeauftragten im administrativen Umgang mit personenbezogenen Daten geschult. Sie unterliegen einer besonderen Geheimhaltungsverpflichtung für IT-Administratoren.

4 Weitergabekontrolle

4.1 Der Datenaustausch zwischen Auftraggeber und Auftragnehmer erfolgt grundsätzlich verschlüsselt per SFTP/HTTPS.

4.2 Die Daten des Auftraggebers werden auf mobilen Datenverarbeitungsgeräten (Laptop, Tablet-PC, Smartphone etc.) gemäß den Richtlinien für mobile Datenverarbeitungsgeräte als Teil der IT-Richtlinie des Unternehmens geschützt.

5 Eingabekontrolle

5.1 Die Änderung und Löschung von Daten des Auftraggebers auf Systemen des Unternehmens wird namensscharf protokolliert.

5.2 Die regelmäßige Löschfrist für die Logfiles beträgt 2 Jahre.

6 Auftragskontrolle

6.1 Die eingesetzten Mitarbeiter werden auf Vertraulichkeit und rechtmäßige Verarbeitung verpflichtet.

6.2 Die eingesetzten Mitarbeiter werden auf die Einhaltung der IT-Richtlinie des Unternehmens verpflichtet.

6.3 Die eingesetzten Mitarbeiter werden in Bezug auf die Daten der Kunden auf absolute Geheimhaltung verpflichtet.

6.4 Die eingesetzten Mitarbeiter werden regelmäßig gemäß der Datenschutzrichtlinie als Teil der IT-Richtlinie des Unternehmens geschult.

6.5 Sollten Subunternehmer eingesetzt werden, so werden diese dazu verpflichtet, technische und organisatorische Maßnahmen anzuwenden, die dem Sicherheitsniveau dieser TOM im Mindesten gleichstehen.

7 Verfügbarkeitskontrolle

7.1 Der gesamte relevante Datenbestand wird täglich vollständig gesichert. Durch ein rotierendes System werden mehrere Generationen vorgehalten. Zusätzlich findet eine nächtliche Spiegelung der relevanten Daten auf ein NAS statt.

7.2 Die relevanten Systeme werden durch unternehmensangehörige Administratoren, im Bedarfsfall unter Zuhilfenahme externer Dienstleister, gewartet. Die Dienstleister werden verpflichtet, technische und organisatorische Maßnahmen anzuwenden, die dem Sicherheitsniveau dieser TOM im Mindesten gleichstehen.

8 Trennungskontrolle

8.1 Die Daten des Auftraggebers werden in eigenen Mandanten oder abgeschlossenen Bereichen vorgehalten.

8.2 Das Berechtigungskonzept gewährleistet, dass ausschließlich Mitarbeiter die für diesen Auftrag eingesetzt werden, Zugriff erhalten.

8.3 Die Mitarbeiter werden auf die Einhaltung der IT-Richtlinie des Unternehmens verpflichtet. Diese beinhaltet auch das Verbot, Daten aus einem Auftrag in einem anderen Auftrag in irgendeiner Weise zu verwenden.

9 Grundsätzliche Organisation

9.1 Alle Verantwortlichen für Informationssicherheit und IT-Administration sind benannt und allen Beschäftigten und Beauftragten des Unternehmens bekannt.

9.2 Richtlinien zur Informationssicherheit und IT-Sicherheit sind vorhanden und intern veröffentlicht. Sie regeln den Umgang mit Informationen hinsichtlich der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Nachweisbarkeit. Sie unterliegen der ständigen Aktualisierung sowie der Anpassung an den Stand der Technik und der Bedrohungslagen. Sie werden jährlich vom Zuständigen für IT-Sicherheit, dem Beauftragten für den Datenschutz und der Geschäftsführung auf Vollständigkeit, Aktualität und Wirksamkeit überprüft.

9.3 Richtlinien zum Datenschutz sind vorhanden und intern veröffentlicht. Sie ergänzen die IT-Richtlinien hinsichtlich betrieblicher Organisation und Besonderheiten hinsichtlich Datenschutz. Sie unterliegen der ständigen Aktualisierung sowie der Anpassung an die Rechtslage. Sie werden jährlich vom Beauftragten für den Datenschutz und der Geschäftsführung auf Vollständigkeit, Aktualität und Wirksamkeit überprüft.

9.4 Alle Personen, die Umgang mit personenbezogenen Daten haben sind auf Vertraulichkeit und rechtmäßige Verarbeitung verpflichtet. In diesem Zusammenhang erfolgt ebenfalls eine Belehrung durch den Beauftragten für den Datenschutz.

9.5 Verarbeitete Daten sind hinsichtlich ihres Schutzbedarfs eingestuft. Hier findet eine Schutzbedarfsanalyse statt, die folgendes beinhaltet: Identifizierung der zu schützenden Objekte (Daten), Bewertung der Vertraulichkeit, Analyse der möglichen Bedrohungen, Bewertung der Risiken und des möglichen Schadens. Hieraus werden die Schutzmaßnahmen festgelegt. Für personenbezogene Daten findet dazu eine Einstufung in das 5-Stufen-Modell des LDSB Niedersachsen statt.

9.6 Das Informationssicherheitskonzept ist einem kontinuierlichen Verbesserungsprozess unterworfen. Es erfolgen regelmäßige interne Audits, die Ergebnisse werden

dokumentiert. Maßnahmen aus den Auditergebnissen werden unter Berücksichtigung der Ergebnisse abgeleitet und umgesetzt.

10 Betrieblicher Datenschutzbeauftragter

10.1 Das Unternehmen hat einen betrieblichen Datenschutzbeauftragten bestellt. Dieser hat u. a. die Aufgabe die Einhaltung der Bestimmungen dieser TOM zu überwachen.

10.2 Datenschutzbeauftragter ist Boris Koppenhöfer, erreichbar per E-Mail unter datenschutz@venturisit.de.

Glossar

Betriebssystem	Steuerprogramm auf einem Rechner, das die Hardware des Rechners verwaltet und die Ausführung von Anwendungsprogrammen steuert.
Daten	Informationen, die mittels Datenverarbeitungskomponenten oder Datenverarbeitungsgeräten erstellt, gespeichert, verarbeitet, gelöscht oder transportiert werden.
Datenträger	Physikalische Einheit, die die gespeicherten Daten beinhaltet.
Datenträger, mobile	Tragbare Datenträger, Datenträger, die für den nicht-ortsfesten Einsatz geeignet sind, z. B. CD-ROM, DVD, Speicherkarte, Speicherstick, Magnetband.
E-Mail	Elektronische Post. Versenden von Text und Dateien über ein privates oder öffentliches Netz.
Firewall	Ein System aus Hard- und Software, welches die unerlaubte Kommunikation zwischen Netzen oder Netzabschnitten verhindert.
Hardware	Alle physikalischen Teile eines Rechners oder anderem Datenverarbeitungsgerätes.
Internet	Öffentliches Netz, an dem einzelne Rechner oder ganze Netzwerke angeschlossen sind.
Internetzugang	Zugang zum Internet.
Intranet	Unternehmensinternes Netz, ansonsten wie Internet.
IT	Informationstechnik, Zusammenfassung von Elektronischer Datenverarbeitung, Telekommunikation und der damit verbundenen Geräte.
IT-Richtlinie	Regelwerk zum Umgang mit der Unternehmens-IT.
Kennwort	Schlüsselwort, das den Zugriff auf IT-Systeme ermöglicht.
Server	Zentraler Rechner, der Daten und Anwendungen zur Nutzung im Netzwerk bereithält.
Software	Programme, die auf einem Rechner zur Ausführung kommen können.

Virenscanner	Software, die Dateien auf enthaltende Viren prüft, diese ggf. sperrt, verlagert oder löscht.
Virus	Programm oder Datei mit ausführbaren Anteilen, die auf einem Rechner den kompletten oder Teile des Datenbestandes verfälschen, zerstören oder an Unberechtigte weiterleiten können. Kann sich selbst durch Anhängen an Dateien oder Software verbreiten.

Anhang 2

Genehmigte Unterauftragsverhältnisse

Vertrieblich
Bentley Systems Germany GmbH
Bentley Systems Interantional Ltd.
Venturis GmbH, Ettingen
SOLAR-COMPUTER GmbH
mh-Software GmbH
Alias Ltd.

Support
Venturis GmbH, Ettingen
Polycad Software Entwicklung W. Spiegel
Bentley Systems Germany GmbH
Bentley Systems Interantional Ltd.
SOLAR-COMPUTER GmbH
mh-Software GmbH
Alias Ltd.
SC CADINTER SRL