Vereinbarung zur Auftragsverarbeitung

- nachfolgend „Leistungsvereinbarung" -

Zwischen

KalusControl Unternehmensberatung
André Kalus
Brückentor 6
36396 Steinau an der Straße

- nachfolgend „Verantwortlicher" -

und

ADDVALUE GmbH
Ernst-Barlach-Straße 20
36041 Fulda

- nachfolgend „Auftragsverarbeiter" -

- beide nachfolgend gemeinsam „Vertragsparteien" -

wird die folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Inhalt

Präambel

Die Vertragsparteien sind mit der Leistungsvereinbarung ein Auftragsverarbeitungsverhältnis gemäß EU-Datenschutz-Grundverordnung (EU-DSGVO) eingegangen. Um die Rechte und Pflichten aus dem Auftragsverarbeitungsverhältnis gemäß der gesetzlichen Verpflichtung zu konkretisieren, schließen die Vertragsparteien die nachfolgende Vereinbarung.

§ 1 Anwendungsbereich
Diese Vereinbarung findet Anwendung auf alle Tätigkeiten, die Gegenstand der Leistungsvereinbarung sind und bei deren Verrichtung Mitarbeiter des Auftragsverarbeiters oder durch den Auftragsverarbeiter nach Maßgabe dieser Vereinbarung beauftragte Dritte mit personenbezogenen Daten in Berührung kommen, für die der Verantwortliche die gemäß Art. 4 Nr. 7 EU-DSGVO verantwortliche Stelle ist oder die er im Auftrag der verantwortlichen Stelle nach Art. 28 EU-DSGVO erhebt, verarbeitet oder nutzt. Die Vereinbarung gilt unbefristet und gilt bis zur Beendigung der Inanspruchnahme der Leistungen des Auftragsverarbeiters. Etwaige Sonderkündigungsrechte bleiben davon unberührt. Diese Vereinbarung ersetzt alle bisherigen, nach den Vorgaben des BDSG, geschlossenen Vereinbarungen zur Auftragsdatenverarbeitung.

§ 2 Begriffsbestimmung
Diese Vereinbarung bezieht sich nur auf die Durchführung der technischen Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach einem vom Verantwortlichen vorgegebenen Verfahren. Dadurch begründet sich eine Auftragsverarbeitung nach Art. 28 EU-DSGVO. Eine Funktionsübertragung wird mit dieser Vereinbarung nicht getroffen.

§ 3 Konkretisierung des Auftragsinhalts
(1) Die von den Vertragsparteien vereinbarte Auftragsverarbeitung beinhaltet unter anderem:

Entwicklung einer Softwarelösung sowie Weiterentwicklung und Wartung dieser Softwarelösung.

Der detaillierte Umfang der einzelnen Leistungen ergibt sich auch aus den jeweiligen Einzelaufträgen.

(2) Folgenden Datenarten oder -kategorien sind Gegenstand der Erhebung, Verarbeitung und/oder Nutzung durch den Auftragsverarbeiter:

- Kommunikationsdaten (z. B. Telefon, E-Mail)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Vertragsabrechnungs- und Zahlungsdaten
- Auskunftsangaben von z. B. Dritten
- Buchhalterische Daten (z.B. personenbezogene Rückstellungen, Rechnungen)

(3) Der Kreis der durch den Umgang mit ihren personenbezogenen Daten Betroffenen umfasst:

- Kunden
- Beschäftigte

§ 4 Verantwortlichkeit und Weisungsbefugnis
(1) Der Verantwortliche ist für die Einhaltung der datenschutzrechtlichen Bestimmungen, insbesondere für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Er kann jederzeit die Herausgabe, Berichtigung, Löschung und Sperrung der Daten verlangen. Soweit ein Betroffener sich zwecks Ausübung seiner Recht nach EU-DSGVO Art. 12 – 23 (z.B. Löschung, Berichtigung oder Datenübertragung) unmittelbar an den Auftragsverarbeiter wendet, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.
(2) Der Auftragsverarbeiter darf Daten ausschließlich im Rahmen der Weisungen des Verantwortlichen erheben, verarbeiten oder nutzen. Eine Weisung ist die auf einen bestimmten Umgang des Auftragsverarbeiters mit personenbezogenen Daten gerichtete schriftliche Anordnung des Verantwortlichen. Die Weisungen werden zunächst durch die Konkretisierung in § 3 dieser Vereinbarung] definiert und können von dem Verantwortlichen danach in schriftlicher Form durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden. Trifft den Auftragsverarbeiter eine gesetzliche Verpflichtung oder eine rechtliche Anordnung zur Verarbeitung oder Herausgabe personenbezogener Daten für die der Verantwortliche die Verantwortung trägt informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(3) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen datenschutzrechtliche Vorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen bestätigt oder geändert wird.
(4) Verfahrensänderungen des Verarbeitungsgegenstandes dürfen nur mit dokumentierter Zustimmung des Verantwortlichen umgesetzt werden.
(5) Auskünfte an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen erteilen. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben.
(6) Der Verantwortliche führt ein Verzeichnis aller Verarbeitungstätigkeiten. Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Wunsch Informationen zur Aufnahme in das Verzeichnis zur Verfügung.
(7) Die Verarbeitung und Nutzung der Daten findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum statt. Eine Verlagerung in einen Staat außerhalb der Europäischen Union bzw. des Abkommens über den Europäischen Wirtschaftsraumes bedarf der vorherigen Zustimmung des Verantwortlichen. Die besonderen Voraussetzungen der Art. 44 ff EU-DSGVO bleiben unberührt.
(8) Weisungsbefugte Beschäftigte des Verantwortlichen sowie Weisungsempfänger des Auftragsverarbeiters sind im Anhang „Weisungsbefugte Beschäftigte und Weisungsempfänger" namentlich zu nennen. Eine Änderung der benannten Personen ist der entsprechend anderen Vertragspartei dokumentiert mitzuteilen.

§ 5 Beachtung zwingender gesetzlicher Pflichten durch den Auftragsverarbeiter
(1) Neben den vertraglichen Regelungen dieser Vereinbarung und der Leistungsvereinbarung treffen den Auftragsverarbeiter die nachfolgenden Pflichten.
(2) Der Auftragsverarbeiter stellt sicher, dass die mit der Verarbeitung befassten Mitarbeiter zur Vertraulichkeit verpflichtet und in die für sie relevanten Bestimmungen des Datenschutzes eingewiesen worden sind. Dies umfasst auch die Belehrung über die in diesem Auftragsverarbeitungsverhältnis bestehende Weisungs- und Zweckbindung.
(3) Der Auftragsverarbeiter ist nach Art. 37 EU-DSGVO verpflichtet einen Datenschutzbeauftragten zu bestellen und hat stellt dessen Kontaktdaten auf der Website jederzeit aktuell zur Verfügung. Ein Wechsel des Datenschutzbeauftragten ist dem Verantwortlichen unverzüglich mitzuteilen.
(4) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich über Kontrollen, Maßnahmen oder Ermittlungen durch die Aufsichtsbehörden.
(5) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen, die zur Durchführung einer Datenschutzfolgenabschätzung benötigt werden, auf Anforderung zur Verfügung.
(6) Weitere gesetzliche Pflichten bleiben von dieser Vereinbarung unberührt.

§ 6 Technisch-organisatorische Maßnahmen und deren Kontrolle
(1) Die Auftragsverarbeiter stellt dem Verantwortlichen eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach Art. 32 Abs. 1 EU-DSGVO vor Beginn der Verarbeitung zur Verfügung. Das im Anhang "Technische und organisatorische Maßnahmen" beschriebene Sicherheitskonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT- Systeme und Verarbeitungsprozesse beim Auftragnehmer dar. Das Sicherheitskonzept wird mit der Akzeptanz durch den Verantwortlichen zum Vertragsbestandteil.
(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das vereinbarte Sicherheitsniveau nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.
(3) Der Auftragsverarbeiter sichert dem Verantwortlichen im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu.
(4) Der Verantwortliche kann sich jederzeit zu Prüfzwecken in den Betriebsstätten des Auftragsverarbeiters zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse der für die Auftragsverarbeitung einschlägigen Datenschutzgesetze überzeugen. Eine Vorlaufzeit von 2 Wochen gilt als angemessen und muss

eingehalten werden. Wird die Prüfung in den Betriebsstätten ohne Vorankündigung unter Einhaltung der Vorlaufzeit durchgeführt erlischt die Duldungs- und Mitwirkungspflicht des Auftragsverarbeiters.

§ 7 Mitteilung bei Verstößen durch den Auftragsverarbeiter

(1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen umgehend bei schwerwiegenden Störungen seines Betriebsablaufes, bei Verdacht auf Verstöße gegen vertragliche oder gesetzliche Datenschutzbestimmungen, bei Verstößen gegen solche Bestimmungen oder anderen Unregelmäßigkeiten bei der Verarbeitung der Daten, damit dieser seiner Meldepflicht nachkommen kann.
(2) Der Auftragsverarbeiter stellt dem Verantwortlichen sämtliche relevante Informationen im Rahmen der Informationspflicht dem Betroffenen gegenüber unverzüglich zur Verfügung.

§ 8 Löschung und Rückgabe von Daten

(1) Überlassene Datenträger und Datensätze verbleiben im Eigentum des Verantwortlichen. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zu Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten des Auftragsverarbeiters erforderlich sind.
(2) Nach Abschluss der vertraglich vereinbarten Leistungen oder früher nach Aufforderung des Verantwortlichen, jedoch spätestens mit Beendigung der Leistungsvereinbarung hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände (wie auch hiervon gefertigten Kopien oder Reproduktionen), die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung des Verantwortlichen in einem dem Schutzniveau entsprechenden Verfahren zu vernichten. Gleiches gilt für Test- und Ausschussmaterial.
(3) Der Auftragsverarbeiter kann Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren. Alternativ kann er sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.
(4) Absätze 1 – 3 gelten auch im Fall einer Kündigung durch den Verantwortlichen aufgrund der Bestimmungen des § 11 dieser Vereinbarung.

§ 9 Subunternehmer

(1) Der Verantwortliche ist über die Vergabe von Aufträgen an Subunternehmer zu informieren.
(2) Wenn Subunternehmer durch den Auftragsverarbeiter eingeschaltet werden, hat der Auftragsverarbeiter sicherzustellen, dass seine vertraglichen Vereinbarungen mit dem Subunternehmer so gestaltet sind, dass das Datenschutzniveau mindestens der Vereinbarung zwischen dem Verantwortlichen und dem Auftragsverarbeiter entspricht, hinreichende Garantien für die Sicherheit der Verarbeitung vorliegen und alle gesetzlichen und vertraglichen Pflichten beachtet werden.
(3) Dem Verantwortlichen sind in der vertraglichen Vereinbarung mit dem Subunternehmer Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung einzuräumen. Ebenso ist der Verantwortliche berechtigt, auf schriftliche Anforderung vom Auftragsverarbeiter Auskunft über den wesentlichen Vertragsinhalt, die Umsetzung der datenschutzrelevanten Verpflichtungen des Subunternehmers und die Garantien zur Sicherheit der Verarbeitung zu erhalten.
(4) Zu Beginn der Verarbeitung sind die beauftragten Subunternehmer in der Anlage „Subunternehmer" aufzuführen.
(5) Nicht als Leistungen von Subunternehmen im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen und Wartungen von Datenverarbeitungsanlagen bei denen der Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen. Für die Vergabe von Nebenleistungen erteilt der Verantwortliche eine allgemeine Genehmigung.

§10 Kündigungsrecht
Der Verantwortliche kann diesen Vertrag jederzeit ohne Einhaltung von Kündigungsfristen kündigen, wenn

- der Auftragsverarbeiter gegen eine wesentliche Pflicht dieses Vertrages oder die Vorschriften der EU-DSGVO verstößt,
- der Auftragsverarbeiter eine Weisung des Verantwortlichen missachtet,
- der Auftragsverarbeiter die Ausübung von Kontrollrechten des Verantwortlichen verweigert oder nicht nur unerheblich behindert oder
- der Auftragsverarbeiter den Zutritt des Verantwortlichen oder eines entsprechend Beauftragten zu den Betriebsräumen, in denen Daten auf Grund dieses Vertrages verarbeitet bzw. genutzt werden, vertragswidrig verweigert.
- der Auftragsverarbeiter keine hinreichenden Garantien für die Sicherheit der Verarbeitung mehr bietet.

§ 11 Haftung
(1) Verantwortlicher und Auftragsverarbeiter haften im Außenverhältnis nach Art. 82 Abs. 1 EU-DSGVO für materielle und immaterielle Schäden, die einer betroffenen Person wegen eines Verstoßes gegen die EU-DSGVO erleidet. Sind sowohl der Verantwortliche als auch der Auftragsverarbeiter für einen solchen Schaden gemäß Art. 82 Abs. 2 EU-DSGVO verantwortlich, haften die Parteien im Verhältnis für diesen Schaden entsprechend ihres Anteils an der Verantwortung. Nimmt eine betroffene Person in einem solchen Fall eine Partei ganz oder überwiegend auf Schadensersatzanspruch, so kann diese von der jeweils anderen Partei Freistellung verlangen, soweit dies ihren Anteil an der Verantwortung entspricht.
Die Haftung des Auftragsverarbeiters gegenüber dem Verantwortlichen für schuldhafte Verletzungen dieses Vertrags regelt sich nach den gesetzlichen Bestimmungen.
(2) Der Auftragsverarbeiter haftet für ein Verschulden seines Unterauftragsverarbeiters und seiner Unter-Unterauftragsverarbeiter wie für eigenes Verschulden.
(3) Der Auftragsverarbeiter trägt die Beweislast dafür, dass der Schaden oder Verlust nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit Daten unter diesem Vertrag verarbeitet werden. Der Auftragsverarbeiter kommt seiner Beweispflicht nach, wenn er darlegen kann, dass er bei der Erhebung bzw. Verarbeitung der Daten die Regelungen dieses Vertrags beachtet hat und insbesondere die technischen und organisatorischen Sicherheitsmaßnahmen wie vereinbart umgesetzt hat.

§ 12 Schlussbestimmungen
(1) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich der Garantien des Auftragsverarbeiters - 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.
(2) Der Anhang „Technische und organisatorische Maßnahmen" ist Bestandteil dieser Vereinbarung.
(3) Der Anhang „Weisungsbefugte Beschäftigte und Weisungsempfänger" ist Bestandteil dieser Vereinbarung.
(4) Der Anhang „Subunternehmer" ist Bestandteil dieser Vereinbarung.

Steinau, 6.3.2020
Ort, Datum

Verantwortlicher Unterschrift, Funktion

Kalus Control Unternehmensberatung

FULDA, 05.03.2020
Ort, Datum

Auftragsverarbeiter Unterschrift, Funktion

Anlage 1:
Technisch-organisatorische Maßnahmen gemäß Art. 32 DSGVO

Dieses Dokument dient der Erfüllung gesetzlicher Anforderungen und soll eine allgemeine Beschreibung darstellen, die es ermöglicht, vorläufig zu beurteilen, ob die getroffenen Datensicherheitsmaßnahmen zu den unten angesprochenen Aspekten angemessen sind. Während der Dauer des Vertragsverhältnisses ist dieses Datensicherheitskonzept ständig an die aktuellen Gegebenheiten der Auftragsdurchführung anzupassen und zu aktualisieren. Alle Anpassungen und Änderungen in den Verfahren zur Vertragsdurchführung sind hierbei schriftlich zu dokumentieren. Das Dokument ist Bestandteil des Vertrages und dem Auftraggeber bei wesentlichen Änderungen und im Übrigen jährlich zur Durchführung der Auftragskontrolle vorzulegen.

Dokumentation der nach 32 DSGVO zu treffenden technischen und organisatorischen Maßnahmen.

1. Pseudonymisierung
Wie wird die Pseudonymisierung der Daten gewährleistet?

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in der Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren Person zugewiesen werden.

- Das System bietet die Möglichkeit, mit Pseudonymen in Stammdatenfeldern zu arbeiten.

2. Verschlüsselung
Wie wird die Verschlüsselung gewährleistet?

Die Verschlüsselung transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die "Schlüssel" genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll.

- *Nutzung von kryptografischen Tools*
- *Data Hashing*
- *Transportverschlüsselung (SSL/TLS)*
- *Nutzung von VPN*

3. Fähigkeit der Vertraulichkeit
Wie wird die Fähigkeit der Vertraulichkeit der Daten dauerhaft gewährleistet?

Vertraulichkeit heißt, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind.

- *Physische Zugangskontrolle*
  Unsere Server und Datenbanksysteme sind in einem Rechenzentrum entsprechend der ISO 27001-Zertfzierung installiert. Somit ist kein unbefugter Zugang zu diesen
- *Datenverarbeitungseinrichtungen möglich.*
- *Zutritt nur für befugte Personen (Betriebsangehörige)*
- *Berechtigungsausweise (RFID) oder Schlüssel*

- *Firmenfremde sind nicht zugangsberechtigt und werden wie Besucher behandelt*
- *Anwesenheitsaufzeichnungen*
- *Besucherausweise*
- *Definierte Sicherheitsbereiche*
- *RFID-gesicherter Eingang wird auch für Lieferungen genutzt*
- *Türen sind gesichert durch elektrische Türschließer und Ausweisleser*
- *Sicherheitstüren und/oder -fenster*
- *Mit Beendigung der Arbeitsverhältnisse werden die Zutrittsberechtigungen der Mitarbeiter entzogen.*
- *Kundendaten sind physisch getrennt von Entwicklungsdaten und Testdaten und innerhalb der Systeme nochmals logisch getrennt.*
- *Die Entwicklungsdaten sind jeweils auf getrennten Servern gespeichert (physische Trennung).*
- *Es wird die Mandantentrennung eingesetzt. Die Daten je Kunde werden logisch getrennt transferiert, verarbeitet und gespeichert. Zugang zu den Daten ist nur den Mitarbeitern gewährt, die für die Datenverarbeitung zuständig sind.*

weitere Maßnahmen:

- *Spezielle Schutzvorkehrungen für den Serverraum am Standort*
- *Elektronische Zugangskontrolle*
- *Passwortrichtlinie nach Stand der Technik*
- *Log-Screen nach kurzer Inaktivität*
- *Berechtigungskonzept nach dem Need-to-Know-Prinzip*
- *Zusätzlicher Log-In für bestimmte Anwendungen*
- *E-Mail-Versand verschlüsselter oder passwortgeschützter Dateianhänge*
- *Verschlüsselung von Datenträgern*
- *VPN (Virtual Private Network)*
- *Gesichertes WLAN / Gäste-WLAN*
- *SSL-Verschlüsselung bei Web-Access*
- *Regelmäßige Schulungs- und Sensibilisierungsmaßnahmen*
- *Mitarbeiterverpflichtung auf Vertraulichkeit*
- *Vertragsgestaltung mit Dienstleistern*
- *Firewall*
- *Virenschutz*
- *Sicherheitsupdates werden regelmäßig installiert.*
- *Protokollierung sämtlicher Zugriffe*

4. Fähigkeit der Integrität

Wie wird die Fähigkeit der Integrität der Daten dauerhaft gewährleistet?

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. Maßnahmen sollten ergriffen werden, die die Beschädigung/Veränderung der geschützten Daten während der Verarbeitung oder Übertragung verhindern.

- *Interne Zugangskontrolle*
- *Transportverschlüsselung bei Datenübermittlungen*
- *Der Datentransfer erfolgt immer verschlüsselt oder kryptisch auf den vereinbarten Übertragungswegen.*
- *Kontrolle der Dateneingabe*
- *Funktionelle Verantwortlichkeiten / Rollenkonzept*
- *Vertreterregelung*
- *Berechtigungskonzept nach dem Need-to-Know-Prinzip*

- *Die personenbezogenen Daten werden nur innerhalb des geschlossenen Systems von autorisierten Usern bearbeitet.*
- *Protokollierung von Zugriffen: Lesen, kopieren, ändern oder löschen*

5. Fähigkeit der Verfügbarkeit
Wie wird die Fähigkeit der Verfügbarkeit der Daten dauerhaft gewährleistet?

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

- *Es erfolgt die aktive Überwachung sämtlicher Systeme während der Arbeitszeit.*
- *Die unternehmensrelevanten Daten werden täglich gesichert.*
- *Das Verfahren für Wiederherstellung und Hoch-/Herunterfahren der Systeme wird regelmäßig dokumentiert, geprüft und getestet.*
- *Verfügbarkeitskontrolle*
- *Backup-Konzeption*
- *Unterbrechungsfreie Stromversorgung (USV)*
- *Virenschutz*
- *Firewall*
- *Meldeverfahren*
- *Monitoring*
- *Notallplanung*
- *Spiegeln von Festplatten*
- *Klimaanlagen*
- *Brand- und Löschwasserschutz*
- *geeignete Archivierungsräumlichkeiten*

6. Fähigkeit der Belastbarkeit
Wie wird die Fähigkeit der Belastbarkeit der Daten dauerhaft gewährleistet?

Systeme sind belastbar, wenn sie so widerstandsfähig sind, dass ihre Funktionsfähigkeit selbst bei starkem Zugriff bzw. starker Auslastung gegeben ist.

- *Monitoring*
- *Managed Services*
- *Clusterfähige Systeme*

7. Wiederherstellbarkeit der Verfügbarkeit und des Zugangs
Wie wird gewährleistet, dass personenbezogene Daten nach Sicherheitsvorfällen rasch wieder verfügbar und zugänglich sind?

- *Durch unsere hochverfügbare technische Clusterumgebung ist eine rasche Wiederherstellung und die Verfügbarkeit der Systeme und Daten sichergestellt.*
- *Backup-Verfahren*
- *Unterbrechungsfreie Stromversorgung (USV)*
- *Vertretungsregelungen*

8. Verfahren zur regelmäßigen Überprüfung
Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?

- *Datenschutzmanagement*
- *Reaktionsmanagement*

- *Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen bei Eigenentwicklungen*
- *Auftrags- oder Vertragskontrolle*

9. Unrechtmäßiger Zugang zu personenbezogenen Daten
Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?

- *Individueller Log-In und Kennwortverfahren*
- *Zusätzlicher Log-In für bestimmte Anwendungen*
- *Automatsche Sperrung der Clients (Zeitablauf)*
- *Verwaltung von Berechtigungen*
- *Dokumentation von Berechtigungen*

10. Verarbeitung personenbezogener Daten nur nach Anweisung
Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden?

- *Mitarbeiter sind zu Verhaltensregeln verpflichtet*
- *Definierte Weisungsempfänger*
- *Implementierung unternehmensinterner Datenschutz-Richtlinien*
- *Verpflichtung der Mitarbeiter auf Vertraulichkeit*
- *Schulungen aller zugriffsberechtigten Mitarbeiter*
- *Rollenkonzept*
- *Dokumentation von Verantwortlichkeiten*

Anlage 2:
Weisungsbefugte Beschäftigte und Weisungsempfänger

Weisungsbefugte Beschäftigte		
Name	**Abteilung/Position**	**Kontakt**
André Kalus	KalusControl	andre.kalus@kaluscontrol.de
Mensur Memic	KalusControl	mensur.memic@kaluscontrol.de
Roccina Schröder	KalusControl	roccina.schroeder@kaluscontrol.de
Eileen Gärtner	KalusControl	eileen.gaertner@kaluscontrol.de
Patricia Kley	KalusControl	patricia.kley@kaluscontrol.de
Anita Kalus	KalusControl	anita.kalus@kaluscontrol.de
Jana Noll	KalusControl	jana.noll@kaluscontrol.de

Weisungsempfänger		
Name	**Abteilung/Position**	**Kontakt**
Roman Geis	Geschäftsführer	roman.geis@addvalue.de
Melanie Müller	Projektleitung	Melanie.mueller@addvalue.de
Erik Kothe	Entwicklung	Erik.kothe@addvalue.de
Tom Meiselbach	Entwicklung	Tom.meiselbach@addvalue.de

Anlage 3:
Subunternehmer

Subunternehmer	Kontakt	Tätigkeit
Global Business IT GmbH Johannesberger Straße 2 36041 Fulda	denis.stolz@global-bit.de	Betrieb der IT-Infrastruktur