Vertrag über die Auftragsverarbeitung i. S. d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

Auftraggeber:	**Auftragnehmer:**
Firma Straße, Nr. PLZ, Ort	Spree systems GmbH Oderstr. 45 14513 Teltow
vertreten durch den Geschäftsführer	vertreten durch den Geschäftsführer
Name GF	Herrn Michael Wick

Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Hauptvertrag in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

§ 1. Gegenstand, Dauer und Spezifizierung der Verarbeitung

1.1 Gegenstand der Verarbeitung ist die Installation, Konfiguration, Integration, Instandhaltung und Wartung von IT-Systemen sowie Fehlersuche und Fehlerbehebung per Fernzugriff oder vor Ort.

1.2 Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Wartungsvertrag vom 00.00.0000 (im Folgenden „Hauptvertrag“) und/ oder auf der jeweiligen Beauftragung zu Lieferungen und Leistungen im Einzelfall.

1.3 Im Einzelnen sind insbesondere die in Anlage 1 genannten Daten Bestandteil der Datenverarbeitung:

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüberhinausgehende Verpflichtungen ergeben.

1.4 Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

1.5 Die Verarbeitung erfolgt ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum. Jede Verlagerung der Dienstleistung oder von Teilarbeiten in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt werden.

§ 2. Anwendungsbereich und Verantwortlichkeit

2.1 Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DSGVO).

2.2 Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

§ 3. Pflichten des Auftragnehmers

3.1 Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DSGVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

3.2 Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird die in der **Anlage 4** beschriebenen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz--Grundverordnung (Art. 32 DSGVO) genügen.

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. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen der technischen und organisatorischen Maßnahmen sind zu dokumentieren und mit dem Auftraggeber abzustimmen.

3.3 Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO sowie bei der Einhaltung der in Art. 33 bis 36 DSGVO genannten Pflichten.

3.4 Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere 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 verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

3.5 Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.
Der Auftragnehmer trifft die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab.

3.6 Der Datenschutzbeauftragte und Ansprechpartner beim Auftragnehmer für im Rahmen des Vertrages anfallende Datenschutzfragen ist:

Herr Jan Wandrey
Motzener Straße 25
12277 Berlin
kontakt@agidat.de

Änderungen des Datenschutzbeauftragten werden dem Auftraggeber unverzüglich mitgeteilt.

3.7 Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 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 und diese entsprechend zu dokumentieren.

3.8 Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart.

In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.

3.9 Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen.

3.10 Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

3.11 Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 2** benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

3.12 Der Zugriff auf Daten per Fernzugriff erfolgt nur mit vorheriger Zustimmung des Auftraggebers. Der Auftragnehmer stellt in diesem Fall sicher, dass die Maßnahmen gemäß Art. 32 der DSGVO entsprechend erfüllt sind.

§ 4. Pflichten des Auftraggebers

4.1 Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

4.2 Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, gilt §3 Abs. 10 entsprechend.

4.3 Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen. Diese sind in **Anlage 2** aufgeführt.

§ 5. Anfragen betroffener Personen

5.1 Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung, oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 6. Nachweismöglichkeiten

6.1 Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

6.2 Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

6.3 Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

§ 7. Vergütung

7.1 Eine Vergütung des Auftragnehmers wird gesondert vereinbart.

§ 8. Unterauftragsverhältnisse (weitere Auftrags Verarbeiter)

8.1 Die Beauftragung von Unterauftragnehmern als weiteren Auftrags Verarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

8.2 Ein zustimmungspflichtiges Unterauftragnehmer Verhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

8.3 Die zum Zeitpunkt der Vertragsschließung bekannten Unterauftragnehmer sind mit der Beschreibung Ihrer Leistungen bzw. Teilleistungen in Anlage 3 aufgeführt.

8.4 Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer holt der Auftragnehmer die Zustimmung des Auftraggebers ein, wobei diese nicht ohne wichtigen datenschutzrechtlichen Grund verweigert werden darf.

8.5 Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund – gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben.

8.6 Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

§ 9. Haftung und Schadensersatz

9.1 Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung.

§ 10. Informationspflichten, Schriftformklausel, Rechtswahl

10.1 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. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher « im Sinne der Datenschutz-Grundverordnung liegen.

10.2 Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, 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.

10.3 Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

10.4 Es gilt deutsches Recht.

Anlagen

Anlage 1:

Kategorien von Daten und betroffenen Personen, Art und Zweck der Datenverarbeitung

Anlage 2:

Weisungsberechtigte Personen

Anlage 3:

Unterauftragnehmer mit Beschreibung der Leistungen / Teilleistungen

Anlage 4:

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (vgl. auch § 3 Abs. 2)

Unterschriften

Ort, Datum (Auftraggeber)	Ort, Datum (Auftragnehmer)

Anlage 1:

Kategorien von Daten und betroffenen Personen, Art und Zweck der Datenverarbeitung

Art der Daten:	Adressdaten, Kommunikationsdaten, Userdaten, Projektdaten, Bild- und Tondaten, IT-Nutzungsdaten, Zeiterfassungsdaten, Vertragsdaten, Maschinendaten, Funktionsbezeichnung, Bankverbindungsdaten
Art und Zweck der Datenverarbeitung:	Angebot, Auftrag, Bereitstellung, Abrechnung, Installation, Konfiguration, Integration, Instandhaltung, Wartung von IT-Systemen sowie Fehlersuche und Fehlerbehebung per Fernzugriff oder vor Ort.
Kategorien betroffener Personen:	Kunden, Mitarbeiter (Leiharbeiter, Praktikanten, Werkstudenten, Auszubildende, etc.), Lieferanten, Dienstleister und weitere für den Kunden tätige Personen

Grundsätzlich werden nur Daten erhoben und verarbeitet, die für den Zweck, die Durchführung sowie die Abrechnung von Aufträgen notwendig sind. Daten werden nur im notwendigen Umfang erhoben und verarbeitet.

Die Daten werden nur an Dritte weitergegeben, wenn dies für den Zweck, die Durchführung sowie die Abrechnung notwendig ist (z.B. Kunden- und Kommunikationsdaten für die Erstellung von Lizenzen, Erstellung von Benutzer-Accounts, Abwicklung von Garantieansprüchen, etc.).

Anlage 2:

Weisungsberechtigte Personen

Weisungsberechtigte Personen des Auftraggebers:

Name, Vorname	Telefonnummer	E-Mail-Adresse

Weisungsberechtigte Personen des Auftragnehmers

Name, Vorname	Telefonnummer	E-Mail-Adresse
Michel, George	03328 33878-12	george.michel@spreesystems.de
von Ahlen, Oliver	03328 33878-14	oliver.von.ahlen@spreesystems.de
Polzin, Dennis	03328 33878-11	dennis.polzin@spreesystems.de
Wick, Michael	03328 33878-0	michael.wick@spreesystems.de

Anlage 3:

Beauftragte Unterauftragnehmer, Beschreibung der Teilleistungen

Liste der beauftragten Unterauftragnehmer:

Name, Anschrift des beauftragten Unterauftragnehmers	**Beschreibung der Leistungen/ Teilleistungen**
TeamViewer Germany GmbH Jahnstr. 30 73037 Göppingen	Herstellung von Verbindungen zum Zwecke des Fernzugriffs auf entfernte Computersysteme
1Password (AgileBits) Suite 303, 49 Spadina Ave, Toronto, Ontario, M5V 2J1, Canada https://1password.com/de/legal/gdpr/	Speicherung von Passwörtern und Zugängen in einem verschlüsselten Passwort-Tresor
Microsoft Corporation One Microsoft Way Remond, WA 98052-6399 USA https://www.microsoft.com/de-de/trust-center/privacy/gdpr-overview	Bereitstellung von Plattformen für Cloud Services und Serverinfrastrukturen, Bereitstellung von Softwareprodukten und Services.
Jens Erlebach Im Winkel 1 14467 Potsdam	Unterstützung bei Supportleistungen für Kunden (remote und vor Ort)
Björn Mehler Wietstocker Dorfstr. 1 14974 Ludwigsfelde	Unterstützung bei Supportleistungen für Kunden (remote und vor Ort)

Die genannten Unterauftragnehmer unterliegen denselben Datenschutzpflichten, wie der Auftragnehmer. Die Überprüfung der technischen und organisatorischen Maßnahmen der Unterauftragnehmer obliegt dem Datenschutzbeauftragten des Auftragnehmers. Er ist auch bei der Auswahl der beauftragten Firmen/ Unternehmer auf Anfrage beteiligt.

Der Auftraggeber stimmt dem Einsatz der oben genannten Unterauftragnehmer unter der Maßgabe der ordentlichen Überprüfung der technischen und organisatorischen Maßnahmen bis auf Widerruf zu.

Anlage 4:

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Nr.	Gebiet	Beschreibung
0	**Organisation**	
	Wie ist die Umsetzung des Datenschutzes organisiert?	Ein externer Datenschutzbeauftragter wird zur Wahrnehmung der Beratungs- und Kontrollfunktionen nach DSGVO eingesetzt.
	Name und die Kontaktdaten des Datenschutzbeauftragten.	Jan Wandrey Motzener Straße 25 12277 Berlin kontakt@agidat.de Tel: +49 30 720102230
	In welcher Form werden die Mitarbeiter auf die Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen geschult, die für diese Verarbeitung in Anwendung kommen?	Das Schulungskonzept beinhaltet sowohl eine Datenschutzunterweisung bei Beginn der Tätigkeit, als auch eine konstante Sensibilisierung durch Datenschutznewsletter, fachbezogene Webschulungen und persönliche Sensibilisierung durch den externen Datenschutzbeauftragten.
	Sind die Verarbeitungen hinsichtlich datenschutzrechtlicher Zulässigkeit dokumentiert?	Im Rahmen des Verzeichnisses von Verarbeitungstätigkeiten sind die Datenströme dokumentiert und die Zulässigkeit der Verarbeitung und Nutzung nach DSGVO nachgewiesen. Für jede Verarbeitung findet eine Risikobewertung statt.
1	**Vertraulichkeit (Art. 32 Abs. 1 lit. b DC-GVO)**	
1.1	**Zutrittskontrolle**	
	Wie werden die Gebäude, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Das Gebäude ist mit einer elektronischen Sicherheits-Schließanlage ausgerüstet. Betriebsfremde Personen werden am Haupteingang persönlich in Empfang genommen.
	Wie werden die Räume / Büros, in denen die Verarbeitung stattfindet, vor unbefugtem Zutritt gesichert?	Die Räume werden durch ein elektronisches Sicherheitsschließsystem gesichert. Der Zutritt ist durch ein Berechtigungskonzept eingeschränkt. Der Zutritt zum Serverraum

Nr.	Gebiet	Beschreibung
		wird elektronisch dokumentiert und ist nur wenigen ausgewählten Mitarbeitern gestattet.
	Wie werden die umgesetzten Zutrittskontrollmaßnahmen auf Tauglichkeit geprüft?	Im Rahmen der Kontrollen durch den externen Datenschutzbeauftragten werden auch die Zutrittskontrollmaßnahmen überprüft.
1.2	**Zugangskontrolle**	
	Wie erfolgt die Vergabe von Benutzerzugängen?	Benutzerzugänge werden selektiv und nur nach Genehmigung durch die IT-Abteilung, abgesprochen mit der Geschäftsführung, vergeben. Rechtevergabe und Änderung sind dokumentiert. Zugriff auf kaufmännische Dokumente und Kommunikationsinformationen sind durch Passwörter geschützt.
	Wie wird die Gültigkeit von Benutzerzugängen überprüft?	Eine regelmäßige Revision der vergebenen Rechte ist Teil der Prüfungen der Maßnahmen und wird zusammen mit dem externen Datenschutz-beauftragten durchgeführt und von diesem dokumentiert.
	Wie werden Benutzerzugänge inkl. Antragstellung, Genehmigungsverfahren etc. dokumentiert?	Die Anlage und Veränderung von Benutzerzugängen wird im firmeneigenen Ticketsystem dokumentiert.
	Wie wird sichergestellt, dass die Anzahl von Administrationszugängen ausschließlich auf die notwendige Anzahl reduziert ist und nur fachlich und persönlich geeignetes Personal hierfür eingesetzt wird?	Die Entscheidungen zur Rechtevergabe halten sich streng an die entsprechenden Vorgaben, Datenvermeidung und Datensparsamkeit.
	Ist ein Zugriff auf die Systeme / Anwendungen von außerhalb des Unternehmens möglich und wie ist der Zugang gestaltet?	Fernwartungszugänge sowie Zugriffe auf Daten erfolgen verschlüsselt, per VPN mit Zertifikat, welches zuvor lokal installiert werden muss und ausschließlich über firmeneigene Geräte (z.B. Handy als Access Point). Die Anzahl der Berechtigten und Art der Berechtigung wird auf das nötigste begrenzt.
1.3	**Zugriffskontrolle**	
	Wie wird erreicht, dass Passwörter nur dem jeweiligen Benutzer bekannt sind?	Die Passwörter werden vom jeweiligen Mitarbeiter selbst vergeben. Die strengen Systemvoreinstellungen zwingen zu einer hohen Passwortkomplexität. Passwörter werden nicht gespeichert.

Nr.	Gebiet	Beschreibung
	Wie werden die Verarbeitungsanlagen vor unbefugtem Zugriff geschützt?	Es wird ein Passwortschutz verwendet und es gibt ein Berechtigungskonzept. Gegen Zugriffe von außen ist das System durch eine Firewall geschützt.
	Welche Anforderungen werden an die Komplexität von Passwörtern gestellt?	Die Vorgaben Empfehlungen des BSI dienen als Vorbild für die o.g. Systemeinstellungen (mind. 8 Zeichen, mind. ein Groß- und ein Kleinbuchstabe, mind. eine Zahl, mind. ein Sonderzeichen)
	Wie wird gewährleistet, dass der Benutzer sein Passwort regelmäßig ändern kann / muss?	Systemeinstellungen, Gruppenrichtlinie (Passwortänderung spätestens alle 90 Tage)
	Welche organisatorischen Vorkehrungen werden zur Verhinderung von unberechtigten Zugriffen auf personenbezogene Daten am Arbeitsplatz getroffen?	Schulung und Sensibilisierung der Mitarbeiter, Arbeitsplätze werden vor dem verlassen gesperrt, bzw. heruntergefahren.
	Wie wird sichergestellt, dass Zugriffsberechtigungen anforderungsgerecht und zeitlich beschränkt vergeben werden?	Siehe auch Punkt Vergabe von Benutzerzugängen Punkt 1.2; die IT-Abteilung prüft in regelmäßigen Abständen die Rechte und Benutzerstruktur
	Wie erfolgt die Dokumentation von Zugriffsberechtigungen?	Regelmäßige Reports aus dem Berechtigungssystem
	Wie wird sichergestellt, dass Zugriffsberechtigungen nicht missbräuchlich verwendet werden?	Anlassbezogene und Anlasslose Durchsicht der Systemprotokolle durch die IT-Abteilung
	Wie lange werden Protokolle aufbewahrt? Wer hat Zugriff auf die Protokolle und wie oft werden sie ausgewertet?	Keine festgelegten Fristen, meist Systemparameter. Auswertung ausschließlich durch befugte Personen.
1.4	**Trennungskontrolle**	
	Wie wird sichergestellt, dass Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt voneinander verarbeitet werden?	Physische oder logische Trennung der Daten
1.5	**Pseudonymisierung**	
	Welche organisatorischen Maßnahmen wurden getroffen, damit die Verarbeitung	Alle mit der Verarbeitung von personenbezogenen Daten betrauten Personen wurden entsprechend verpflichtet. Ein Datenschutzkonzept wird im Unternehmen

Nr.	Gebiet	Beschreibung
	personenbezogener Daten gesetzeskonform erfolgt?	eingesetzt und ist allen Mitarbeitern bekannt gemacht. Das Schulungskonzept beinhaltet sowohl eine Datenschutzunterweisung bei Beginn der Tätigkeit, als auch eine konstante Sensibilisierung durch Datenschutznewsletter, fachbezogene Webschulungen und persönliche Sensibilisierung durch den externen Datenschutzbeauftragten.
	Wie werden personenbezogene Daten verarbeitet /aufbewahrt, so dass diese nicht den betroffenen Personen zugeordnet werden können?	Daten, die nicht mehr benötigt werden, werden gelöscht, bzw. gesperrt, sofern diese Aufbewahrungsfristen unterliegen. Auf gesperrte Datensätze haben nur bestimmte verantwortliche Personen Zugriff.
2	**Integrität (Art. 32 Abs. 1 lit. b DS-GVO)**	
2.1	**Weitergabekontrolle**	
	Wie gewährleisten Sie die Integrität und Vertraulichkeit bei der Weitergabe von personenbezogenen Daten?	Es werden keine personenbezogenen Daten weitergegeben. Verpflichtung von Subunternehmen durch AV-Vertrag.
	Werden Verschlüsselungssysteme bei der Weitergabe von personenbezogenen Daten eingesetzt und wenn ja, welche?	n/a
	Wie wird die Weitergabe personenbezogener Daten dokumentiert?	n/a
	Wie wird der unberechtigte Abfluss von personenbezogenen Daten durch technische Maßnahmen beschränkt?	Eine strikte Rechtevergabe sichert die Daten vor unberechtigtem Zugriff.
	Gibt es ein Kontrollsystem, das einen unberechtigten Abfluss von personenbezogenen Daten aufdecken kann?	Dies wird im Rahmen der Kontrollen unter Punkt 1 mit geprüft.
2.2.	**Eingabekontrolle**	
	Welche Maßnahmen werden ergriffen, um nachvollziehen zu können, wer wann und wie lange auf Applikationen zugegriffen hat?	n/a
	Wie ist nachvollziehbar, welche Aktivitäten auf den entsprechenden Applikationen durchgeführt wurden?	Rollen-/Rechtekonzepte und diverse Lizenzmodelle mit unterschiedlichen Berechtigungskonzepten

Nr.	Gebiet	Beschreibung
	Welche Maßnahmen werden ergriffen, damit die Verarbeitung durch die Mitarbeiter nur gemäß den Weisungen des Auftraggebers erfolgen kann?	Zugriffskontrolle anhand des Rollen-/ Rechtekonzepts zur ordnungsgemäßen Datenbearbeitung und Speicherung
	Welche Maßnahmen werden getroffen, damit auch Unterauftragnehmer ausschließlich im vereinbarten Umfang personenbezogene Daten des Auftraggebers verarbeiten?	Sämtliche Unterauftragnehmer unterliegen den gleichen Vorgaben wie der Auftragnehmer. Entsprechende Verträge sind geschlossen. Die Pflichten zur Überprüfung der Unterauftragnehmer übernimmt der Datenschutzbeauftrage des Unternehmens. Er ist auch bei der Auswahl der beauftragten Firmen auf Anfrage beteiligt.
	Wie wird die Löschung / Sperrung von personenbezogenen Daten am Ende der Aufbewahrungsfrist bei Unterauftragnehmern sichergestellt?	Festlegung durch Vertragsbindung, bei Wegfall des Zweckes ist ebenfalls eine Löschung der Daten indiziert.
3	**Verfügbarkeit und Belastbarkeit**	
3.1.	**Verfügbarkeitskontrolle**	
	Wie wird gewährleistet, dass die Datenträger vor elementaren Einflüssen (Feuer, Wasser, elektromagnetische Abstrahlung etc.) geschützt sind?	Gesicherte Daten sind räumlich getrennt von Produktivdaten; ältere Backup Medien werden räumlich getrennt sicher verwahrt.
	Welche Schutzmaßnahmen werden zur Bekämpfung von Schadprogrammen eingesetzt und wie wird deren Aktualität gewährleistet?	Ständig aktuelle Virenscanner und Spamfilter finden Einsatz. Die Systeme werden regelmäßig upgedatet.
	Wie wird sichergestellt, dass nicht mehr benötigte bzw. defekte Datenträger ordnungsgemäß entsorgt werden?	Physische Löschung bei funktionsfähigen Datenträgern und mechanische Zerstörung defekter Datenträger vor der Entsorgung
3.2.	**Wiederherstellbarkeit**	
	Welche organisatorischen und technischen Maßnahmen werden getroffen, um auch im Schadensfall die Verfügbarkeit von Daten und Systemen schnellstmöglich zu gewährleisten? (rasche Wiederherstellbarkeit nach Art. 32 Abs.1 lit.c DS-GVO)	Sicherung nach Backupkonzept, Eingerichtetes mehrstufiges-stufiges Backup-Verfahren. Wiederherstellung der Datenstände der vergangenen 7 Tage auf Anforderung; Wiederherstellung älterer Datenstände durch Einspielen von Backup-Medien.

Nr.	Gebiet	Beschreibung
4.	**Verfahren zur regelmäßigen Überprüfung, Bewertung, Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO, Art. 25 Abs. 1 DS-GVO)**	
	Welche Verfahren gibt es zur regelmäßigen Bewertung/Überprüfung, um die Sicherheit der Datenverarbeitung zu gewährleisten (Datenschutz-Management)?	Der externe Datenschutzbeauftragte überprüft regelmäßig und teilweise auch unangekündigt, die Einhaltung der technisch-organisatorischen Maßnahmen.
	Wie wird auf Anfragen bzw. Probleme reagiert (Incident-Response-Management)?	Einsatz eines Ticketsystems
	Welche datenschutzfreundlichen Voreinstellungen gibt es (Art. 25 Abs. 2 DS-GVO)?	Keine Vorbelegung durch Haken; bei Anmeldung im System erfolgen keine Vorbelegungen; Benutzer muss die Anmeldeinformationen jeweils eintragen
4.1	**Auftragskontrolle**	
	Welche Vorgänge gibt es zur Weisung bzw. dem Umgang mit der Auftragsdatenverarbeitung (Datenschutz-Management)?	Das Vertragswerk wurde entsprechend den neuen Richtlinien zur Auftragsdatenverarbeitung gestaltet. Der externe Datenschutzbeauftragte nimmt entsprechende Beratungs- und Kontrollpflichten wahr.