Vereinbarung zur Auftragsverarbeitung nach EU-Datenschutz-Grundverordnung (DS-GVO)

Zwischen

webmaster@mkbug.de

– Auftraggeber –

und

Buhl Data Service GmbH

Am Siebertsweiher 3/5

57290 Neunkirchen

– Auftragnehmer –

über Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO). Etwaige zwischen den Parteien zur alten Rechtslage geschlossenen Verträge (Auftragsdatenverarbeitung gemäß § 11 BDSG) werden beendet und durch diesen Vertrag ersetzt.

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Hauptvertrag zur Leistungserbringung in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag zur Leistungserbringung in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten. Bei mehreren Hauptverträgen umfasst die Vereinbarung alle Auftragsverarbeitungen des Auftragnehmers, für die ein jeweiliger Vertrag zur Leistungserbringung mit dem Auftraggeber besteht (nach Login abrufbar im Kundenkonto des Auftraggebers unter www.buhl.de). Sollte der Auftraggeber in seiner Funktion als Berufsgeheimnisträger diesen Auftragsverarbeitungsvertrag abschließen, so gilt zusätzlich unsere Verschwiegenheitsverpflichtung, abrufbar unter https://www.buhl.de/go/41244.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Hauptvertrag zur Leistungserbringung ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

1. Art der Daten:
    - Art der personenbezogenen Daten sind alle Arten personenbezogener Daten, die der Auftragnehmer im Auftrag des Kunden verarbeitet. Insbesondere sind dies:

        - Personenstammdaten (z.B. Name und Anschrift, Bild)
        - Kommunikationsdaten (z.B. Telefon, E-Mail)
        - Vertragsstammdaten (z.B. Abrechnungs- und Zahlungsdaten, Bankverbindung)
        - Kundenhistorie
        - Nutzungsdaten
        - Kenndaten (z.B. Steueridentifikationsnummer, Ausweisnummer)
    - Hiervon umfasst sein können auch besondere Kategorien personenbezogener Daten.

2. Art und Zweck der Datenverarbeitung
    - Die Art der Verarbeitung umfasst alle Arten von Verarbeitungen im Sinne der DS-GVO.
    - Zwecke der Verarbeitung sind alle zur Erbringung der vertraglich vereinbarten Leistung erforderlichen Zwecke. Dies sind insbesondere:
        - Bereitstellung von IT-Infrastruktur, sowie Speicherung und Sicherung der Daten im Rahmen der Cloud-Hosting-Dienste des Auftragnehmers
        - Diagnose und Wartung per Fernzugriff, bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann.
3. Kategorien betroffener Personen
    - Kategorien betroffener Personen sind insbesondere
        - Kunden, Interessenten des Auftraggebers
        - Beschäftigte des Auftraggebers (z.B. Ansprechpartner)
        - Personen, deren Daten der Auftragnehmer im Auftrag verarbeitet (z.B. Mieter, Vereinsmitglieder, Lieferanten)

Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrages zur Leistungserbringung, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüberhinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag zur Leistungserbringung und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieser Vereinbarung 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 DS-GVO).
2. Die Weisungen werden anfänglich durch den Hauptvertrag zur Leistungserbringung festgelegt und können vom Auftraggeber danach schriftlich oder in Textform (z.B. E-Mail) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert,

ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Hauptvertrag zur Leistungserbringung nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform vom Auftraggeber zu bestätigen.

§ 3 Pflichten des Auftragnehmers

1. Der Auftragnehmer darf personenbezogene Daten, die Gegenstand des Auftrags sind, nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor und dessen Voraussetzungen werden gewahrt.

2. 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. Der Auftragnehmer wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz- Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat insbesondere technische und organisatorische Maßnahmen zu treffen, gemessen am Risiko für die Rechte und Freiheiten der betroffenen Personen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Die Einzelheiten dieser technischen und organisatorischen Maßnahmen ergeben sich aus dem **Anhang** dieser Vereinbarung. Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Diese sind vom Auftragnehmer entsprechend zu dokumentieren. Dabei darf das Sicherheitsniveau der im **Anhang** genannten Maßnahmen nicht unterschritten werden.

4. Der Auftragnehmer unterstützt den Auftraggeber angemessen bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruchs im Rahmen seiner Möglichkeiten zu unterstützen.

5. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Beschäftigten 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 zuständigen Personen zur Vertraulichkeit verpflichtet haben und diese Vertraulichkeitsverpflichtung auch nach Beendigung des Auftrages fortbesteht.

6. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Eine Meldung von Datenschutzverletzungen muss mindestens enthalten:

    - eine Beschreibung des Vorfalls, soweit möglich mit Angabe der Art der Verletzung des Schutzes personenbezogener Daten, Angabe der Kategorien und der

ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze

- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
- eine Beschreibung der wahrscheinlichen Folgen des gemeldeten Vorfalls, eine Beschreibung der ergriffenen Maßnahmen zur Behebung und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

7. Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Hauptvertrages zur Leistungserbringung anfallende Datenschutzfragen.
8. Der Auftragnehmer gewährleistet, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen (Art. 32 Abs. 1 lit. d DS-GVO).
9. Während der Vertragslaufzeit berichtigt oder löscht der Auftragnehmer auf Weisung des Auftraggebers die vertragsgegenständlichen Daten (mit Ausnahme von routinemäßig gesicherten Kopien in Back-Ups).
   In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe. Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Hauptvertrag zur Leistungserbringung bereits vereinbart.
10. Daten, Datenträger sowie sämtliche Dokumente sind nach Auftragsende auf Verlangen (schriftlich oder in Textform) des Auftraggebers entweder herauszugeben, sofern sie im Eigentum des Auftraggebers sind, oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.
11. Der Auftragnehmer bietet dem Auftraggeber die Möglichkeit, Daten der Cloud-Anwendung zu exportieren. Diese exportierbaren Daten können zum Wechsel zu Diensten von Drittanbietern oder zu einer Infrastruktur in den eigenen Räumlichkeiten des Auftraggebers verwendet werden. Der Auftraggeber hat den Wechsel 2 Monate vorher in Textform anzukündigen. Die Datenübertragung erfolgt spätestens nach Ablauf einer Übergangsfrist von höchstens 30 Kalendertagen ab Ablauf der zweimonatigen Ankündigungsfrist. Der Auftragnehmer behält sich das Recht vor, den Export von Daten zu beschränken, die die Sicherheit der Dienste oder das geistige Eigentum des Auftragnehmers gefährden könnten. Der Auftragnehmer leistet angemessene Unterstützung beim Export der Daten. Der Datenexport ist ohne zusätzliche Kosten möglich. Der Vertrag gilt als beendet, wenn der Wechsel erfolgreich vollzogen ist oder die Daten nach Ablauf der zweimonatigen Ankündigungsfrist auf Verlangen des Auftraggebers gelöscht wurden. Sollte der Wechsel des Auftraggebers zu einer vorzeitigen Vertragsbeendigung führen, hat der Auftraggeber die bis zum regulär nächstmöglichen Vertragsende vereinbarten Kosten zu tragen.

§ 4 Pflichten des Auftraggebers

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

2. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DS-GVO, gilt §3 Abs. 4 entsprechend.

§ 5 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Anträgen gemäß Art. 15-21 DS-GVO an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen und leitet den Antrag an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung dieser Anträge der betroffenen Personen im erforderlichen Umfang.

§ 6 Nachweismöglichkeiten

1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in dieser Vereinbarung niedergelegten Pflichten mit geeigneten Mitteln nach. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Aufforderung die dokumentierten Kontrollen und erforderlichen Auskünfte zur Verfügung zu stellen. Insbesondere ist die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO nachzuweisen.
2. Der Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten kann erfolgen durch
    - aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
    - Selbstaudits
    - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz, ISO 27001, ISO 27018, ISO 27701)
    - die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO
    - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO
3. Kontrollrechte
    - Der Auftragnehmer verpflichtet sich, den Auftraggeber bei seinen Prüfungen gemäß Art. 28 Abs. 3 S. 2 lit. h DS-GVO zur Einhaltung der Vorschriften zum Datenschutz sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang zu unterstützen.
    - Die Prüfungen werden durch den Auftraggeber selbst oder einen von ihm beauftragten Dritten durchgeführt. Sollte der durch den Auftraggeber beauftragte Dritte in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Beauftragte Dritte müssen durch den Auftraggeber zur Verschwiegenheit verpflichtet werden. Dem Auftragnehmer steht das Recht zu, die Abgabe einer separaten Verschwiegenheitserklärung des beauftragten Dritten zu verlangen. Dies gilt insbesondere für die Abgabe von Erklärungen zur berufsrechtlichen oder gesetzlichen Verschwiegenheit.

- Eine Prüfung kann insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch weitere Maßnahmen erfolgen. Zu den weiteren Maßnahmen zählen die Anforderung von Zertifizierungen, Berichte zu Datenschutzaudits und Inspektionen vor Ort. Inspektionen vor Ort nimmt der Auftraggeber mit angemessener Vorankündigung während der üblichen Geschäftszeiten vor. Die Prüfungen müssen ohne Störung des Betriebsablaufs sowie unter Wahrung der Sicherheits- und Vertraulichkeitsinteressen des Auftragnehmers durchgeführt werden und sind auf eine Prüfung pro Kalenderjahr beschränkt. Ausgenommen sind anlassbezogene Kontrollen. Der Auftraggeber erstattet dem Auftragnehmer die durch die Durchführung der Prüfung entstandenen Kosten, sofern diese den typischerweise zu erwartenden Umfang übersteigen.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

1. Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.
2. Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Hauptvertrag zur Leistungserbringung vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. für Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software in Anspruch nimmt, sofern ein Zugriff auf personenbezogene Daten ausgeschlossen werden kann.
3. Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer informiert der Auftragnehmer den Auftraggeber. Der Auftraggeber kann der Änderung innerhalb einer Frist von 4 Wochen – aus wichtigem Grund – gegenüber der vom Auftragnehmer bezeichneten Stelle widersprechen. Widerspricht der Auftraggeber der Hinzuziehung oder Ersetzung von Subunternehmern, hat dieser zugleich den Hauptvertrag zur Leistungserbringung zu kündigen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben.
4. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus dieser Vereinbarung dem Subunternehmer zu übertragen.

§ 8 Übermittlung in Drittstaaten

Eine Übermittlung findet nur auf dokumentierte Weisung des Verantwortlichen in Drittstaaten außerhalb der EU und des EWR statt, sofern die Voraussetzungen nach Art. 44ff DS-GVO eingehalten werden.

§ 9 Informationspflichten, Schriftformklausel, Rechtswahl

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.
2. Änderungen und Ergänzungen dieser Vereinbarung 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.
3. Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Hauptvertrages zur Leistungserbringung vor. Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
4. Es gilt deutsches Recht.

§ 10 Haftung und Schadensersatz

1. Eine zwischen den Parteien im Leistungsvertrag (Hauptvertrag zur Leistungserbringung) vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, außer soweit ausdrücklich etwas anderes vereinbart wurde.
2. Soweit keine Haftungsregelung vereinbart wurde, haften Auftraggeber und Auftragnehmer gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

Hinweis: Diese Vereinbarung erfolgt mittels elektronischer Zustimmung.

Anhang über technische und organisatorische Maßnahmen nach Art. 32 DS-GVO

Kontrollziele	**Beschreibung der technischen und/oder organisatorischen Sicherungsmaßnahmen**
Pseudonymisierung und Verschlüsselung personenbezogener Daten	• HTTPS-Verschlüsselung in der Webkommunikation (Data-at-Transport) • obligatorische Verschlüsselung aller administrativen Zugriffe • Obligatorische Verschlüsselung aller ausgehenden E-Mails • Verwendung einer speziellen Hardware-Verschlüsselung für besonders kritische Daten (HSM) • Verschlüsselung aller Datensicherungsbänder
Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen	• Zugang zu Systemen nur mit individuellen Benutzernamen und Kennwörtern, • Obligatorische Mehr-Faktor-Authentifizierung für Fernzugriffe • Zentraler selbst-gehosteter individueller Passwort-Safe für alle Beschäftigte • Berechtigte können nur auf für sie berechtigte Daten zugreifen, • personenbezogene gespeicherte Daten können nur im Rahmen der Berechtigungsstufen gelesen, kopiert, verändert oder entfernt werden, • Einsatz eines Firewall- und Web-Application-Firewallsystems • Ausschließliche Verwendung der vom Hersteller der Hardware und Virtualisierungssoftware freigegebenen Software, • Verpflichtung der Mitarbeiter auf das Datengeheimnis • Redundante Klimaanlagen, redundante USVs in Serverräumen • Alert-Meldung bei Ausfällen der Serversysteme • Virtualisierung/Dynamische Zuteilung der Anwendung auf getrennte Serverräumen • Kein Zugang für Unbefugte zu den Datenverarbeitungsanlagen des Rechenzentrums, • Besucher der Rechenzentren (z.B. für Wartungszwecke) werden zwingend begleitet • Festlegung der berechtigten Personen für die sensiblen Bereiche der Rechenzentren Einbruchschutzmaßnahmen, Alarmanlage mit Aufschaltung auf Wachdienst • Besonderer Perimeterschutz für RZ-Bereiche • Protokollierung des Zutritts zu den Rechenzentren über entsprechende Transponder • Sichere Löschung von Datenträgern. • Videoüberwachung (Empfang und RZs), • Regelungen zur Kontrolle von externer Wartung und Fernwartung • Brandfrüherkennung und Gas-Löschanlage in besonderen RZ-Bereichen • Brandmeldeanlage mit Aufschaltung auf Feuerwehrleitstelle • Redundante Internetanbindung mit erdkabelfreier Breitband-Fallback-Anbindung • Schutz vor Netz-Überlastungsangriffen (DDoS) auf TIER 1- Ebene
Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen	• Doppelt- oder Mehrfachvorhaltung aller Komponenten bei der Datenverarbeitung (z. B. Datensicherung und Spiegelung von Hardwarekomponenten); • Datensicherungs- und Recoverykonzept • Auslagerung von Backups zu einem entfernten, eigenen Disaster-Recovery Standort umgehend nach Erstellung • besonders geschützte Rechenzentrumsabschnitte in getrennten Brandabschnitten und Gebäuden • unterbrechungsfreie Stromversorgung, • Überwachungs- und Meldesysteme, • Netzersatzanlage (NEA)
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Verarbeitung	• Regelmäßige Prüfung, ob/in welchem Umfang Zugangsrechte noch erforderlich sind, • Regelmäßige Prüfung, ob/in welchem Umfang Zugriffsrechte noch erforderlich sind, • Incident-Response-Management • Auftragskontrolle bei Auftragsverarbeitung • Regelmäßige Ausfalltests der Infrastrukturkomponenten