Auftrag gemäß Art. 28 DSGVO zur Auftragsverarbeitung

zwischen

der
Cyberse GmbH & Co. KG
Arzbergweg 39
91217 Hersbruck

nachfolgend „Auftragnehmerin“

und der
Mustermann GmbH
Musterstraße 1
91217 Hersbruck

nachfolgend „Auftraggeber“

(nachfolgend beide Parteien auch bezeichnet als „Partei“ oder „Parteien“)

§ 1 Einleitung, Geltungsbereich, Definitionen, kostenpflichtige Tätigkeiten

1. Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmerin (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.
2. Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter der Auftragnehmerin oder durch sie beauftragte Unterauftragnehmer (Subunternehmer) personenbezogene Daten des Auftraggebers verarbeiten.
3. In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU-Datenschutz-Grundverordnung zu verstehen.
4. Sofern in diesem Vertrag eine kostenpflichtige Tätigkeit der Auftragnehmerin vereinbart worden ist, so werden diese Tätigkeiten entsprechend den normalen Service-Entgelten der Auftragnehmerin abgerechnet.

§ 2 Gegenstand, Dauer der Verarbeitung

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

Definition der Aufgaben:

- Durchführung von IT-Dienstleistungen verschiedener Art

- Bereitstellung von Serverhosting, Speicherplatz, Bandbreite und Datenverkehr aus der Colocation der Auftragnehmerin

- Dienstleistungen im Bereich der IT-Sicherheit (speziell der Betrieb von Endpoint-Sicherheitslösungen sowie Firewalls zur Anbindung an die Colocation der Auftragnehmerin)

- Dienstleistungen imManagement von Cosplaytalenten

- Artverwandte Themen gemäß dem Unternehmenszweck aus dem Handelregistereintrag der Auftragnehmerin

Die Verarbeitung beruht auf dem zwischen den Parteien bestehenden Dienstleistungsauftrag.

2. Dauer des Auftrags

Die Verarbeitung beginnt zum Zeitpunkt der Beauftragung der Dienstleistung und erfolgt auf unbestimmte Zeit bis zur Kündigung der Dienstleistung durch eine Partei.

§ 3 Konkretisierung des Auftragsinhalts

1. Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, Kategorien betroffener Personen

Die Verarbeitungsart ist im Hauptvertrag konkret beschrieben. Die Verarbeitung umfasst folgende Arten: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten.

Der Verarbeitungszweck ist im Hauptvertrag konkret beschrieben. Die Verarbeitung der personenbezogenen Daten dient folgendem Zweck: Zweckerfüllung der vertraglich vereinbarten Dienstleistung.

2. Art der Daten

Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten sind folgende Datenarten / -kategorien (Aufzählung / Beschreibung der Datenkategorien):

- Kommunikationsdaten (z. B. Telefon/E-Mail)
- Vertragsstammdaten (Vertragsbeziehungen, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- ggf. weiteres:

3. Kategorien der betroffenen Personen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen umfasst (Aufzählung / Beschreibung der betroffenen Personenkategorien):

- Kunden / Mandanten des Auftraggebers
- Interessenten
- Lieferanten
- Mitarbeiter
- ggf. weiteres:

§ 4 Anwendungsbereich und Verantwortlichkeit

1. Die Auftragnehmerin 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 die Auftragnehmerin 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 Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die von der Auftragnehmerin bezeichneten 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.

§ 5 Pflichten der Auftragnehmerin

1. Die Auftragnehmerin verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, es liegt ein Ausnahmefall i. S. des Art. 28 Abs. 3 a) DS-GVO vor. Die Auftragnehmerin informiert den Auftraggeber unverzüglich, wenn sie der Auffassung ist, daß eine Weisung gegen anwendbare Gesetzte verstößt. Die Auftragnehmerin darf die Umsetzung der Weisung solange aussetzten, bis sie vom Auftraggeber bestätigt oder abgeändert wird.

2. Die Auftragnehmerin wird in ihrem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Sie wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Die Auftragnehmerin 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. Der Auftraggeberin sind diese technischen und organisatorischen Maßnahmen bekannt, sie trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten.

3. Die Auftragnehmerin verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

4. Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

5. Die Auftragnehmerin sichert zu, dass die bei ihr zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Die Auftragnehmerin trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden und dass es diesen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten.

6. Im Zusammenhang mit der beauftragten Verarbeitung wird die Auftragnehmerin den Auftraggeber kostenpflichtig bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung unterstützen.

7. Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich die Auftragnehmerin, den Auftraggeber im erforderlichen Umfang kostenpflichtig zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

8. Die Auftragnehmerin unterstützt, soweit vereinbart, den Auftraggeber kostenpflichtig bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.

10. Auskünfte an Dritte oder den Betroffenen darf die Auftragnehmerin nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an sie gerichtete Anfragen wird sie unverzüglich an den Auftraggeber weiterleiten, sofern eine Zuordnung an den Auftraggeber anhand der Angaben der betroffenen Person möglich ist. Die Auftragnehmerin haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

11. Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch die Auftragnehmerin sicherzustellen. Die hierfür anfallenden Kosten trägt der Auftraggeber.

12. Soweit gesetzlich verpflichtet, bestellt die Auftragnehmerin eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Die Auftragnehmerin teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt die Auftragnehmerin dem Auftraggeber unverzüglich mit. Als Datenschutzbeauftragter ist bei der Auftragnehmerin der Inhaber bestellt.

13. Die Auftragnehmerin unterrichtet den Auftraggeber unverzüglich, wenn ihr Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Die Auftragnehmerin 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.

14. Die Auftragnehmerin gewährleistet, ihren Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

15. Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich die Auftragnehmerin, den Auftraggeber bei der Abwehr des Anspruchs im Rahmen ihrer Möglichkeiten zu unterstützen. Die Parteien werden hierzu eine Vergütung vereinbaren.

16. Die Auftragnehmerin nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

17. Die Verarbeitung und Nutzung der Daten findet grundsätzlich innerhalb der EU oder des EWR statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und erfolgt nur unter den in Kapitel V der DS-GVO enthaltenen und den Bedingungen dieses Vertrages.

§ 6 Pflichten des Auftraggebers

1. Der Auftraggeber hat die Auftragnehmerin unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

2. Der Auftraggeber nennt der Auftragnehmerin den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

§ 7 Nachweismöglichkeiten, Inspektionen

1. Die Auftragnehmerin weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten mit geeigneten Mitteln nach.

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. Die Auftragnehmerin 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 zum Auftragnehmer stehen, hat die Auftragnehmerin ein Ablehnungsrecht.

3. Sofern die Inspektion mit einem unverhältnismäßig hohen Aufwand für die Auftragnehmerin verbunden ist, hat diese einen entsprechenden Kostenerstattungsanspruch gegen den Auftraggeber.

4. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich § 7 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

§ 8 Löschung von Daten und Rückgabe von Datenträgern

1. Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat die Auftragnehmerin sämtliche in ihren Besitz gelangte 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.

2. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch die Auftragnehmerin entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Sie kann sie zu ihrer Entlastung bei Vertragsende dem Auftraggeber übergeben.

§ 9 Technisch-organisatorische Maßnahmen

1. Die Auftragnehmerin hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung sichergestellt. Diese dokumentierten Maßnahmen werden als Anlage I Bestandteil dieses Vertrages. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

2. Die Auftragnehmerin hat die Sicherheit gem. Art. 32 DS-GVO insbesondere i. V. m. Art. 5 Abs. 1 und 2 DS-GVO herzustellen.

3. Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden oder durch adäquate alternative Maßnahmen ersetzt werden, solange das in Anlage I vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat die Auftragnehmerin unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

4. Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt die Auftragnehmerin den Auftraggeber unverzüglich.

5. Die Auftragnehmerin sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

6. Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

7. Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

8. Die Auftragnehmerin hat geeignete technische und organisatorische Maßnahmen für die rechtmäßige Verarbeitung der Daten ergriffen, die in Anlage I aufgeführt sind.

9. Die Auftragnehmerin nutzt ein nach ISO 27001 zertifiziertes Rechenzentrum. Die Parteien vereinbaren, dass dies für die Auftragnehmerin für den Nachweis geeigneter Garantien ausreicht.

10. Sollte eine Zertifizierung nach § 42 DS-GVO erfolgen, wird der Auftraggeber darüber informiert.

11. Sofern genehmigte Verhaltensregeln nach § 40 DS-GVO bestehen und sich die Auftragnehmerin diesen unterwerft, kann die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfter Wirksamkeit auch damit nachgewiesen werden.

12. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt der Auftragnehmerin vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

§ 10 Berichtigung, Einschränkung und Löschung von Daten

1. Soweit vom Leistungsumfang umfaßt, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch die Auftragnehmerin sicherzustellen.

§ 11 Unterauftragsverhältnisse

1. Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall zugelassen.

2. Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmerin und Subunternehmer.

   Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender vom Auftraggeber akzeptierter Subunternehmer durchgeführt:

   Teilleistung: Colocation Flächenbetreiber
   Name und Anschrift des Subunternehmers: NorthC Deutschland GmbH, Am Tower 5, 90475 Nürnberg, Telefon: +49 9128 99093 00, support@northcdatacenters.de

   Teilleistung: Unterstützungsleistung im Bereich Datacenter-Netzwerk / Routing
   Name und Anschrift des Subunternehmers: handily networks GmbH, Hauptstr. 37, 91227 Leinburg, Telefon: +49 9120 4179960, support@handily.network

3. Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer informiert die Auftragnehmerin den Ansprechpartner des Auftraggebers. Der Auftraggeber kann der Änderung innerhalb einer angemessenen Frist, die im Regelfall zwei Wochen beträgt, gegenüber dem Ansprechpartner der Auftragnehmerin widersprechen. Erfolgt kein Widerspruch innerhalb dieser Frist, gilt die Zustimmung zur Änderung als gegeben.

§ 12 Haftung und Schadensersatz

1. Sofern nicht anders geregelt, finden die Bestimmungen aus Artikel 82 der Datenschutzgrundverordnung (DSGVO) Anwendung.

§ 13 Informationspflichten, Schriftformklausel, Rechtswahl

1. Sollten die Daten des Auftraggebers bei der Auftragnehmerin durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat die Auftragnehmerin den Auftraggeber unverzüglich darüber zu informieren. Die Auftragnehmerin wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als Verantwortlichem im Sinne der DS-GVO liegen.

2. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen der Auftragnehmerin – 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 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.

4. Es gilt deutsches Recht.

Ort / Datum	*Ort / Datum*
Auftraggeber	*Auftragnehmerin: Cyberse GmbH & Co. KG*

Anlage 1 zum Auftrag gemäß Art. 28 DSGVO zur Auftragsverarbeitung

Allgemeine technische und organisatorische Maßnahmen

Der Auftragsverarbeiter setzt folgende technisch und organisatorische Maßnahmen zum Schutz der vertragsgegenständlichen personenbezogenen Daten um. Die Maßnahmen wurden im Einklang mit Art. 32 DS-GVO festgelegt und mit dem Auftraggeber abgestimmt.

I. Zweckbindung und Trennbarkeit

Folgende Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- logische softwareseitige Mandantentrennung
- Berechtigungskonzept
- Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- Versehen der Datensätze mit Zweckattributen / Datenfeldern und Signaturen
- pseudonymisierte Daten: Trennung der Zuordnungsdatei und der Aufbewahrung in einem getrennten und abgesicherten IT-System
- Interne Mandantenfähigkeit des Systems
- Funktionstrennung von Produktiv- und Testsystem

II. Vertraulichkeit und Integrität

Folgende Maßnahmen gewährleisten die Vertraulichkeit und Integrität der Systeme des Auftragsverarbeiters:

- Verschlüsselung
  Die Daten des Auftraggebers werden entsprechend dem Auftrag verschlüsselt.

- Pseudonymisierung
  Pseudonymisierung bedeutet, dass die personenbezogenen Daten in einer Weise verarbeitet werden, die eine Identifizierung der betroffenen Person ohne Hinzuziehung weiterer Informationen ausschließt (z.B. Verwendung von Fantasienamen, die ohne zusätzliche Informationen keiner bestimmten Person zugeordnet werden können).

- Zutrittskontrolle
  Es werden folgende Maßnahmen getroffen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu hindern:
  - Alarmanlage
  - Kameraüberwachung und Aufzeichnung mit Infrarotsystem
  - Automatisches Zugangskontrollsystem mit biometrischen Zugangsdaten über Fingerabdruckleser
  - Protokollierung sämtlicher Zu- und Ausgänge

- Unterteilung der Flächen in 3 zutrittsgeschützte Räume
- Zugang erfolgt ausschließlich durch Schleusen
- es ist 24x7 Personal vor Ort anwesend
- abgetrennte und gesicherte Räume für Batterien, USV und Stromversorgung
- Automatisches Zugangskontrollsystem mit Chipkarten

- Zugangskontrolle
  Es werden folgende Maßnahmen getroffen, um die Nutzung der Datensysteme durch unbefugte Dritte zu verhindern:
  - Zuordnung von Benutzerrechten und Einrichtung eines Benutzerstammsatzes pro Nutzer
  - Erstellung von Benutzerprofilen
  - differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte)
  - Passwort vergaben
  - Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)
  - automatische Sperrung (z. B. Kennwort oder Pausenschaltung)
  - Authentifikation mit Benutzernamen und Passwort
  - Zuordnung von Benutzerprofilen zu IT-Systemen
  - Einsatz von VPN-Technologie bei Übertragung von Daten
  - Sperren externer Schnittstellen (USB etc.)
  - Sicherheitsschlösser
  - Schlüsselregelung (Schlüsselausgabe etc.)
  - Personenkontrolle beim Pförtner / Empfang
  - Protokollierung der Besucher
  - Sorgfältige Auswahl von Reinigungspersonal
  - Sorgfältige Auswahl von Wachpersonal
  - Tragepflicht von Berechtigungsausweisen
  - Einsatz von Intrusion-Detektion-Systemen
  - Einsatz von Anti-Viren-Software
  - Verschlüsselung von Datenträgern in Laptops / Notebooks
  - Einsatz einer Hardware-Firewall
  - Einsatz einer Software-Firewall

- Zugriffskontrolle
  Es wurden folgende Maßnahmen getroffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:
  - Berechtigungskonzept
  - Verwaltung der Rechte durch Systemadministrator
  - regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern o.Ä.)
  - Anzahl der Administratoren ist das „Notwendigste“ reduziert
  - Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
  - Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
  - Sichere Aufbewahrung von Datenträgern
  - physische Löschung von Datenträgern vor Wiederverwendung
  - ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)

- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Protokollierung der Vernichtung
- Verschlüsselung von Datenträgern

- Eingabekontrolle
  Mit Hilfe folgender Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:
  - Protokollierung der Eingabe, Änderung und Löschung von Daten
  - Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
  - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
  - Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
  - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

- Auftragskontrolle
  Folgende Maßnahmen gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:
  - vorherige Prüfung der und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen
  - schriftliche Weisungen an den Auftragsverarbeiter (z.B. durch Auftragsverarbeitungsvertrag)
  - Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis
  - Auftragsverarbeiter hat Datenschutzbeauftragten bestellt
  - Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
  - Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart
  - laufende Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten

- Transport- und Weitergabekontrolle
  Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können:
  - Einsatz von VPN-Tunneln
  - Protokollierungsystem
  - Schnittstellenanalyse
  - Verschlüsselung der Kommunikationswege
  - Verschlüsselung physischer Datenträger bei Transport
  - Übertragung mit elektronischer Signatur
  - Transportsicherung

III. Verfügbarkeit, Wiederherstellung und Belastbarkeit der Systeme:

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- redundante unterbrechungsfreie Stromversorgung (USV) mit bis zu 2.1000kVA Leistung, GreenPower USV Systeme von Socomec
- zwei getrennte Stromfeeds durch 2 Unterverteilungen in jedem Rack
- 10kw Stromaufnahme je Rack und mehr möglich
- Notstromversorgung durch 1000kVA Dieselaggregate
- direkter Nachbar des Umspannwerkes
- 3-Stufiger Überspannungsschutz – Grobschutz in Hauptverteilung, Mittel- / Feinschutz in Unterverteilungen, optionaler weiterer Schutz durch kundeneingene Stromanschlußleisten
- VESDA System zur Früherkennung von Rauchentwicklung
- CO2-Feuerlöscher in allen Bereichen sofort griffbereit
- VDS-Alarmanlagen
- direkte Alarmierung des technischen Personals vor Ort sowie externer Mitarbeiter
- Klimatisierung der Serverräume mit einer Mischung aus direkter und indirekter Freikühlung
- Kaltwasserversorgung durch energiesparende Aggregate von Emerson Networks
- Luftaustausch durch Geräte jüngster Generation von Weiss Klimatechnik
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- belastbares Datensicherungs- und Widerherstellungskonzept vorhanden
- Maßnahen zur Datensicherung (physikalisch / logisch)
- Backup-Verfahren
- Spiegelung von Festplatten mittels Raid-Verfahren
- Einsatz eines Monitoring-Programms
- permanente Überwachung der ordnungsgemäßen Funktionalität
- Einsatz von CWDM Technik für hohe Skalierung der Bandbreiten
- Routing durch moderne Juniper Router
- Coreswitching durch moderne Cisco Switches
- Uplinks wahlweise in 100Mbit, 1GBit oder 10GBit
- Redundante Netzversorgung durch zahlreiche Carrier wie Tiscali International oder die deutsche Telekom
- Peeringverbindungen an diversen Exchangepunkten wie DECiX, AMSiX, KleyReX, ViX und NIX

IV. Besondere Datenschutzmaßnahmen:

Es liegen schriftlich vor:

- interne Verhaltensregeln
- Risikoanalyse
- Datenschutz-Folgenabschätzung
- Datensicherheitskonzept
- Wiederanlaufkonzept

V. Überprüfung, Evaluierung und Anpassung der vorliegenden Maßnahmen:

Der Auftragsverarbeiter wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen im Abstand von einem Jahr und anlassbezogen prüfen, evaluieren und bei Bedarf anpassen.