Ergänzende Vereinbarung über die Verarbeitung personenbezogener Daten i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (AV)

zwischen

.....

Firma oder Name des Auftraggebers

.....

Straße und Hausnummer

.....

PLZ, Ort, Land

– nachstehend **Auftraggeber** genannt –

und

der TELiAS Business Center GmbH, vertreten durch den Geschäftsführer Tim Lüghausen
Hohenstaufenring 62 in 50674 Köln, Deutschland

– als Auftragsverarbeiter, nachstehend **Auftragnehmer** genannt –

1 Präambel

Diese Vereinbarung konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragspartner, die sich aus der Beauftragung des Auftragsnehmers durch den Hauptvertrag bzw. durch die Hauptverträge ergeben.

Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag oder den Verträgen in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

2 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Der Gegenstand und die Dauer des Auftrages sowie Umfang und Art der Datenerhebung, Datenverarbeitung oder Datennutzung sind im Hauptvertrag bzw. in den Hauptverträgen und in den Allgemeinen Geschäftsbedingungen sowie den Leistungsbeschreibungen des Auftragnehmers konkretisiert.

Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des jeweiligen Hauptvertrages, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüber hinausgehende Verpflichtungen ergeben.

3 Konkretisierung des Auftragsinhalts

3.1 Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten

Der Auftragnehmer erbringt im wesentlichen Sekretariatsdienstleistungen und/oder Business Center Dienste für den Auftraggeber. Umfang, Art und Zweck der Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret in den Allgemeinen Geschäftsbedingungen und den Leistungsvereinbarungen beschrieben.

Der Auftragnehmer kann die vom Auftraggeber zur Verfügung gestellten und im Rahmen seiner Leistungserbringung zusätzlich gewonnenen Daten für rein statistische Zwecke aggregieren und daraus erstellte Statistiken ohne Nennung des Auftraggebers und in eigenem Namen veröffentlichen. Dies beschränkt sich auf ausschließlich anonymisierte, aggregierte Daten ohne jeglichen Personenbezug.

3.2 Ort der Verarbeitung und Speicherung von Daten

Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

3.2.1 Unternehmensstandorte:

Hohenstaufenring 38-40
50674 Köln, Deutschland
Hohenstaufenring 62
50674 Köln, Deutschland

3.2.2 Anbieter Rechenzentrum:

Host Europe GmbH
Welserstraße 14
51149 Köln, Deutschland

3.3 Art der Daten

Die Art der verwendeten personenbezogenen Daten ist in den Allgemeinen Geschäftsbedingungen und den Leistungsvereinbarungen beschrieben. Hierzu zählen insbesondere:

- Personenstammdaten
- Kommunikationsdaten (z.B. Adressdaten, Telefon- und Telefax-Nummern, E-Mail Adressen)
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Kundenhistorie
- Vertragsabrechnungs- und Zahlungsdaten
- Bankverbindungen
- Inhalte der Gesprächsnotizen sowie Zeitpunkt und Dauer der Anrufe
- ggf. Planungs- und Steuerungsdaten
- ggf. Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)

3.4 Kreis der Betroffenen

Betroffene der Datenverarbeitung sind der Auftraggeber selbst sowie Anrufer und Absendern von Postsendungen des Auftraggebers und ggf. auch andere Kunden des Auftraggebers, soweit er dem Auftragnehmer deren personenbezogenen Daten übermittelt hat.

4 Anwendungsbereich und Verantwortlichkeit

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag bzw. in den Hauptverträgen und in den Allgemeinen Geschäftsbedingungen und den Leistungsbeschreibungen des Auftragnehmers 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 (»verantwortliche Stelle« im Sinne des Art. 4 Nr. 7 DS-GVO).

Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt und sind folglich zusätzlich gegenüber dem Auftragnehmer zu vergüten. Mündliche Weisungen sind zusätzlich schriftlich oder in Textform vom Auftraggeber einzureichen.

5 Pflichten des Auftragnehmers

Der Auftragnehmer darf Daten von Betroffenen nur im Rahmen des Auftrages und den Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikels 28 Abs. 3a DS-GVO 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.

Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zur angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) entsprechen. 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 sicherzustellen (siehe Anhang über technische und organisatorische Maßnahmen nach Art. 32 DS-GVO).

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

Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten. Unterstützende Tätigkeiten, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt und sind folglich zusätzlich gegenüber dem Auftragnehmer zu vergüten. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen per Verpflichtung 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.

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

Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

Der Auftragnehmer verwendet die überlassenen Daten für keine anderen Zwecke als die der Vertragserfüllung. Der Auftragnehmer berichtigt, löscht oder sperrt die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist soweit dem nicht berechtigte Interessen des Auftragnehmers entgegenstehen.

Die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe.

Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

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 Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

6 Pflichten des Auftraggebers

Der Auftraggeber verpflichtet sich, der Informationspflicht (u.a. Zweckbestimmung, Datenspeicherung) gegenüber seinen Kontakten nachzukommen, die sich aus der Verarbeitung der vom Auftragnehmer übermittelten personenbezogenen Daten ergibt.

Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
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 Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.
Der Auftraggeber steht dem Auftragnehmer als Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen zur Verfügung.

7 Anfragen Betroffener

Wendet sich ein Betroffener mit Forderungen zur Berichtigung, Löschung, Sperrung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer den Betroffenen 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.

8 Unterauftragsverhältnisse

Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen Unternehmen innerhalb der TELiAS-Gruppe zur Leistungserfüllung heranzieht.

Eine Weitergabe von Aufträgen im Rahmen der vereinbarten Tätigkeiten an weitere Subunternehmer durch den Auftragnehmer erfolgt nicht.

Ein zustimmungspflichtiges Subunternehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei externem Personal-, Telekommunikations-, Post- und Versanddienstleistungen, Wartung und Webhosting.

Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Datenschutz zu gewährleisten.

9 Nachweismöglichkeiten

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

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.

Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich die o.g. Regelung für Inspektionen. 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.
Kosten, die der Auftragnehmerin durch ihre Unterstützungshandlung entstehen, sind ihr im angemessenen Umfang zu erstatten.

10 Informationspflicht, Schriftformklausel, Rechtswahl

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 „verantwortliche Stelle“ im Sinne des Bundesdatenschutzgesetzes liegen.
Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
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.
Es gilt deutsches Recht.

11 Haftung und Schadenersatz

Eine zwischen den Parteien im Leistungsvertrag (Hauptvertrag zur Leistungserbringung) vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, außer soweit ausdrücklich etwas anderes vereinbart.

Unterschrift (Auftraggeber)	Unterschrift
Name , Position	Name, Position
Ort, Datum	Ort, Datum

TELiAS

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

Die nachfolgenden Maßnahmen gelten für alle Standorte. Abweichende Regelungen an den Standorten sind differenziert dargestellt. Die interne Organisation sieht eine Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung in regelmäßigen Abständen vor.

1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1 Zutrittskontrolle (Räume und Gebäude):

Kontrollziele:	Maßnahmen:
Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden bzw. in denen personenbezogene Daten gelagert werden.	Standort Hohenstaufenring 38-40, 50674 Köln: Es besteht eine restriktive Zutrittsregelung zu den Büroräumen am o.g. Standort. Im Voraus angekündigte Besucher und Lieferanten haben ausschließlich Zugang über einen zentralen Empfang. Diese Besucher dürfen sich ausschließlich in Begleitung von Mitarbeitern im Gebäude bewegen. Standort Hohenstaufenring 62, 50674 Köln: Es existiert ein zentraler Empfangsbereich am Haupteingang des Gebäudes, der durch einen Wachdienst besetzt ist. Ein Empfang ist am Eingang des Business Centers zusätzlich eingerichtet. Die Räume sind in öffentliche und nicht öffentliche Bereiche aufgeteilt. Die Zutrittsberechtigung ist auf Raumebene geregelt. Nur Mitarbeiter und Büromieter erhalten per Schlüsselberechtigung (Transponder) Zugang. Gäste melden sich am Empfang und werden entweder von Mitarbeitern oder Büromietern begleitet. Sonstige Besucher (z.B. Nutzer der Konferenzräume, Tagesbüros oder des Loungebereichs) sind entweder persönlich bekannt oder haben sich im Voraus angekündigt und erhalten deshalb Zugang zu öffentlichen Bereichen des Business Centers. Nicht öffentliche Bereiche unterliegen einer restriktiven Zutrittsregelung und werden nur von Mitarbeitern betreten. Für beide Standorte gilt weiter: Ausgenommen sind regelmäßig wiederkehrende betriebsfremde Personen (z.B. Reinigungspersonal externer Reinigungsfirmen); diese dürfen auch ohne Begleitung die Büroräume betreten, sofern sie sich schriftlich sowohl den gesetzlichen Datenschutzbestimmungen, denen von TELiAS, und dem Datengeheimnis verpflichtet haben. Die individuell ausgegebenen Zugangsmittel werden manuell dokumentiert und nach Ablauf der Berechtigung erfolgt eine dokumentierte Rücknahme. Die Aufbewahrung dieser Dokumente erfolgt für mindestens 12 Mo-

	nate. Der Zugang zu Serverräumen ist gesondert gesichert. Der Kreis der zugangsberechtigten Personen ist auf eine kleine Gruppe (Systemadministratoren, die Geschäftsführung und die Assistenz der Geschäftsführung) reduziert. Betriebsfremde Personen dürfen nur nach vorheriger Terminvereinbarung und Genehmigung durch die Geschäftsführung die Serverräume betreten.

1.2 Zugangskontrolle (IT-System & Anwendungen):

Kontrollziele:	Maßnahmen:
Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	Grundsätzlich sind alle Zugänge zu personenbezogenen Daten zugangsgeschützt. Zugänge werden grundsätzlich nur personengebunden mit individuellen Zugangsdaten vergeben. Neue Zugänge werden auf Grundlage der Rolle der Person oder nach schriftlicher Genehmigung von der Geschäftsführung erteilt. Zugänge von ausgeschiedenen Personen werden umgehend deaktiviert. Die Authentifikation der Benutzer erfolgt durch Benutzername und Passwort über ein Active Directory. Ein Gruppen- / Rollenkonzept sowie eine Passwortrichtlinie sind umgesetzt. Eine Sicherung der Bildschirmarbeitsplätze bei Abwesenheit und laufendem System erfolgt mittels passwortgeschütztem Bildschirmschoners. Die Abschottung interner Netze gegen Zugriffe von außen und von innen erfolgt per Firewall (Verschlüsselung, VPN). Es besteht Softwareschutz gegen eine Verletzung der Systemintegrität (Viren- und Spywarescanner). Die Daten werden ausschließlich auf Servern gespeichert. Es befinden sich keine lokalen Kopien auf den Clients. Sämtliche Netzwerkzugänge werden IT-seitig verwaltet und bei Nichtnutzung deaktiviert.

1.3 Zugriffskontrolle (auf Daten):

Kontrollziele:	Maßnahmen:
Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems berechtigten Personenausschließlich 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.	Ein Berechtigungskonzept (Benutzer- und Administrationsberechtigung) stellt sicher, dass der Zugriff auf Daten des Systems nur in dem Umfang ermöglicht wird, wie es für die jeweilige Rolle erforderlich ist. Ein Zugriff auf personenbezogene Daten ist den hierzu berechtigten Personen (Anwender) nur über eine Clientsoftware möglich. Es sind differenzierte Berechtigungen für Lesen, Verändern oder Löschen von Daten eingerichtet. Für alle Anwendungsprogramme (Benutzer) zur Verarbeitung der personenbezogenen Daten, wird eine Historie vorgehalten, die erfasst, welcher Nutzer wann welche Aktion ausgeführt hat, sofern die Aktion persönliche Daten modifiziert. Darüber hinaus wer-

	den noch weitere Aktionen protokolliert, um in der Anwendung selbst Änderungsverläufe etc. darstellen zu können. Es existiert ein Berechtigungskonzept (Einrichtung von Administrationsrechten und Verwaltung der Zugriffsrechte durch die Systemadministratoren). Es erfolgt eine Trennung von Test- und Produktionsbetrieb. Die datenschutzgerechte Entsorgung nicht mehr benötigter Dokumente und Datenträger ist durch den Einsatz von abgeschlossenen Datentonnen, deren Inhalt durch einen autorisierten Dienstleister abgefahren wird, gewährleistet. Die private Nutzung von Internet- und E-Mail für Mitarbeiter ist vertraglich ausgeschlossen. <u>Standort Hohenstaufenring 62, 50674 Köln:</u> Mieter des Business Centers erhalten über ein abgetrenntes System Zugang zum Internet. Der Zugriff erfolgt über ein eigenes VLAN (drahtlos und/oder drahtgebunden) oder über einen WPA2 gesichertes WLAN.

1.4 Trennungskontrolle:

Kontrollziele:	Maßnahmen:
Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	In einem Berechtigungskonzept sind die Zugriffsrechte festgelegt. Ein direkter Zugriff auf Rohdaten oder mehrere Kunden gleichzeitig ist nur den Administratoren möglich. Es erfolgt eine eindeutige Verknüpfung über Schlüssel in der Datenbank (logische Trennung).

2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Weitergabekontrolle (von Daten):

Kontrollziele:	Maßnahmen:
Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	Es erfolgt eine Dokumentation von Datenempfängern, der Transport- und Übermittlungswege, der zur Übermittlung befugten Personen und der zu übermittelnden Daten. Die Übertragung erfolgt verschlüsselt (SSL-Verschlüsselung bei Zugriff über einen Web-browser und bei Übertragung zwischen den Systemen über öffentliche Netzwerke). Eingesetzte Verschlüsselungstechnik ist TLS-Verschlüsselung mit AES und 256 Bit-Schlüssel, sowie RSA mit 2048 Bit-Austausch. Die Verschlüsselung von Daten entfällt, wenn Daten (z.B. Gesprächsnotizen) per Standard E-Mail und SMS übermittelt werden. Eine Dokumentation der Abruf- und Übermittlungsprogramme wird durchgeführt. Die Zulässigkeit einer Datenübermittlung wird stichprobenartig geprüft.

	<u>Standort Hohenstaufenring 62, 50674 Köln:</u> Sämtliche Dokumente, die über das im öffentlichen Bereich zugängliche Druck- & Scan-System der TELiAS erfolgen, werden erst nach Eingabe einer persönlichen Kennung am Gerät gedruckt und ausgegeben (Vertrauensdruck). Postsendungen der Mieter werden an einem zentral zugänglichen Bereich, getrennt in verschossenen Postboxen hinterlegt. Mieter können mittels Schlüssel die Postsendungen von dort entnehmen. Postsendungen von Kunden die eine Weiterleitung beauftragt haben, sowie Päckchen und Pakete werden in einem nicht öffentlich zugänglichen Bereich zentral gelagert. Postsendungen von Kunden werden nur nach schriftlicher Vollmacht zwecks Digitalisierung geöffnet. Etwaige vom Kunden beauftragte und/oder vertraglich vereinbarte Vernichtung von Post erfolgt ausschließlich über gesicherte Datentonnen.

2.2 Eingabekontrolle (in Datenverarbeitungssysteme):

Kontrollziele:	**Maßnahmen:**
Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt wurden.	Führung revisionssicherer Zugriffsberechtigungen (Rollenkonzept). Die Eingabe von personenbezogenen Daten ist den hierzu berechtigten Mitarbeitern (Anwender) nur über eine Clientsoftware möglich. Es sind differenzierte Berechtigungen für das Lesen, Verändern oder Löschen von Daten eingerichtet. Für alle Anwendungsprogramme (Benutzer) zur Verarbeitung der personenbezogenen Daten, wird eine Historie vorgehalten, die erfasst, welcher Nutzer wann welche Aktion ausgeführt hat, sofern die Aktion persönliche Daten modifiziert. Darüber hinaus werden noch weitere Aktionen protokolliert, um in der Anwendung selbst Änderungsverläufe etc. darstellen zu können. Die Protokolle werden stichprobenartig oder bei Bedarf (Auffälligkeiten/Unstimmigkeiten) geprüft.

3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

3.1 Verfügbarkeitskontrolle (von Daten):

Kontrollziele:	Maßnahmen:
Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	Es gibt eine Funktionstrennung zwischen Fachabteilungen und IT-Abteilung. Beschaffung von Hard- und Software erfolgt mittels eines standardisierten Einkaufsprozesses bei ausgewählten Lieferanten. Es werden mehrmals täglich Schattenkopien angefertigt. Einmal täglich erfolgt eine Sicherung von Komplettabbildern (Disaster-Recovery) der virtuellen Maschinen, einmal wöchentlich erfolgt eine inkrementelle Sicherung der Daten. Die Sicherungen werden an getrennten Standorten aufbewahrt. Es erfolgt eine unregelmäßige Kontrolle der Backup-Software (Simulation der Wiederherstellung). Die Datensicherung wird auf externe Festplatten durchgeführt. Backups werden (gemäß Löschkonzept) nach 14 Tagen überschrieben. Alle Server sind als virtuelle Maschinen ausgeführt, welches ein schnelles Disaster-Recovery (unabhängig von der Hardware) ermöglicht. Maßnahmen für den Notfall sind in einem Handbuch dokumentiert. Schutzmaßnahmen am und im Serverraum (Feuerlöscher, Brandmelder, Klimaanlage, USV etc.) sind umgesetzt. Eine Risiko- und Schwachstellenanalyse für den gesamten DV-Bereich erfolgt in regelmäßigen Abständen. Eine rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO) ist mit unserem Recovery-Prozess abgedeckt.

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

4.1 Datenschutz-Management

Kontrollziele:	Maßnahmen:
Es ist die Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und nach Außerbetriebnahme von Verfahren zur Informationsverarbeitung sicher zu stellen.	Der Datenschutzprozess ist als zyklischer Prozess ausgelegt und stellt bei geändertem Umfeld die Einhaltung geltenden Datenschutzrechtes sicher. Die Organisation der Aufgaben verteilt sich auf die jeweiligen Anlaufstellen der Abteilungen, den Datenschutzkoordinator und den Datenschutzbeauftragten, die sich in der operativen Ebene unterscheiden. Ein Regelprozess sieht eine regelmäßige Kontrolle des Datenschutzprozesses vor.

4.2 Incident-Response-Management

Kontrollziele:	Maßnahmen:
Die Meldewege im Falle eines Datenschutzvergehens sind zu definieren und deren Ablauf sicher zu stellen.	Die Mitarbeiter werden regelmäßig zum Thema Datenschutz und über den Umgang in der Verarbeitung personenbezogener Daten informiert. Die Schulungsunterlagen beinhalten eindeutige Indikatoren, aus denen sich Situationen zu möglichen Datenschutzvergehen ergeben. Bei Verdacht auf ein Datenschutzvergehen handelt die jeweilige Anlaufstelle im Sinne der im Datenschutzkonzept beschriebenen Arbeitsanweisung. Diese beinhaltet in jedem Falle immer eine zeitnahe Einbindung des internen Datenschutzkoordinators und ggf. der betroffenen Person/en. Im Rahmen der gesetzlichen Pflicht werden bei vorliegendem Datenschutzvergehen der Datenschutzbeauftragte sowie die Aufsichtsbehörde benachrichtigt.

4.3 Auftragskontrolle:

Kontrollziele:	Maßnahmen:
Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (vgl. Art. 28 DS-GVO).	Die Kontrolle der Einhaltung von Datensicherheitsbestimmungen und die Meldung über Verstöße oder der Verdacht auf unzureichende Datensicherheitsvorgaben sind eingerichtet. Sämtliche Mitarbeiter haben eine Vertraulichkeits-/ Verschwiegenheitspflicht. Eine Weitergabe von Aufträgen im Rahmen der vereinbarten Tätigkeiten an Subunternehmer erfolgt nicht. Ausnahmen bilden Nebenleistungen. TELiAS wird im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Datenschutz zu gewährleisten und sämtliche Weisungen des Auftraggebers beachten. TELiAS stellt allen Kunden einen passwortgeschützten Servicepoint zwecks Verwaltung von Kundendaten und Administration der vereinbarten Dienste zur Verfügung. Der Servicepoint sowie die Daten werden in einem Rechenzentrum von einem deutschen Anbieter gehostet. Für den Hostingvertrag gilt ausschließlich deutsches Recht, insbesondere das deutsche Datenschutzrecht.