Anhang über technische und organisatorische Maßnahmen nach Art. 32 DSGVO

1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

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.	Es existiert ein zentraler Empfangsbereich am Haupteingang des Gebäudes, der durch einen Wachdienst besetzt ist. Ein Empfang am Etagen-Eingang ist 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. Nicht öffentliche Bereiche unterliegen einer restriktiven Zutrittsregelung und werden nur von Mitarbeitern betreten. 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 Monate. Der Zugang zu Serverräumen ist gesondert gesichert. Der Kreis der zugangsberechtigten Personen ist auf eine kleine Gruppe (Systemadministratoren, Standortleiter sowie 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. Alle Passwörter unterliegen Längen- und Komplexitätsanforderungen gemäß den einschlägigen Empfehlungen des BSI und werden bei deren

	Änderungen angepasst. 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 werden 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. 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 ein 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 DSGVO)

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-/TLS-**Verschlüsselung bei Zugriff über einen Webbrowser 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. Kreditkartendaten werden im Rahmen der Zahlungsabwicklung ausschließlich direkt durch den eingesetzten Zahlungsdienstleister verarbeitet und nicht auf eigenen Systemen gespeichert oder verarbeitet. Intern erfolgt lediglich eine Referenzierung über tokenisierte Zahlungskennungen. 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 verschlossenen 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 DSGVO)

3.1 Verfügbarkeitskontrolle (von Daten):

Kontrollziele:	Maßnahmen:
Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	Es besteht eine klare Funktionstrennung zwischen Fachabteilungen und IT-Abteilung. Die Beschaffung von Hard- und Software erfolgt über standardisierte Prozesse bei ausgewählten Lieferanten. Zur Sicherstellung der Verfügbarkeit und Integrität der Daten werden regelmäßig Datensicherungen erstellt. Die Sicherung erfolgt automatisiert und in mehreren Stufen (mehrmals täglich, wöchentlich sowie monatlich). Die Datensicherung erfolgt verschlüsselt, ist vom Dienstleister nicht einsehbar (Zero Knowledge beim Dienstleister) und getrennt von den produktiven Systemen. Die Speicherung erfolgt bei einem vertraglich gebundenen Auftragsverarbeiter in Rechenzentren eines ISO / IEC 27001-zertifizierten Dienstleisters innerhalb der Europäischen Union. Der Zugriff auf die Datensicherungen ist auf autorisierte Mitarbeitende der IT-Abteilung beschränkt. Zugriffe werden protokolliert. Backups werden gemäß definiertem Lösch- und Aufbewahrungskonzept für einen begrenzten Zeitraum vorgehalten und anschließend automatisiert überschrieben. Alle Server sind als virtuelle Maschinen ausgeführt, wodurch eine schnelle und hardwareunabhängige Wiederherstellung (Disaster Recovery) ermöglicht wird. Es bestehen definierte Verfahren zur Wiederherstellung von Daten im Falle eines technischen oder physischen Zwischenfalls. Hierzu werden i.S.d. Art. 32 Abs. 1 lit. c DSGVO in definierten Abständen Wiederherstellungstests (Restore-Tests) anhand repräsentativer Systeme / Daten durchgeführt und dokumentiert. Maßnahmen für Notfälle sind in entsprechenden Handbüchern dokumentiert. Schutzmaßnahmen im Rechenzentrums- und Serverumfeld (z. B. Brandmelder, Klimatisierung, unterbrechungsfreie Stromversorgung) sind umgesetzt. Eine Risiko- und Schwachstellenanalyse für den gesamten IT-Bereich erfolgt unter Berücksichtigung der eingesetzten Dienstleister und Rechenzentren in regelmäßigen Abständen.

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

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 DSGVO).	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 an nicht genehmigte Unterauftragnehmer erfolgt nicht. Externe Dienstleister, insbesondere Zahlungsdienstleister zur Abwicklung von Kreditkartenzahlungen, werden vor Einsatz datenschutzrechtlich und sicherheitstechnisch bewertet und dokumentiert. Soweit externe Zahlungsdienstleister eingesetzt werden, kann die Verarbeitung personenbezogener Daten teilweise weisungsgebunden im Sinne des Art. 28 DSGVO sowie teilweise in eigener datenschutzrechtlicher Verantwortlichkeit erfolgen. 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.