Kontrollziele gemäß Anlage § 9 BDSG und Beschreibung der technischen und/oder organisatorischen Sicherheitsmaßnahmen

Die nachfolgenden Maßnahmen gelten für alle Standorte. Abweichende Regelungen an den Standorten sind differenziert dargestellt.

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

TELiAS

Kontrollziele gemäß Anlage § 9 BDSG und Beschreibung der technischen und/oder organisatorischen Sicherheitsmaßnahmen

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. Die Passwortrichtlinie (8 Zeichen, Klein- / Großbuchstaben, Zahlen, Sonderzeichen, Wechselintervall 3 Monate) wird serverseitig per Gruppenrichtlinie erzwungen. 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 dem Server gespeichert. Es befinden sich keine lokalen Kopien auf den Clients. Sämtliche Netzwerkzugänge werden IT-seitig verwaltet und bei Nichtnutzung deaktiviert.

3 Zugriffskontrolle (auf Daten):

Kontrollziele:	Maßnahmen:
Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems berechtigten Personen 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.	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 Administrationsrech-

	ten 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. Standort Hohenstaufenring 62, 50674 Köln: 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.

4 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 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 auf Wunsch des Kunden 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. Standort Hohenstaufenring 62, 50674 Köln: 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.

5 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.

6 Auftragskontrolle:

Kontrollziele:	Maßnahmen:
Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	Die Kontrolle der Einhaltung von Datensicherheitsbestimmungen und die Meldung über Verstöße oder der Verdacht auf unzureichende Datensicherheitsvorgaben sind eingerichtet. Sämtliche Mitarbeiter sind auf das Datengeheimnis (§ 5 BDSG, teilweise zusätzlich auf § 203 StGB) verpflichtet. 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 in Deutschland gehostet. Weder die Daten noch der Servicepoint (Software) selbst verlassen Deutschland, außer der Auftraggeber verlangt dies. Für den Hostingvertrag gilt ausschließlich deutsches Recht, insbesondere das deutsche Datenschutzrecht.

Kontrollziele gemäß Anlage § 9 BDSG und Beschreibung der technischen und/oder organisatorischen Sicherheitsmaßnahmen

7 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. Durchführung einer Risiko- und Schwachstellenanalyse für den gesamten DV-Bereich ist in Bearbeitung.

8 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).