Kontrollen	Auswahl	Begründung
Zugangskontrolle **Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte**		
Gibt es für die Verabeitung von personenbezogenen Daten einen dafür vorgesehen Serverraum	ja	Es gibt einen Serverraum am Standort der ONTEC, so wie ein versperrter Rack in einem dafür vorgesehenen Rechenzentrum.
Ist der Serverraum versperrt	ja	Sowohl mechanische als auch biometrisch.
Wird der Zutritt zum Serverraum protokolliert	ja	An beiden Standorten wird der Zutritt protokolliert
Gibt es eine Liste von zutrittsberechtigten Personen	ja	Für beide Standorte.
Wird diese Liste regelmäßig und in Anlassfällen auf Aktualität überprüft	ja	Im Zuge des Benutzerberechtigungsprozesses
Werden mobile Arbeitsgeräte (Laptop, Handy, Tablet, etc.) sicher verwahrt wenn diese unbeaufsichtigt sind	ja	
Gibt es dafür eine dokumentierte Regelung	ja	In Policy "ONTEC IT Nutzungsbestimmungen"
Werden Büroräumlichkeiten bei Verlassen des letzten Mitarbeiters versperrt	ja	In Policy "ONTEC IT Nutzungsbestimmungen"
Datenträgerkontrolle **Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern**		
Gibt es eine Regelung zum sicheren Umgang mit Datenträgern	ja	In Policy "ONTEC IT Nutzungsbestimmungen"
Werden personenbezogene Daten ausschließlich auf dafür bestimmten Datenträgern (Server oder Client) gespeichert	ja	
Gibt es dafür eine dokumentierte Regelung	ja	In Policy "ONTEC IT Nutzungsbestimmungen"
Werden Datenträger nach Ihrem Ausscheiden sicher entsorgt	ja	Verschlüsselt bzw. sicher entsorgt
Benutzerkontrolle **Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte**		

Können ausschließlich nur Befugte auf personenbezogene Daten zugreifen	ja	In Policy "ONTEC IT Nutzungsbestimmungen"
Gibt es dafür eine dokumentierte Regelung	ja	Im Zuge des Benutzerberechtigungsprozesses
Werden Benutzerrechte regelmäßig, dokumentiert überprüft und falls notwendig, angepasst	ja	Im Zuge des Benutzerberechtigungsprozesses
Zugriffskontrolle **Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben**		
Können Benutzer nur auf die Daten zugreifen, für die es auf Grund ihrer Tätigkeit auch die Notwendigkeit und die Berechtigung gibt	ja	Technisch geregelt
Gibt es dafür eine dokumentierte Regelung	ja	Im Zuge des Benutzerberechtigungsprozesses
Gibt es eine Regelung zur Verwaltung von Kennwörtern	ja	Technisch geregelt
Gibt es eine protokollierte Zugriffsüberwachung	ja	Technisch geregelt
Übertragungskontrolle **Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können**		
Gibt es eine dokumentierte Regelung, wie personenbezogene Daten an andere Berechtigte (auch Dritte) übermittelt werden müssen	ja	In Policy "ONTEC IT Nutzungsbestimmungen"
Werden personenbezogene Daten ausschließlich verschlüsselt übermittelt	nein	Nur dort wo vertraglich gefordert.
Werden personenbezogene Daten auch unter Verwendung transportabler Datenträger übermittelt	nein	In Policy "ONTEC IT Nutzungsbestimmungen" geregelt

Eingabekontrolle **Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind**		
Gibt es eine Regelung zur Verwendung einer Ereignisprotokollierung	nein	Es gibt eine Ereignisprotokollierung aber keine dedizierte Regelung hierzu.
Kann nachträglich festgestellt werden, welcher Benutzer zu welcher Zeit von welchem Ort auf personenbezogene Daten zugegriffen hat	ja	
Werden die Ereignisprotokolle für Systeme und Anwendungen von personenbezogenen Daten mindestens 3 Monate vor Manipulation und unberechtigtem Zugriff geschützt aufbewahrt	ja	Ausgenommen Firewall-Logfiles: kleiner 3 Monate
Gibt es eine gesonderte Ereignisprotokollierung für privilegierte Benutzer (Admins, Fernwartungsuser - Dritte, etc.)	ja	
Transportkontrolle **Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können**		
Gibt es eine Regelung zum Umgang mit mobilen Datenträgern	ja	In Policy "ONTEC IT Nutzungsbestimmungen"
Werden USB-Sticks, Smartphones, Tablets, externe Festplatten, Speicherkarten, etc. für den Transport oder die Ablage von personenbezogenen Daten verwendet	nein	Ausnahme Kontaktdaten in verschlüsseltem Container.
Dürfen diese Datenträger nur von dafür bestimmten Personen transportiert werden	n.a.	
Wird sichergestellt, dass sich bei zur Reperatur befindlichen Geräten keine personenbezogenen Daten auf den Datenspeichern befinden	ja	es werden keine Geräte mit personenbezogenen Daten an Dritte weitergegebn.
Ist sichergestellt, dass es eine Vertraulichkeitsvereinbarung bzgl. personenbezogener Daten zwischen Sender und Empfänger und gegebenenfalls Dritter gibt	ja	

Wiederherstellung **Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können**		
Gibt es ein Datensicherungs- und Wiederherstellungskonzept	ja	Backup
Gibt es ein Archivierungskonzept	ja	Dort wo es rechtliche Vorgaben gibt.
Gibt es regelmäßige Datensicherungen	ja	
Können verlorengegangene oder fälschlich oder vorsätzlich veränderte Daten zeitnahe wiederhergestellt werden	ja	
Werden alle vorgegebenen Servicevereinbarungen (SLAs) eingehalten	ja	
Gibt es regelmäßige Funktionstests für die Wiederherstellung von Daten	ja	
Werden alle rechtlichen und vertraglichen Anforderung in Bezug auf die Aufbewahrungsdauer erfüllt	ja	
Datenintegrität **Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können**		
Gibt es einen Prozess für das betriebliche Kontinuitätsmanagement (BCM)	ja	Continuity Management Prozess
Gibt es einen Change-Managementprozess	ja	Change Management Prozess
Gibt es einen Prozess der sicherstellt, dass vor allem sicherheitsrelevante Updates zeitnahe eingespielt werden	ja	Security Incident Prozess
Gibt es einen angemessenen, dem Stand der Technik entsprechenden Schutz vor Schadsoftware	ja	Virenscanner, Firewall, etc.
Gibt es einen angemessenen, dem Stand der Technik entsprechenden Schutz vor Angreifern von aussen (Hacker)	ja	Firewall

Gibt es eine Regelung welche sicherstellt, dass im Rahmen der wirtschaftlichen Möglichkeiten und dem Stand der Technik entsprechend Schutzmaßnahmen identifiziert und zeitnahe umgesetzt werden	ja	Security Incident Prozess
Personelle Sicherheit **Sicherstellen, dass nur qualifizierten, dafür vorgesehenen und verlässlichen Personen der Zugang zu personenbezogenen Daten gewährt wird**		
Gibt es einen dokumentierten Prozess zur Personalsuche welcher die genauen Anforderungen spezifiziert	ja	Screening policy und terms and conditions of employment
Gibt es eine Regelung welche sicherstellt, dass nur mit geeigneten und zuverlässigen Auftragnehmern zusammengearbeitet wird	ja	dort wo relevant für Verarbeitung von personenbezogenen Daten (z.B. Rechenzentrum)
Wird sichergestellt, dass bei Änderungen während der Beschäftigung, Karenzierung oder des Auftragsverhältnisses Benutzerrechte angepasst werden	ja	Im Zuge des Benutzerberechtigungsprozesses
Wird sichergestellt, dass bei Beendigung des Beschäftigungs- oder Auftragsverhältnisses auch die jeweiligen Benutzerberechtigungen zeitnahe und dokumentiert entzogen werden	ja	Im Zuge des Benutzerberechtigungsprozesses
Wird sichergestellt, dass es eine gültige und dem Zweck entsprechende Vertraulichkeits- oder Geheimhaltungsvereinbarung mit allen Beschäftigten und relevanten Auftragnehmern gibt	ja	Im Dienstvertrag, bzw. mit Lieferanten dort wo relevant für Verarbeitung von personenbezogenen Daten (z.B. Rechenzentrum)