Anlage 1 – Technische und Organisatorische Maßnahmen

Maßnahmenforderung	gesetzliche Anforderung	Umsetzung in der Praxis
Zutrittskontrolle	Unbefugten den Zutritt zu DV-Anlagen verwehren	Das Betriebsgebäude wird durch einen Sicherheitsdienst bewacht. Alle Zugänge zum Gebäude werden videoüberwacht. Der Haupteingang ist mit einem Pförtner besetzt. Alle Seiteneingänge sind nur über Chip-karten zu öffnen. Die Haupteingangstüren des Gebäudes sind außerhalb der Betriebs-zeiten fest verschlossen. Dritte haben zu den Räumlichkeiten keinen Zutritt. Gebäude- sowie Bürotüren sind alarmgesichert. Besucher werden vom Pförtner in Empfang genommen und ihre Anmeldung wird kontrolliert. Über ein elektronisches Schließsystem wird durch verschiedene Berechtigungs-stufen gewährleistet, dass Mitarbeiter neben den allgemeinen Bereichen nur Räume betreten können, für diese sie speziell berechtigt wurden. Serverräume lassen sich nur durch autorisierte Mitarbeiter mit Chipkarten betreten. Eintritte zu Räumlichkeiten mit einem erhöhtem Sicherheitsbedarf sind über Chipkarten und spezielle Berechtigungen zugänglich und werden elektronisch festgehalten und überwacht.
Zugangskontrolle	Nutzung von DV-Anlagen durch Unbefugte verhindern	Alle Rechner der Mitarbeiter verfügen über einen Virenschutz. Um Zugang zu Datenverarbeitungssystemen zu bekom-men, müssen sich Mitarbeiter mindestens mit Benutzererkennung & Passwort identifizieren. Die Bildschirme werden automatisch nach kurzer Zeit der Inaktivität gesperrt. Jeder Mitarbeiter hat ein eigenes Benutzerkonto mit individuellen Zugriffs-rechten. Die Anzahl der Login-Versuche werden protokolliert und nach Über-schreitung der maximalen Anzahl fehlerhafter Login-Versuche, wird das Benutzerkonto gesperrt. Eine Entsper-rung ist nur durch eine Administration nach Authentifikation des Mitarbeiters, möglich. Nach der Entsperrung wird der Anwender aufgefordert ein persönliches Passwort zu vergeben.

		Mobiles Arbeiten für Mitarbeiter ist durch VPN gesichert. Alle Endgeräte und Datenträger sind, wenn möglich, verschlüsselt. Die Firmennetzwerke sind durch Firewalls abgesichert. Die Netzwerksegmente sind durch eine Firewall getrennt. Die Firewall-Einstellungen werden regelmäßig geprüft. Eine Richtlinie zum Ausscheiden von Mitarbeitern (Rechteentzug) sowie eine Passwortrichtlinie sind verabschiedet.
Zugriffskontrolle	Gewährleistung der Benutzung einer DV-Anlage und der gespeicherten Daten entspre-chend der Berechtigung	Alle Zugriffsmöglichkeiten und Benutzer-rollen sind in Berechtigungs-konzepten festgehalten und analog geregelt. Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet. Zertifikate werden zur Authentifizierung ausgegeben und Zugriffe werden in Logs protokolliert. Zusätzlich werden Protokolle eingesetzt, die eine Transport-verschlüsselung beinhalten.
Weitergabekontrolle/ Übermittlungs-kontrolle	Übermittlung von Daten darf nur an berechtigte Empfänger geschehen	Transportverschlüsselungen werden ein-gesetzt. Datensätzen werden anhand von IDs, anstatt durch Klarnamen oder anderer persönlichen Daten, identifiziert. Der Grundsatz der Datenminimierung wird eingehalten. Ein standardisierter Prozess zum datenschutzkonformen Vernichten von Datenträgern wird ein-gehalten.
Plausibilitätskontrolle /Transaktions-kontrolle	Gewährleistung der Nachver-folgbarkeit von (gewollten und ungewollten) Datenmanipu-lationen	Plausibilitätsprüfungen werden durchge-führt.
Auftragskontrolle/ Vertragskonformitäts-kontrolle	Sicherstellung der weisungs-gemäßen Verarbeitung von Daten im Auftrag	Zum Schutz personenbezogener Daten werden Auftragnehmer hinsichtlich der technischen und organisatorischen Maß-nahmen sorgfältig ausgewählt und entsprechende Auftragsverarbeitungsverträge werden geschlossen. Die technischen und organi-satorischen Maßnahmen werden im regelmäßigen Turnus überprüft.
Verfügbarkeits-kontrolle	Sicherung von Daten gegen zufällige Zerstörung oder Ver-lust	Verfügbarkeit, rasche Wiederherstell-barkeit und einen Schutz gegen Verluste werden gewährleistet durch unter-brechungsfreie Stromversorgung (USV) mit Überspannschutz, RAID-Lösungen und tägliche Backups. Alle Büros und Serverräume sind mit Feuer- und Rauchmeldeanlagen ausge-stattet. Eine Analyse der Serverraumlage wurde vorgenommen, Serverräume sind klimatisiert.

		Auf allen Systemen erfolgen regelmäßig Updates.
Datentrennungs-kontrolle/Mandanten-trennungskontrolle	Sicherstellung der Trennung zu unterschiedlichen Zwecken er-hobener Daten	Entwicklungs-/Test- und Produktivum-gebung sind voneinander getrennt und Datenverarbeitungssysteme sind zweck-gebunden voneinander getrennt. Ein externer Datenschutzbeauftragter ist gestellt. Es werden nur diejenigen personen-bezogenen Daten erhoben, die für den jeweiligen Zweck erforderlich sind. Während des Entwicklungsprozesses neuer Software wird bereits sicher-gestellt, dass diese datenschutzfreundlich realisiert wird.