Technisch Organisatorische Maßnahmen

Zutrittskontrolle	**entb.**	**ja**	**teilw.**	**nein**
Gesicherter Eingang, einbruchshemmende Fenster	X			
Abschließen der Räume mit Sicherheitsschlössern		X		
Festlegung der befugten Personen durch Sonderschlüsselvergabe bzw. durch Kennung des Codes für eventuelle Zahlentürschlösser		X		
Personenkontrolle durch Schlüsselsystem bzw. In-Empfangnahme		X		
Abschließen der Räume mit Sicherheitsschlössern bzw. durch Kennung des Codes für eventuelle Zahlentürschlösser		X		
Sicherung durch Alarmanlagen mit automatischer, telefonischer Benachrichtigung der MA in festgelegter Reihenfolge		X		
Spezielle Regelung für Reinigung, Wartung, Reparatur und Besucher		X		
Bauliche Vorkehrungen (Gitter, Sichtblenden, Raumteiler)	X			
Zugangskontrolle	**entb.**	**ja**	**teilw.**	**nein**
Prüfung der Zugangsberechtigung durch Authentifizierung (Passwort): Persönliches Passwort, mindestens 10 Zeichen, Vergabe durch Benutzer selbst		X		
Änderungspflicht nach 365 Tagen		X		
Kennwortchronik		X		
2-Faktorauthentifizierung bei Anmeldung am System		X		
Maximal 3 Anmeldeversuche technisch vorgesehen		X		
Zugriffskontrolle	**entb.**	**ja**	**teilw.**	**nein**
Festlegen und Kontrolle der Zugriffsbefugnisse, differenziert nach Daten, Programmen und Zugriffsart		X		
Identifikation der Zugreifenden		X		
Protokollierung der Zugriffe sowie von Missbrauchversuchen (Ggf. Auswertung der Protokolle)		X		
Funktionsbegrenzung (funktionell/zeitlich)		X		
Automatisches Log-off bzw. Bildschirmsperre		X		
Archivierung von Daten in einem Panzerschrank		X		
Beschränkung des Zugriffs auf bestimmte Betriebssystembereiche, bei besonders sensitiven Daten Ausschluss des Zugriffs auf das Benutzersystem		X		
Benutzerspezifische, abgestufte Rechteverwaltung auf Unterverzeichnis- und Dateiebene		X		
Zugriffbeschränkung auf IP-Ebene über VPN		X		
Verschlüsselung von Notebookfestplatten			X	
Weitergabekontrolle	**entb.**	**ja**	**teilw.**	**nein**
Protokollierung der Abruf- und Übermittlungsaktivitäten		X		
Verschlüsselte Weitergabe		X		
Lese-/Schreib-Schutz der lokalen Festplatte gegenüber anderen Netzanwendern		X		
Kein Einsatz von Programmen, die eine Zuordnung von fremden Datenträgern erlauben		X		

Technisch Organisatorische Maßnahmen

Eingabekontrolle	**entb.**	**ja**	**teilw.**	**nein**
Automatisierte Protokollierung der Dateneingabe, Änderung oder Löschung		X		
Automatisierte Protokollierung der Administrator-Aktivitäten			X	
Sicherung der Protokolldaten gegen Verlust oder Veränderung		X		
Auswertungsverfahren für automatisiert erstellte Protokolldaten		X		
Freigabeverfahren und Dokumentation der aktuellen Programmversion			X	
Aufzeichnung über die Datenerfassungskräfte sowie der zur Dateneingabe, Änderung oder Löschung berechtigten Personen		X		
Protokollierung der Eingaben, Änderung und Löschung in besonderen Protokolldateien		X		
Plausibilitätskontrollen		X		
Auftragskontrolle	**entb.**	**ja**	**teilw.**	**nein**
Auswahl des Auftragnehmers unter Sorgfalt-Gesichtspunkten		X		
Verwendung von Form- und Merkblättern zur Sicherung vollständiger und klarer Weisungen		X		
Verpflichtung des Personals des Auftragnehmers auf die Verarbeitung personenbezogener Daten ausschließlich auf Weisung des Arbeitgebers entsprechend Art. 29 DSGVO sowie Art. 32 Abs. 4 DSGVO		X		
Abgrenzung der Verantwortlichkeit zwischen Auftraggeber und Auftragnehmer		X		
Verfügbarkeitskontrolle	**entb.**	**ja**	**teilw.**	**nein**
Datensicherungskonzept mit Auslagerung und Aufbewahrungsfristen und Anweisungen		X		
Systemdokumentation		X		
Einrichtung einer unterbrechungsfreien Stromversorgung		X		
Verwendung von geeigneten Tresoren		X		
Dokumentation der Sicherungsläufe		X		
Standards für Eigenprogrammierung, Test- und Freigabeverfahren			X	
Wiederanlaufkonzept			X	
Aufstellen einer Brand- und Katastrophenordnung		X		
Virenschutz, Firewall		X		
Trennungsprinzip	**entb.**	**ja**	**teilw.**	**nein**
Logische Trennung		X		
Bestellung eines betrieblichen Datenschutzbeauftragten		X		