Im Einzelnen werden folgende Maßnahmen bestimmt (Art. 32 Abs. 1 lit b. DSGVO):

Nr.	Maßnahme	Umsetzung der Maßnahme
Vertraulichkeit der Daten		
1.	Zutrittskontrolle Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	Zutrittskontrollsystem, Ausweisleser, Magnetkarte, Chipkarte, Schlüssel, Werkschutz, Pförtner, Überwachungseinrichtung, Alarmanlage, Türsicherung
2.	Zugangskontrolle Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.	Technische Kennwort- / Passwortschutz (inkl. Sonderzeichen, Minimallänge, Passwortänderungen), automatisches ausloggen und Datenverschlüsselung
3.	Zugriffskontrolle Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten 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.	Bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung, Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren (Beispiele: differenzierte Berechtigungen wie Profile, Rollen etc. Auswertungen, Kenntnisnahme, Veränderung, Löschung
4.	Trennungskontrolle Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten, Mandantenfähigkeit, Funktionstrennung zwischen Produktion / Test
5	Pseudonymisierung Es ist zu gewährleisten, dass die Verarbeitung personenbezogener Daten in einer Weise erfolgt, die das Risiko minimieren. Hierzu gehört die Pseudonymisierung von Daten.	Personenbezogene Daten werden verschlüsselt auf dem Server hinterlegt
Integrität der Daten		
6.	Weitergabekontrolle	

	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.	Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung wird ein Verwendung von dem Stand der Technik entsprechendes Verschlüsselungsverfahren verwendet
7.	Eingabekontrolle Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung wird durch ein Protokollierungs- und Protokollauswertungsverfahren gewährleistet
Verfügbarkeit und Belastbarkeit		
8.	Verfügbarkeitskontrolle Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.	Backup-Verfahren, Spiegeln von Festplatten, unterbrechungsfreie Stromversorgung, Firewall, Notfallplan
9.	Rasche Widerherstellbarkeit Es ist zu gewährleisten, dass die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt wird	Hochverfügbare Backups gewährleisten eine rasche Wiederherstellung der Daten
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung		
10.	Auftragskontrolle Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	Abgrenzung der Kompetenz zwischen Auftraggeber und Auftragnehmer
11.	Datenschutz-Management Es ist zu gewährleisten, dass durch ein Datenschutz-Management die Überprüfung gewährleistet ist.	Regelmäßige Kontrollen der Maßnahmen durch einen Datenschutzbeauftragten