Checkliste:
Technische und organisatorische Maßnahmen

Folgende technische und organisatorische Maßnahmen wurden nach Artikel 5 DSGVO und §64 BDSG für folgende verantwortliche Stelle getroffen:

1. Zutrittskontrolle

Ist gewährleistet, dass Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird?

	Technische Maßnahmen		Organisatorische Maßnahmen
	Manuelles Schließsystem		Schlüsselregelung / Schlüsselbuch
	Sicherheitsschlösser		
	Alarmanlage		
	Absicherung von Gebäudeschächten		
	Automatisches Zugangskontrollsystem		Protokollierung der Besucher / Besucherbuch
	Biometrische Zugangssperren		Personenkontrolle beim Pförtner / Empfang
	Chipkarten- / Transponder-Schließsystem		Tragepflicht von Mitarbeiter- / Gästeausweisen
	Lichtschranken / Bewegungsmelder		Videoüberwachung der Zugänge
	Schließsystem mit Codesperre		Sorgfältige Auswahl von Sicherheitspersonal

2. Zugangskontrolle (§64 BDSG)

Wir verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?

	Technische Maßnahmen		Organisatorische Maßnahmen
	Authentifikation mit Benutzer + Passwort		Erstellen von Benutzerprofilen
	Einsatz von Anti-Viren-Software		Benutzerberechtigungen verwalten
	Einsatz von Firewalls		Passwortvergabe / Passwortregeln
	Verschlüsselung von Datenträgern		Sorgfältige Auswahl von Reinigungspersonal
	Gehäuseverriegelungen		Schlüsselregelung / Schlüsselbuch
	Sperren von externen Schnittstellen (z.B. USB-Anschlüsse)		Protokollierung der Besucher / Besucherbuch
	Authentifikation mit biometrischen Daten		Personenkontrolle beim Pförtner / Empfang

			Sorgfältige Auswahl von Sicherheitspersonal
Mobile Geräte			
	Einsatz von Mobile Device Management		
	Einsatz von VPN-Technologie		
	Verschlüsselung von Smartphones		

3. Zugriffskontrolle (§64 BDSG)

Ist gewährleistet, 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?

	Technische Maßnahmen		Organisatorische Maßnahmen
	Protokollierung der Vernichtung von Daten		Erstellen eines Berechtigungskonzepts
	Einsatz von Aktenvernichtern		Verwaltung der Benutzerrechte durch Systemadministratoren
	Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)		Anzahl der Administratoren auf das „Notwendigste“ reduzieren
	Physische Löschung von Datenträgern vor deren Wiederverwendung		Passwortrichtlinie inkl. Länge und Wechsel
			Sichere Aufbewahrung von Datenträgern
	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten		Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit Zertifikat)
	Verschlüsselung von Datenträgern		
	Verschlüsselung von Smartphones		

4. Weitergabekontrolle

Ist gewährleistet, 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?

	Technische Maßnahmen		Organisatorische Maßnahmen
	Einrichtungen von VPN-Tunneln		Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen

	E-Mail-Verschlüsselung		Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
	Sichere Transportbehälter/-verpackungen		Sorgfältige Auswahl von Transportpersonal und –fahrzeugen
			Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

5. Eingabekontrolle (§ 64 BDSG)

Ist gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind?

	Technische Maßnahmen		Organisatorische Maßnahmen
	Protokollierung der Eingabe, Änderung und Löschung von Daten		Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
			Erstellen einer Übersicht, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
			Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

6. Auftragskontrolle (§64 BDSG)

Ist gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können?

	Technische Maßnahmen		Organisatorische Maßnahmen
			Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
			Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
			Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungs-vertrag) i.S.d. § 11 Abs. 2 BDSG
			Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
			Verpflichtung der Mitarbeiter des Auftrag-nehmers auf das Datengeheimnis (§ 5 BDSG)
			Vertragsstrafen bei Verstößen

			Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechender Dokumentation
			Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbaren

7. Verfügbarkeitskontrolle (§64 BDSG)

Ist gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind?

	Technische Maßnahmen		Organisatorische Maßnahmen
	Feuerlöschgeräte in Serverräumen		Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
	Feuer- und Rauchmeldeanlagen		Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen		Erstellen eines Backup- & Recoverykonzepts
	Klimaanlage in Serverräumen		Erstellen eines Notfallplans
	Schutzsteckdosenleisten in Serverräumen		Testen von Datenwiederherstellung
	Unterbrechungsfreie Stromversorgung (USV)		Serverräume nicht unter sanitären Anlagen
			In Hochwassergebieten: Serverräume über der Wassergrenze

8. Trennungsgebot (64 BDSG)

Ist gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können?

	Technische Maßnahmen		Organisatorische Maßnahmen
	Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System		Erstellung eines Berechtigungskonzepts
	Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern		Festlegung von Datenbankrechten
	Trennung von Produktiv- und Testsystem		Logische Mandantentrennung (softwareseitig)
	Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden		Versehen der Datensätze mit Zweckattributen/Datenfeldern