Kurzcheck: Technische und Organisatorische Maßnahmen (TOMs)	
Name und Anschrift des Unternehmens	
Standort (falls abweichend)	
Ansprechpartner	
Datum	

Verarbeitungstätigkeit (Abteilung)	

Der Auftragnehmer trifft nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit i.S.d. Art. 32 DSGVO.

1. Vertraulichkeit

Zutrittskontrolle

Es wurden folgende Maßnahmen getroffen, um Unbefugte am Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu hindern:

☐ Alarmanlage
☐ Absicherung von Gebäudeschächten
☐ Automatisches Zugangskontrollsystem
☐ Chipkarten-/Transponder-Schließsystem
☐ Schließsystem mit Codesperre
☐ Manuelles Schließsystem
☐ Biometrische Zugangssperren
☐ Videoüberwachung der Zugänge
☐ Lichtschranken / Bewegungsmelder
☐ Sicherheitsschlösser
☐ Schlüsselregelung (Schlüsselausgabe etc.)
☐ Personenkontrolle beim Pförtner / Empfang
☐ Protokollierung der Besucher
☐ Sorgfältige Auswahl von Reinigungspersonal
☐ Sorgfältige Auswahl von Wachpersonal
☐ Tragepflicht von Berechtigungsausweisen
☐ Zutrittskonzept / Besucherregelung
☐ Sonstige:

_____

_____

Zugangskontrolle

Es wurden folgende Maßnahmen getroffen, die die Nutzung der Datensysteme durch unbefugte Dritte verhindern:

☐ Zuordnung von Benutzerrechten
☐ Erstellen von Benutzerprofilen
☐ Passwortvergabe
☐ Passwort-Richtlinien (regelmäßige Änderung, Mindestlänge, Komplexität etc.)
☐ Authentifikation mit biometrischen Verfahren
☐ Authentifikation mit Benutzername / Passwort
☐ Multifaktor-Authentifizierung für Administratoren (Cloud)
☐ Multifaktor-Authentifizierung für Benutzer
☐ Zuordnung von Benutzerprofilen zu IT-Systemen
☐ Gehäuseverriegelungen
☐ Einsatz von VPN-Technologie bei der Übertragung von Daten
☐ Verschlüsselung mobiler IT-Systeme
☐ Verschlüsselung mobiler Datenträger
☐ Verschlüsselung der Datensicherungssysteme
☐ Sperren externer Schnittstellen (USB etc.)
☐ Einsatz von Intrusion-Detection-Systemen (Eindringling-Erkennungssysteme)
☐ Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
☐ Einsatz von Anti-Viren-Software
☐ Verschlüsselung von Datenträgern in Laptops / Notebooks
☐ Verschlüsselung von Datenträgern in PCs
☐ Verschlüsselung von Datenträgern in Servern
☐ Einsatz einer Hardware-Firewall
☐ Einsatz einer Software-Firewall
☐ Sonstige:

_____

_____

Zugriffskontrolle

Es wurden folgende Maßnahmen getroffen, die 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:

☐ Berechtigungskonzept
☐ Verwaltung der Rechte durch Systemadministrator
☐ regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte (insb. bei Ausscheiden von Mitarbeitern o.Ä.)
☐ Anzahl der Administratoren ist das „Notwendigste“ reduziert
☐ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
☐ Sichere Aufbewahrung von Datenträgern
☐ physische Löschung von Datenträgern vor Wiederverwendung
☐ ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
☐ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
☐ Protokollierung der Vernichtung
☐ Sonstige:

_____

_____

Zweckbindung und Trennbarkeit

Folgende Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

☐ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
☐ Logische Mandantentrennung (softwareseitig)
☐ Berechtigungskonzept
☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
☐ Versehen der Datensätze mit Zweckattributen / Datenfeldern / Signaturen
☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten und abgesicherten IT-System
☐ Trennung von Produktiv- und Testsystem
☐ Sonstige:

_____

_____

Verschlüsselung

Die im Auftrag verarbeiteten Daten bzw. Datenträger werden in folgender Weise verschlüsselt:

_____
_____
_____

(Bitte Verschlüsselungs-Maßnahmen konkret beschreiben)

Pseudonymisierung

„Pseudonymisierung“ bedeutet, dass personenbezogene Daten in einer Weise verarbeitet werden, die eine Identifizierung der betroffenen Person ohne Hinzuziehung weiterer Informationen ausschließt (z.B. Verwendung von Fantasienamen, die ohne zusätzliche Informationen keiner bestimmten Person zugeordnet werden können).

☐ Nein.
☐ Ja, und zwar in folgender Art und Weise:
_____
_____
_____
(Bitte Maßnahmen zur Pseudonymisierung konkret beschreiben)

2. Integrität

Eingabekontrolle

Mit Hilfe folgender Maßnahmen kann nachträglich überprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

☐ Protokollierung der Eingabe, Änderung und Löschung von Daten
☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
☐ Sonstige:

_____

_____

Transport- bzw. Weitergabekontrolle

Folgende Maßnahmen gewährleisten, dass personenbezogene Daten bei der Weitergabe (physisch und / oder digital) nicht von Unbefugten erlangt oder zur Kenntnis genommen werden können:

☐ Einsatz von VPN-Tunneln
☐ Verschlüsselung der Kommunikationswege (z.B. Verschlüsselung des EMail-Verkehrs)
☐ Verschlüsselung physischer Datenträger bei Transport

☐ Sonstige:

_____

_____

3. Verfügbarkeit und Belastbarkeit

Folgende Maßnahmen gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit einwandfrei funktionieren und personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

☐ Unterbrechungsfreie Stromversorgung (USV)
☐ Klimatisierung der Serverräume
☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
☐ Schutzsteckdosenleisten in Serverräumen
☐ Feuer- und Rauchmeldeanlagen in Serverräumen
☐ Feuerlöschgeräte in Serverräumen
☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
☐ Testen von Datenwiederherstellung
☐ Erstellen eines Notfallplans
☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
☐ Serverräume nicht unter sanitären Anlagen
☐ In Hochwassergebieten: Serverräume über der Wassergrenze
☐ belastbares Datensicherungs- und Widerherstellungskonzept vorhanden
☐ Sonstige:

_____

_____

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Der Verantwortliche wird die in dieser Anlage niedergelegten technischen und organisatorischen Maßnahmen im Abstand von einem Jahr prüfen, evaluieren und bei Bedarf anpassen.

☐ Die Beschäftigten des Verantwortlichen werden regelmäßig zum Datenschutz geschult.
  ☐ Schulungsnachweise liegen vor
☐ Die Beschäftigten werden zum vertraulichen Umgang mit personenbezogenen Daten verpflichtet.
☐ Es gibt Richtlinien für Beschäftigte zum Umgang mit personenbezogenen Daten.
☐ Es ist ein Datenschutzbeauftragte benannt worden.
☐ Es gibt ein Verzeichnis von Verarbeitungstätigkeiten i.S.d. Art. 30 Abs. 1 und 2 DSGVO, das jährlich geprüft und aktualisiert wird.
☐ Sonstiges: …….

5. Konzepte oder sonstige Nachweise

5.1. Ist ein Löschkonzept vorhanden?

☐ ja ☐ nein
Wenn ja, bitte den TOMs beifügen.

5.2. Ist ein IT-Sicherheitskonzept vorhanden?

☐ ja ☐ nein
Wenn ja, bitte den TOMs beifügen.

5.3. Sonstiges?

☐ ja ☐ nein
Wenn ja, bitte den TOMs beifügen.

Erfüllungsgrad der Maßnahmen:
Anmerkungen:

Revisionshistorie

Laufende Nr.				
Datum	**Erfasst/geändert durch**	**Datum Prüfung durch DSB**	**Maßnahmen ausreichend?**	**Anmerkungen**
			☐ Ja ☐ Nein	
	Unterschrift	Unterschrift		Termin nächste Überprüfung