

Anhang „Technisch-organisatorische Maßnahmen (TOM)“

zur Vereinbarung zur Auftragsverarbeitung vom 01.01.2000, BA047-25

zwischen

und Vertragspartner

§ 5 der Vereinbarung zur Auftragsverarbeitung verweist zur Konkretisierung der technisch-organisatorischen Maßnahmen auf diesen Anhang.

§ 1 Technische und organisatorische Sicherheitsmaßnahmen

Die Vertragspartner sind verpflichtet, geeignete technische und organisatorische Maßnahmen so durchzuführen, dass die Verarbeitung der Daten im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Person in angemessener Form gewährleistet ist.

§ 2 Innerbehördliche oder innerbetriebliche Organisation des Auftragsverarbeiters

Der Auftragsverarbeiter wird seine innerbehördliche oder innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Daten oder Datenkategorien geeignet sind.

§ 3 Konkretisierung der Einzelmaßnahmen

(1) Im Einzelnen werden folgende Maßnahmen bestimmt, die der Umsetzung der Vorgaben des Art. 32 DSGVO dienen:

Nr.	Maßnahme	Umsetzung der Maßnahme
1.	Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten	
2.	Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung	

Nr.	Maßnahme	Umsetzung der Maßnahme
3.	Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen	
4.	Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung	
5.	Maßnahmen zur Identifizierung und Autorisierung der Nutzer	
6.	Maßnahmen zum Schutz der Daten während der Übermittlung	
7.	Maßnahmen zum Schutz der Daten während der Speicherung	
8.	Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten verarbeitet werden	
9.	Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen	
10.	Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration	

Nr.	Maßnahme	Umsetzung der Maßnahme
11.	Maßnahmen für die interne Governance und Verwaltung der IT und der IT-Sicherheit	
12.	Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten	
13.	Maßnahmen zur Gewährleistung der Datenminimierung	
14.	Maßnahmen zur Gewährleistung der Datenqualität	
15.	Maßnahmen zur Gewährleistung einer begrenzten Speicherdauer	
16.	Maßnahmen zur Gewährleistung der Rechenschaftspflicht	
17.	Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung	
18.	Ggf. Beschreibung der spezifischen technischen und organisatorischen Maßnahmen, die der Auftragsverarbeiter zur Unterstützung des Verantwortlichen ergreifen muss	

(2) Es ist ein Verfahren zu etablieren, das eine regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der zum Einsatz kommenden technischen und organisatorischen Maßnahmen durch die Vertragsparteien ermöglicht.

(3) Folgende Nachweise werden dieser Vereinbarung angefügt (*Zutreffendes bitte ankreuzen*):

- ☐ Einhaltung von Verhaltensregeln nach Artikel 40 DSGVO
- ☐ Zertifizierung nach Artikel 42 DSGVO
- ☐ Prüfberichte, Testate etc. unabhängiger Prüfer, bspw. Wirtschaftsprüfer, Auditoren, Datenschutzbeauftragte etc.
- ☐ geeignete Zertifizierung durch einen Auditprozess