

Die Vorlage zur Erstellung der technischen und organisatorischen Maßnahmen kann folgendermaßen gegliedert werden:

1. Pseudonymisierung

Wikipedia definiert die Pseudonymisierung als einen Vorgang, bei dem persönliche Daten durch z.B. Zahlenfolgen ersetzt werden, so dass diese nicht mehr zuordenbar sind. Also z.B. Ersetzung einer E-Mail Adresse durch eine User-ID.

2. Verschlüsselung

Hier geht es um den Schutz der Daten vor unberechtigten Zugang z.B. durch Passwörter auf Archiven.

3. Gewährleistung der Vertraulichkeit

Hier geht es um alles, was mit Zutritt und Zugang zu tun hat, wie gewährleisten Sie, dass nur Berechtigte Zugang zum Serverraum haben?

4. Gewährleistung der Integrität

Wie gewährleisten Sie, dass die Daten, die Sie verarbeiten an sich richtig sind? Wie steuern Sie Änderungen oder Löschungen?

5. Gewährleistung der Verfügbarkeit

Wie gewährleisten Sie, z.B. bei einem Stromausfall die Verfügbarkeit der Daten?

6. Gewährleistung der Belastbarkeit der Systeme

Machen Sie regelmäßige Checks, ob Ihre Systeme gegen Unfälle oder Eindringlinge sicher sind?

7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach

einem physischen oder technischen Zwischenfall

Haben Sie Vorgehensweisen, bei einem Zwischenfall, der z.B. alle ihre Daten auf einem Server löscht?

8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Prüfen Sie auch, ob die o.g. Maßnahmen effektiv sind? Wenn ja, wie?

9. Schriftliche Dokumentation von sonstigen Maßnahmen

Haben Sie z.B. Datenschutz Anweisungen an Ihre Mitarbeiter ausgegeben? Haben Sie eine IT-Sicherheitszertifizierung?