Inhalte eines Vertrages nach § 11 BDSG:

Auftraggeber

und

Auftragnehmer

1. Gegenstand und Dauer des Auftrags

Gegenstand des Auftrags
Was wird gemacht?
Dauer des Auftrags
Wie lange wird es gemacht?

2. Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen

- Von wem werden
- welche Daten
- warum
- wie erhoben, verarbeitet oder genutzt
-

3. Technisch-organisatorische Maßnahmen

Nach der Anlage zu § 9 BDSG, einzelne Punkte können auch in Anlage ausgelagert werden:

1. **Zutrittskontrolle**
   Wie wird sichergestellt, dass kein Unbefugter räumlichen Zutritt zum System hat?
   Zutrittskontrollsysteme, Schlüssel, Videoüberwachung, Pförtner etc.
2. **Zugangskontrolle**
   Wie wird sichergestellt, dass kein Unbefugter System nutzen kann?
   Kennwort- und Passwortschutz, Sonderzeichen, Mindestlänge, regelmäßiger Wechsel von Passworten, Automatische Sperrung usw.
3. **Zugriffskontrolle**
   Wie wird sichergestellt, dass Berechtigte ausschließlich im Rahmen ihrer Berechtigung agieren?
   Berechtigungskonzept mit rollenspezifischen Zugangsrechten, Überwachung und Protokollierung
4. **Weitergabekontrolle**
   Wie wird sichergestellt, dass Daten bei Transport nicht unbefugt genutzt usw. werden?
   Verschlüsselte Übertragung, Tunnelverbindung, Sicherung bei Transport physischer Datenträger usw.
5. **Eingabekontrolle**
   Wie wird sichergestellt, dass Änderungen nachträglich geprüft werden können?
   Protokollierungs- und Auswertungssysteme
6. **Auftragskontrolle**
   Wie wird sichergestellt, dass Daten nur im Rahmen des Auftrags verarbeitet werden?
   Eindeutige Vertragsgestaltung, Kriterien zur Auswahl von Auftragnehmern, Vertragskontrolle
7. **Verfügbarkeitskontrolle**
   Wie wird sichergestellt, dass Daten nicht zufällig zerstört werden?
   Backup-Verfahren, Unterbechungsfreie Stromversorgung, Virenschutz, Firewall usw.
8. **Trennungskontrolle**
   Wie wird sichergestellt, dass Daten mit verschiedenem Zweck getrennt verarbeitet werden?

Mandantenfähige Systeme, Trennung von Funktionen

4. Berichtigung, Sperrung und Löschung von Daten

Wie wird sichergestellt, dass die Rechte des Betroffenen auf Berichtigung, Löschung und Sperrung von Daten (§ 20) umgesetzt werden?

5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen

- Schriftliche Bestellung eines Datenschutzbeauftragten, soweit vorgeschrieben.
- Verpflichtung aller datenverarbeitenden Personen auf das Datengeheimnis, § 5 BDSG
- Umsetzung der T-O-M und ihre Nachweisbarkeit, ggf. Zertifizierungen
- Unverzügliche Information über Maßnahmen der Datenschutzbehörde nach § 38 BDSG
- Durchführung der Auftragskontrolle durch regelmäßige Prüfungen

6. Unterauftragsverhältnisse

Dürfen Subunternehmer eingeschaltet werden?

7. Kontrollrechte des Auftraggebers

Wie kontrolliert der Auftraggeber?

8. Mitteilung bei Verstößen des Auftragnehmers

Bei Verstößen ist der Auftraggeber zu informieren

9. Weisungsbefugnis des Auftraggebers

Wie erteilt der Auftraggeber Weisungen zur ADV, wie muss der Auftragnehmer mit Weisungen umgehen?

10. Löschung von Daten und Rückgabe von Datenträgern

Was passiert nach Vertragsende mit den Daten? Löschung oder Rückgabe?