

1. IT-Sicherheit als Chefsache

JA NEIN

- Ist der Geschäftsführung das Risiko durch eine unzureichende IT-Sicherheit für das eigene Geschäft bekannt?
- Ist das Management von Risiken und Informationssicherheit explizit Bestandteil der Unternehmenspolitik?
- Wird der Geschäftsführung regelmäßig über Risiken und das Sicherheitsniveau direkt berichtet?
- Wurde ein „fachkundiger und zuverlässiger“ Datenschutzbeauftragter gemäß § 4f BDSG bestellt?

2. IT-Sicherheits-Organisation

JA NEIN

- Wurde der Datenbestand im Hinblick auf Sensibilität/Schutzwürdigkeit bzw. Bedeutung analysiert und klassifiziert?
- Existiert ein Datenschutz-Konzept zur Berücksichtigung der gesetzlichen Vorgaben?
- Existiert eine IT-Security-Policy bzw. IT-Sicherheitskonzept?
- Sind eindeutige Verantwortlichkeiten für geschäftskritische Informationen und Verfahren festgelegt?
- Sind Kontrollverfahren etabliert, um interne und externe Prozesse auf Ordnungsmäßigkeit und Einhaltung zu überprüfen?

3. Technische und organisatorische Maßnahme

JA NEIN

- Entsprechen alle Komponenten im Bereich IT dem „State of the Art“?
- Existiert ein Berechtigungskonzept (inkl. der Rechtevergabe), welches sicherstellt, dass jeder Benutzer ausschließlich auf jene Informationen zugreifen kann, die er zwingend für seine Tätigkeiten benutzt?
- Werden unerlaubte Zugriffsversuche auf vertrauliche Daten protokolliert?
- Ist die Vernichtung von Daten und Hardware verbindlich geregelt?
- Werden regelmäßig Backups und Wiederherstellungstests gemacht?

4. Schulung und Richtlinien

JA NEIN

- Ist der Umgang mit der IT und den Daten in Betriebsvereinbarungen bzw. Arbeitsanweisungen geregelt?
- Werden alle Mitarbeiter bei Einstellung sowie regelmäßig zum Thema IT-Sicherheit und Datenschutz sensibilisiert?

5. Compliance/Ordnungsmäßigkeit beim Outsourcing

JA NEIN

- Sind beim Outsourcing die Sicherheitsanforderungen und -verantwortlichkeiten vertraglich festgelegt?
- Werden beim Outsourcing die gesetzlichen Vorgaben des § 11 BDSG stets beachtet?
- Werden Leistungserbringer wie Baumaßnahmen (z. B. in der Nähe des Serverraums) oder Reinigungskräfte im Unternehmen überwacht bzw. gibt es hierzu verbindliche Regeln?