

| Kriterium/Punkte | Ja 3 | Nein 1 | Offen 2 |
|--|---------|-----------|------------|
| Pflicht zur Bestellung eines Datenschutzbeauftragten | | | |
| Werden im Unternehmen Einzelangaben über persönliche oder sachliche Verhältnisse von natürlichen Personen (personenbezogene Daten) verarbeitet? | | | |
| Falls ja, erfolgt die Verarbeitung automatisiert, z. B. mit Hilfe von Computern? | | | |
| Sind mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten befasst? | | | |
| Ist ein Datenschutzbeauftragter bestellt worden? | | | |
| Zwischensumme | | | |
| Technisch-organisatorische Aspekte (nur wenn bisher mehr als 5 Punkte erreicht wurden) | | | |
| Liegt eine interne Verfahrensübersicht bzw. ein Verzeichnisse vor? | | | |
| Wurden Verfahren bei der zuständigen Aufsichtsbehörde angemeldet ? | | | |
| Sind alle Mitarbeiter/innen, die personenbezogene Daten bearbeiten, auf das Datengeheimnis verpflichtet und wurde dieses dokumentiert? | | | |
| Wurden alle Mitarbeiter/innen durch Schulungen ausreichend sensibilisiert? | | | |
| Ist für jede Bearbeitung personenbezogener Daten festgelegt, zu welchem Zweck sie erfolgt bzw. auf Grund welcher Rechtsgrundlage und mit Hilfe welcher Verfahren die Bearbeitung erfolgt? | | | |
| Sind zentrale IT-Systeme in geschützten Räumen eingerichtet, so dass nur Berechtigte Zutritt haben und nachvollzogen werden kann, wer wann Zutritt erlangte? | | | |
| Existiert ein abgestuftes Berechtigungs- und Zugriffskonzept für Benutzer und Gruppen? | | | |
| Gibt es eine aktuelle, verbindliche und betriebsübergreifende Sicherheitsrichtlinie ? | | | |
| Wurden Vorgaben für die Benutzung von Internet und E-Mail -Diensten erarbeitet? | | | |
| Sind die einschlägigen datenschutzrechtlichen Bestimmungen in einer aktuellen Fassung im Unternehmen zentral einzusehen? | | | |
| Sind die einschlägigen Aufbewahrungsfristen bekannt und werden sie beachtet? | | | |
| Sind verbindliche Fristen zur Löschung personenbezogener Daten festgelegt und werden sie regelmäßig kontrolliert? | | | |

| Kriterium/Punkte | Ja 3 | Nein 1 | Offen 2 |
|---|---------|-----------|------------|
| Ist eine aktuelle, vollständige und nachvollziehbare Systemdokumentation (z. B. eingesetzte Hard- und Software, Patchfeldbelegung) vorhanden? | | | |
| Ist eine Datensicherung nach dem Generationensystem oder Vergleichbares mit einem rückwärtigen Datenbestand von mindestens einem Jahr realisiert? | | | |
| Wird regelmäßig überprüft, ob eine Rekonstruktion der gesicherten Daten tatsächlich möglich ist? | | | |
| Werden personenbezogene Daten an Dritte (z. B. zur Vertragsabwicklung, Abrechnung oder an externe Schreibbüros) weitergegeben und sind in den entsprechenden Verträgen Regelungen zum Datenschutz enthalten? | | | |
| Existiert eine aktuelle, einheitliche und konsistente Lösung zum Virenschutz ? | | | |
| Gibt es eine verbindliche Regelung zur ausschließlichen dienstlichen Nutzung der Informationstechnik (einschließlich Fax, E-Mail, Internet, Software etc.)? | | | |
| Ist verbindlich geregelt, unter welchen Bedingungen Datenträger außer Haus mitgenommen werden dürfen? | | | |
| Ist bei Wartung bzw. Fernwartung von Systemen in Ihrem Unternehmen sichergestellt, dass die Dienstleister keinen Zugriff auf personenbezogene Daten erhalten können? | | | |
| Ergebnis: | | | |

Bewertung:

72-69 Punkte: Sehr gut. Datenschutz wird in Ihrem Unternehmen ernst genommen und die erforderlichen Maßnahmen wurden erfolgreich implementiert. Überprüfen Sie regelmäßig die Wirksamkeit der ergriffenen Maßnahmen, um das hohe Niveau zu halten.

68-57 Punkte: Gut. In Ihrem Unternehmen werden die Vorgaben für den Datenschutz weitgehend befolgt. Die noch existierenden Schwachpunkte sollten möglichst bald festgestellt werden und eine Lösung der offenen Punkte angestrebt werden.

56-37 Punkte: Handlungsbedarf. Es besteht das dringende Erfordernis, die Situation des Datenschutzes in Ihrem Unternehmen kritisch zu betrachten, Missstände zu erkennen und diese wirkungsvoll zu beheben. Das Unternehmen verstößt gegen gesetzliche Regelungen.

Bis 37 Punkte: Akuter Handlungsbedarf. Achtung! In Ihrem Unternehmen bestehen schwere Lücken im Hinblick auf die datenschutzrechtlichen Vorschriften. Es besteht die Gefahr, dass auch der Bereich Sicherheit betroffen ist und somit schwerwiegende Folgen verursachen kann.