Basis-Checkliste Datenschutz

Mandant/Unternehmen: _____

Ansprechpartner: _____

Ort/Datum: _____

	Ja/Nein	Bemerkung
Bestellung eines Datenschutzbeauftragten		
Verarbeiten Sie personenbezogene Daten in Ihrem Unternehmen?		
Verarbeiten Sie diese Daten automatisiert (z.B. unter Zuhilfenahme von Computern)?		
Sind in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt?		
Verarbeiten Sie Daten, die Daten mit hohem Risiko für das Persönlichkeitsrecht des Betroffenen (z.B. Gesundheitsdaten) enthalten?		
Verarbeiten Sie Daten geschäftsmäßig zum Zweck der Übermittlung (z.B. Auskunfteien), der anonymisierten Übermittlung oder der Markt- und Meinungsforschung?		
Wenn hier mindestens eine Frage mit „Ja“ angekreuzt wurde:		
Haben Sie einen Datenschutzbeauftragten schriftlich bestellt?		
Allgemeine Angaben zum Datenschutz		
Existiert eine Datenschutzrichtlinie oder ein Datenschutzkonzept?		
Wurden die Mitarbeiter zur Geheimhaltung personenbezogener Daten verpflichtet?		
Werden die Mitarbeiter regelmäßig über das Thema Datenschutz belehrt und geschult?		
Existiert in Ihrem Unternehmen ein Verzeichnis Ihrer Verarbeitungstätigkeiten mit Angaben zur Datenherkunft, zur Rechtsgrundlage der Verarbeitung, zu Berechtigungskonzepten und zu den getroffenen Datenschutzmaßnahmen?		
Werden Daten in Staaten außerhalb der EU übertragen?		

Haben Sie externe Unternehmen zur Erledigung Ihrer Arbeiten (Auftragsverarbeiter; z.B. Steuerberater, IT-Dienstleister, etc.) eingebunden?		
Wenn ja, haben Sie eine Übersicht über diese Auftragsverarbeiter?		
Haben Sie mit diesen Auftragsverarbeitern schriftliche Vereinbarungen getroffen (Mindestinhalt nach Art. 28 Abs. 3 DSGVO)?		
Werden vertrauliche Unterlagen in Ihrem Unternehmen zugriffsgeschützt gelagert und entsorgt?		
Sind die einschlägigen Aufbewahrungsfristen bekannt?		
Werden Fristen zur Löschung personenbezogener Daten eingehalten und wird dieses regelmäßig kontrolliert?		
Arbeitnehmerdatenschutz		
Erheben Sie Arbeitnehmerdaten?		
Werden personenbezogene Arbeitnehmerdaten an andere Unternehmen übermittelt oder haben andere Unternehmen Zugriff auf diese Daten?		
Werden besonders schützenswerte Daten der Arbeitnehmer erhoben (z.B. Gesundheitszustand, politische Meinungen, Religionszugehörigkeit, Angaben über die Persönlichkeit des Mitarbeiters)?		
Ist geregelt, wie Arbeitnehmern die Einsicht in die über sie gespeicherten Daten gewährt wird?		
Werden elektronische Daten über Bewerbungen (z.B. per E-Mail oder Online-Formular) im Falle einer Absage gelöscht?		
Sind die Löschungsfristen schriftlich festgehalten?		
Internetzugang für Arbeitnehmer		
Existiert in Ihrem Unternehmen eine schriftliche Vereinbarung über private Nutzung des Internetzugangs und der E-Mail-Nutzung?		
Sind die private Nutzung des Internetzugangs und die Versendung privater E-Mails in Ihrem Unternehmen verboten?		
Werden Daten bei der Internet- und E-Mail-Nutzung protokolliert?		
Ist geregelt, welcher Mitarbeiter unter welchen Voraussetzungen Zugang zu den Protokollen erhält?		

Kundendatenschutz		
Erheben, speichern oder nutzen Sie Kundendaten?		
Erfolgt eine Übermittlung dieser Daten an Dritte (z.B. andere Unternehmen)?		
Haben Sie eine Datenschutzrichtlinie auf Ihrer Homepage und ist diese für Kunden einsehbar?		
Verwenden Sie auf Ihrer Homepage einen Geotracker (z.B. Google-Analytics)?		
Verwenden Sie Cookies auf Ihrer Webseite?		
Werden personenbezogene Daten im Internet verschlüsselt übertragen (z.B. über SSL)?		
Wird Kunden auf Anfrage Einsicht in die über sie gespeicherten Daten gewährt?		
Ist dieser Prozess geregelt?		

Datensicherung (Backup)		
Existiert in Ihrem Unternehmen ein Datensicherungskonzept (mit Angaben darüber, wie und in welchen Abständen Daten gesichert werden)?		
Ist der Zugang zu Serverräumen nur für Berechtigte möglich? (Zutrittskontrolle)		
Werden Datensicherungen auf externe Datenträger vorgenommen?		
Wenn ja, werden die Backupdaten auf dem externen Medium verschlüsselt abgelegt?		
Wird mindestens einer der externen Datenträger an einem anderen Ort (z.B. anderes Gebäude, Bankschließfach, etc.) aufbewahrt?		
Wird regelmäßig eine Wiederherstellungsprüfung durchgeführt?		
Ist das Verfahren zur Rekonstruktion des Systems im Notfall ausreichend dokumentiert (Notfall-Handbuch)?		