Checkliste: Datenschutz im Homeoffice sicherstellen

Die folgende Checkliste kann ein erster Ansatz für Sie als Arbeitgeber sein, um die Datenschutzregelungen im Homeoffice richtig umzusetzen und die Schutzpflicht zu erfüllen.

Diese Liste ist nicht allumfassend, sondern soll als Beispiel dienen und kann beliebig erweitert werden bzw. individuell für Ihr Unternehmen angepasst werden.

Achten Sie darauf, dass wir für die Richtigkeit und Vollständigkeit der Liste keine Garantie übernehmen.

- Bevor Sie die Checkliste nutzen, können Sie sich zunächst umfassend in unserem Ratgeber informieren. Lesen Sie dazu den Beitrag „Datenschutz im Homeoffice“.
- Damit Sie sichergehen können, dass die Checkliste den Anforderungen Ihres Unternehmens vollständig genügt, können Sie einen Anwalt zur Unterstützung und Beratung kontaktieren.
- advocado findet für Sie den passenden Anwalt aus einem Netzwerk mit über 500 Partner-Anwälten. Dieser kontaktiert Sie innerhalb von 2 Stunden für eine kostenlose Ersteinschätzung zu Ihrem Anliegen.

Für eine kostenlose Ersteinschätzung von einem unserer Partner-Anwälte können Sie einfach hier Ihre Rechtsfrage eingeben: www.advocado.de/rechtsfrage-stellen.html

Checkliste Datenschutz im Homeoffice:

- **Arbeitsmittel**
  Welche Arbeitsmittel (z. B. Laptops oder Datenträger) dürfen für welchen Zweck von den Mitarbeitern im Homeoffice genutzt werden und welche nicht?

- **Datenschutz**
  Bestimmungen der DSGVO einhalten
  Ggf. Datenschutzschulungen, um Mitarbeiter für den Schutz personenbezogener Daten zu sensibilisieren.

- **Datensicherung**
  Mitarbeiter dazu anhalten, alle gespeicherten Daten regelmäßig auf unternehmensinternen Servern zu sichern.

- **Löschung & Vernichtung von Daten**
  Genaue Vorgaben bei der Löschung und Vernichtung personenbezogener Daten

- **Passwortsicherheit**
  Empfehlung des Bundesamts für Sicherheit in der Informationstechnik (BSI): Passwörter mit mindestens 8 Zeichen, Groß- und Kleinbuchstaben, Sonderzeichen sowie einer Zahl bestehen.

- **Private Software**
  Nutzung privater Software für die Verarbeitung personenbezogener Daten ggf. untersagen.

- **Schutz vertraulicher Informationen**
  Schutz personenbezogener und unternehmensinterner Daten gewährleisten

- **Technischer Support**
  Support für Hardware- und Softwareprobleme damit Mitarbeiter ihre Aufgaben trotz technischer Probleme erfüllen können.

- **Updates**
  Software und Systeme regelmäßig aktualisieren, damit alle verwendeten Tools den vollen Funktionsumfang bieten und Sicherheitsmaßnahmen ihren vollen Schutzumfang entfalten können.

- **Verbindungssicherheit**
  Ein privates WLAN-Netzwerk und darüber ausgetauschte Daten lassen sich durch die Verschlüsselung mit einem mindestens 20-stelligen Passwort schützen.

- **Zugriffsberechtigungen**
  Jeder Mitarbeiter kann nur über die Berechtigungen für Software verfügen, die er für die Erledigung seiner Aufgaben benötigt.