Muster-Richtlinie zur Heimarbeit (Home Office)

1. EINLEITUNG

Sofern den Beschäftigten des Unternehmens die Heimarbeit („Home-Office“) erlaubt wird, sind die Vorgaben aus dieser „Richtlinie zur Heimarbeit („Home-Office“) für die betreffenden Beschäftigten verbindlich einzuhalten. Um eine rechtskonforme Verarbeitung von personenbezogenen Daten im „Home-Office“ zu gewährleisten, sind neben den allgemeinen Verhaltensanweisungen dieser Richtlinie auch ergänzende Weisungen durch Vorgesetzte an die Beschäftigten möglich. Auch diesen ist Folge zu leisten.

2. GELTUNGSBEREICH

Diese Richtlinie gilt für die Verarbeitung personenbezogener Daten durch Beschäftigte im „HomeOffice“. Diese Richtlinie gilt für alle Standorte des Unternehmens. Diese Richtlinie verpflichtet alle Beschäftigten zur Einhaltung der hier festgelegten Pflichten und Vorgaben, soweit Verarbeitung personenbezogener Daten im „Home-Office“ erfolgt.

3. ZIELE

Diese Richtlinie soll dazu beitragen, dass die Rechtsvorschriften zur Verarbeitung personenbezogener Daten eingehalten werden und insbesondere die Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten gewährleistet werden kann.

4. GRUNDSÄTZE FÜR DEN UMGANG MIT PERSONENBEZOGENEN DATEN

Die nachfolgenden Grundsätze sind von allen Beschäftigten einzuhalten, die im „Home-Office“ arbeiten: Es wird ausschließlich die vom Unternehmen bereitgestellte oder genehmigte Hard- und Software genutzt. Alle Beschäftigten sind verpflichtet, alle sie oder ihre Tätigkeit betreffenden Richtlinienvorgaben oder Anweisungen im Umgang mit personenbezogenen Daten auch bei der Arbeit im „Home-Office“ einzuhalten. Dies gilt insbesondere für Vorgaben, die die Sicherheit personenbezogener Daten betreffen. Beschäftigte melden mögliche Datenschutzvorfälle unverzüglich an das Datenschutzteam (DST) oder die dafür vorgesehene interne Organisationseinheit. Ein Datenschutzvorfall liegt insbesondere vor, wenn die Annahme besteht, dass die Datensicherheit, insbesondere die Vertraulichkeit von Daten, gefährdet sein kann. Ein Datenschutzvorfall liegt auch bei jedem Sachverhalt vor, bei dem die Annahme besteht, dass Dritte unbefugt Zugriff oder Zugang zu personenbezogenen Daten haben oder hatten.

5. GRUNDSÄTZE DER NUTZUNG IT-SYSTEMEN IM „HOME-OFFICE“

Die Verarbeitung von personenbezogenen Daten im „Home-Office“ birgt Risiken für die Integrität, Vertraulichkeit und Verfügbarkeit von Daten in sich. Um diese Risiken auszuschließen oder zu minimieren, sind die nachfolgenden Grundsätze bei der Verarbeitung von personenbezogenen Daten im „Home-Office“ durch die Beschäftigten einzuhalten. Daten sind grundsätzlich nicht auf lokalen Festplatten oder Datenspeichern von Endgeräten zu speichern, die nicht im Eigentum oder Besitz des Unternehmens stehen. Die Speicherung von Daten hat grundsätzlich in den Verzeichnissen/Ordnern von Servern bzw. zentralen IT-Systemen des Unternehmens zu erfolgen, die für den Benutzer freigegeben sind. Ausnahmen hiervon dürfen nur gemacht werden, wenn eine Internet-Anbindung an die zentralen IT-Systeme und damit eine Speicherung auf den IT-Systemen nicht möglich ist. In diesen Fällen dürfen personenbezogene Daten auf den von den Beschäftigten im „Home-Office“ verwendeten

Geräten gespeichert werden, wenn sichergestellt ist, dass die Daten auf den verwendeten Datenträgern verschlüsselt gespeichert werden. Beschäftigte, die nicht sicher sind, ob ihre verwendeten Datenträger verschlüsselt speichern, könnten dies beim IT-Support nachfragen. Beschäftigte, die im „Home-Office“ arbeiten, haben sicherzustellen, dass andere Personen keinen Zugang zu den im Zusammenhang mit der Beschäftigung verarbeiteten Daten erhalten. Dies gilt insbesondere für Personen, die in demselben Haushalt leben. Beschäftigte müssen daher beim Verlassen des „Home-Office“-Arbeitsplatzes unverzüglich eine Bildschirmsperre aktivieren, die nur mit einem Passwort aufgehoben werden kann, welches ausschließlich dem Beschäftigten bekannt ist. Dokumente sollten grundsätzlich nicht im „Home-Office“ ausgedruckt werden. Sollte dies für die Erledigung von betriebsbedingten Aufgaben zwingend erforderlich sein, hat der Beschäftigte Sorge dafür zu tragen, dass die ausgedruckten Informationen auch direkt vor Ort geeignet vernichtet werden können. Im Hinblick auf die Installation von Software auf den mobilen IT-Systemen gilt die „IT-Richtlinie für Nutzer“. Besonders schutzbedürftige Informationen sollten nach Möglichkeit nur an Orten im „Home-Office“ verarbeitet werden, die von Dritten nicht einzusehen sind. Sollte dies nicht möglich sein, muss der Nutzer einen Ort bzw. Platz zur Verarbeitung von Daten wählen, der gewährleistet, dass der Bildschirm nicht von Dritten eingesehen werden kann.

6. DATENSICHERUNG

Der Nutzer hat Sorge dafür zu tragen, dass Daten, die ausschließlich auf dem Gerät gespeichert werden, bei nächster Gelegenheit auf Datenspeicher übertragen werden, die üblicherweise für die Speicherung von Unternehmensdaten zugelassen sind. Diese Regelung folgt der IT-Richtlinie für Speicherorte. Bei Fragen zu der Vorgehensweise der Übertragung der Daten hat sich der Nutzer an die IT-Abteilung zu wenden.

7. AUSNAHMEN

Die Unternehmensleitung kann Ausnahmen von den vor genannten Grundsätzen in begründeten Einzelfällen erlauben. Genehmigte Ausnahmen sind inklusive einer Begründung zu dokumentieren.

8. SANKTIONEN

Ein Verstoß gegen diese Richtlinien kann eine arbeitsvertragliche Pflichtverletzung darstellen und entsprechend sanktioniert werden.

Wurde zur Kenntnis genommen:

_____

Datum, Unterschrift (Mitarbeiter)