DATENSCHUTZ AGENTUR
Daten. Schutz. Agenten.

Datenschutzverpflichtung - Richtlinie für die Tätigkeit im Homeoffice (Telearbeit)

Das Unternehmen XYZ GmbH

(im Folgenden „Unternehmen“) gestattet dem unterzeichnenden Mitarbeiter Arbeitsleistungen außerhalb der Geschäftsräume des Unternehmens zu erbringen (Homeoffice bzw. Telearbeit).

Der Mitarbeiter verpflichtet sich, im Rahmen der Leistungserbringung im Homeoffice folgende Maßnahmen zum Schutz personenbezogener Daten einzuhalten:

1) Weisungen

Der Mitarbeiter hat sich stets an einschlägige Weisungen des Arbeitgebers sowie die Regelungen des Arbeitsvertrags zum Datenschutz zu halten.

2) Sicherung der häuslichen Arbeitsräume

Der Mitarbeiter hat dafür zu sorgen, dass der Raum/die Räume, in denen die häusliche Telearbeit geleistet wird, für die Dauer der Telearbeit nicht von unbefugten Dritten betreten werden können. Zur häuslichen Telearbeit dürfen nur abschließbare Räume genutzt werden. Auch bei kurzzeitigem Verlassen der Arbeitsräume (z.B. zum Kaffeekochen) sind die Räume abzuschließen oder anderweitige geeignete Maßnahmen zu treffen, die den unbefugten Zugriff auf die Arbeitsmittel, Daten oder Dokumente verhindern (z.B. Wegschließen von Papierunterlagen, Sperrung des Arbeitsrechners etc.).

3) Sichtschutz

Der Mitarbeiter hat dafür zu sorgen, dass unbefugte Dritte keine dienstlichen Dokumente und Daten einsehen können. Er hat insbesondere dafür zu sorgen, dass der Arbeitsbildschirm von Laptops oder Dokumente nicht „im Vorbeigehen“ einsehbar ist. Dies kann durch Blickschutzfolien oder die Aufstellung von Computerbildschirmen außerhalb des Sichtfelds von Türen und Fenstern gewährleistet werden.

4) Akustischer Schutz

Der Mitarbeiter hat sicherzustellen, dass dienstliche Gespräche nicht von unbefugten Dritten mitgehört werden können. Er hat insbesondere dafür zu sorgen, dass am Telearbeitsplatz keine akustischen Assistenzsysteme (z.B. Alexa) vorhanden sind.

5) Mobiles Arbeiten / Co-Working-Spaces

Der Mitarbeiter ist berechtigt, die Telearbeit außerhalb ihrer häuslichen Arbeitsstätte (z.B. in Co-Working-Spaces) durchzuführen. Er hat dabei jedoch dafür zu sorgen, dass seine Arbeitsunterlagen und Arbeitsmittel vor dem Zugriff unbefugter Dritter geschützt sind. Zu keinem Zeitpunkt sind Arbeitsunterlagen und Arbeitsmittel unbeaufsichtigt zu lassen. Bei der Nutzung von Internetanschlüssen ist die geeignete Sicherung des genutzten Netzwerks sicherzustellen. Bei dem Transport der Arbeitsunterlagen und Arbeitsmittel zum und vom Telearbeitsplatz hat der Mitarbeiter diese stets im Blick zu behalten. Die Arbeitsunterlagen und Arbeitsmittel haben zu jeder Zeit unter Kontrolle des Mitarbeiters zu verbleiben.

6) Nutzung öffentlicher Internetzugänge

Der Mitarbeiter hat vorrangig seinen privaten Internetzugang für die Telearbeit zu nutzen. Dieser ist in geeigneter Weise zu sichern. Öffentliche und/oder fremde Netzwerke (z.B. in öffentlichen Räumen oder Hotels) dürfen nicht benutzt werden, es sei denn, die Sicherheit der Verbindung ist sichergestellt.

*Ergänzen Sie die Richtlinie mit Ihren individuellen Gegebenheiten und Anforderungen.
*Lassen Sie die fertiggestellte Richtlinie von Ihrem Datenschutzbeauftragten prüfen.

7) Im Ausland

Das Verbringen von Arbeitsunterlagen und Arbeitsmitteln in das Ausland sind nur mit ausdrücklicher Zustimmung des Unternehmens erlaubt. Der Mitarbeiter hat das Unternehmen vor der Verbringung von Arbeitsmitteln und Arbeitsunterlagen in das Ausland ausdrücklich darüber aufzuklären und die Zustimmung einzuholen.

8) Datensicherung

Der Mitarbeiter muss Daten, stets entsprechend der Vorgaben des Unternehmens sichern. Werden Daten lokal auf den Arbeitsmitteln gespeichert, sind sie bei nächster Gelegenheit auf Datenspeicher zu übertragen, die das Unternehmen üblicherweise für die Speicherung von Daten verwendet.

9) Zugangsrecht

Der Mitarbeiter hat dem Unternehmen oder dessen Mitarbeitern - nach vorheriger Absprache - Zugang zu seiner häuslichen Arbeitsstätte zu gewähren. Dies ist insbesondere dann der Fall, wenn die Einhaltung dieser Vereinbarung kontrolliert werden muss oder die Einhaltung datenschutzrechtlicher Bestimmungen geprüft werden soll (zum Beispiel durch den Datenschutzbeauftragten des Unternehmens). Der Zugang ist nur zwischen/zu den gängigen Geschäftszeiten zwischen 10 – 17 Uhr zu gewähren. In dringenden Fällen muss der Zugang ohne vorherige Absprache gewährt werden. Die Grundrechte und Grundfreiheiten der Mitarbeiter sind stets einzuhalten.

10) Einhaltung allgemeiner Sicherheitsstandards

Der Mitarbeiter hat im Rahmen der Telearbeiter folgende allgemeinen Sicherheitsmaßnahmen einzuhalten:

Der Mitarbeiter hat sichere Passwörter zu wählen und diese geheim zu halten. Der Mitarbeiter ist verpflichtet alle verfügbaren Sicherheitsupdates auf seinen Dienstgeräten unverzüglich zu installieren. Arbeitsmittel und Arbeitsunterlagen sind nur im Rahmen der konkreten Aufgabenerledigung innerhalb des Arbeitsplatzes zu nutzen. Nach Beendigung der jeweiligen Aufgabe sind die entsprechenden Arbeitsmittel und Arbeitsunterlagen sicher zu verwahren (Clean-Desk-Policy). Computer, Notebook und sonstige elektronische Dienstgeräte sind bei Verlassen des Arbeitsplatzes zu sperren und vor Diebstahl zu sichern. Dies gilt auch bei kurzfristigem Verlassen des Arbeitsplatzes (z.B. zum Kaffeekochen oder zur Mittagspause). Der Mitarbeiter hat beim Zugriff auf die IT-Systeme des Unternehmens den vom Unternehmen bereitgestellten VPN-Zugang zu nutzen.

11) Meldung von Verstößen

Wenn personenbezogene Daten verletzt werden oder eine solche Verletzung droht (z.B. Verlust von Arbeitsgeräten oder Dokumenten, Hacker-Angriffen, Angriffen durch Schadsoftware etc.), hat der Mitarbeiter umgehend die Geschäftsführung, Vorgesetzten oder den Datenschutzbeauftragten zu informieren. Bei IT-Verstößen ist ferner unverzüglich die IT-Abteilung zu informieren.

12) Ausnahmen

Dem Unternehmen steht es frei, Ausnahmen von den vor genannten Grundsätzen in begründeten Fällen zu genehmigen. Solche Ausnahmen sind unter Verweis auf die Genehmigung und Begründung zu dokumentieren.

13) Wichtige Kontaktdaten für:

IT-Notfälle:
Datenschutzbeauftragter: Datenschutz Agentur | Telefon: 0821 90786450 | epost@datenschutz-agentur.de

*Ergänzen Sie die Richtlinie mit Ihren individuellen Gegebenheiten und Anforderungen.
*Lassen Sie die fertiggestellte Richtlinie von Ihrem Datenschutzbeauftragten prüfen.