Leitfaden

zum Umgang mit IT und Dokumenten im „Homeoffice“

Grundsätze

Sie sind als Mitarbeitende im Homeoffice eingeteilt. Homeoffice im Sinne dieses Leitfadens meint insbesondere mobiles Arbeiten und Bring-Your-Own-Device (BYOD). Mobiles Arbeiten zeichnet sich dadurch aus, dass Ihnen von Ihrem Arbeitgeber ein mobiles Endgerät zur Verfügung gestellt wurde, ihr Arbeitsplatz zu Hause aber nicht auf Dauer eingerichtet ist. Beim Arbeiten via BYOD stellen Sie Ihr privates Endgerät zur Arbeitsleistung zur Verfügung.

Hiervon nicht umfasst ist grundsätzlich die Telearbeit, die einen auf Dauer ausgelegten Arbeitsplatz im privaten Bereich bezeichnet und einer zusätzlichen Betrachtung bedarf.

Arbeiten im Homeoffice erfordert von Ihnen eine besondere Sensibilität im Umgang mit personenbezogenen Daten. Es besteht ein gesteigertes Risiko der unberechtigten Kenntnisnahme Dritter, insbesondere aus Ihrem familiären Bereich.

Datenschutz

Datenschutz befasst sich insbesondere mit dem Schutz personenbezogener Daten. „Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Neben dem Schutz personenbezogener Daten sind Sie ebenso arbeitsrechtlich verpflichtet, keine Geschäftsgeheimnisse zu offenbaren.

Technische Maßnahmen

Grundsätzlich haben Sie dieselben technischen Schutzmaßnahmen einzurichten, als wären Sie an Ihrem festen Arbeitsplatz im Unternehmen tätig.

Im Falle von mobilem Arbeiten erhalten Sie ein vom Unternehmen eingerichtetes Endgerät. Ihre Aufgabe liegt nun vor allem darin, Ihr Heimnetzwerk sicher zu gestalten. Sollten Sie einen W-LAN-Router nutzen, muss dieser passwortgeschützt sein. Es bietet sich hierbei der Standard WPA-2 als Verschlüsselungsmethode an, welcher in den meisten Fällen als Standard eingestellt ist. Aufgrund der Umstände bietet es sich an, dieses jetzt einmal neu zu erstellen. So können Sie sichergehen, dass Sie die Kontrolle auf Zugriffe auf Ihr Heimnetzwerk beibehalten und nur Personen hierauf zugreifen können, denen Sie vertrauen. Das Passwort muss sich vom Admin-Passwort auf dem Router unterscheiden.

Abschließend sollten Sie überprüfen, ob Ihr Router auch alle aktuellen Updates eingespielt hat, da hierdurch in der Regel signifikante Sicherheitslücken geschlossen werden.

Im Falle von BYOD sind die eben genannten Maßnahmen ebenso einzurichten und sicherzustellen. Da Ihr Gerät aber keinem direkten Zugriff Ihrer Unternehmens-IT-Abteilung unterliegt, bedarf es Ihrerseits einen Standard selbst einzurichten. Ihr Endgerät muss passwortgeschützt sein und dieser Account darf nicht mit anderen Personen in Ihrem Haushalt geteilt werden. Richten Sie eine Bildschirmsperre ein. Diese sollte bestenfalls nach zwei Minuten Inaktivität aktiviert werden. Außerdem muss ein Antivirenprogramm auf Ihrem Endgerät aktiv sein. Auf Microsoft Rechnern ist typischerweise der Windows-Defender installiert. Installieren Sie außerdem alle notwendigen Updates auf Ihrem Rechner. Sollten Ihr Endgerät noch auf Windows 7 basieren, halten Sie bitte Rücksprache mit Ihrer IT-Abteilung, ob eine andere Lösung gefunden werden kann, da Windows-7-Rechner keine Sicherheitsupdates mehr erhalten.

Ein Zugriff auf unternehmensinterne Daten und Ordner wird typischerweise via eines VPN-Zugriffes ermöglicht werden. Speichern Sie Daten nicht lokal auf Ihrem eigenen Rechner, sondern ausschließlich direkt innerhalb der IT-Infrastruktur in Ihrem Unternehmen.

Falls Sie USB-Sticks benutzen müssen, verwenden Sie ausschließlich sichere, aus bekannter Herkunft und auf Viren geprüfte. Diese sollten im Regelfall verschlüsselt werden. Bitlocker 2 Go ist hierzu eine konforme Lösung.

Falls Sie weitere Fragen zur technischen Einrichtung haben, richten Sie sich an Ihre IT-Abteilung. Diese hilft Ihnen gerne weiter.

Paperwork

Ausdrucke und Aktenordner bedürfen einer besonderen Aufsicht. Falls Sie zwingend notwendige Aktenordner mit nach Hause genommen haben, sind auch diese jederzeit vor unberechtigtem Zugriff zu schützen. Alle Ausdrucke und Ordner müssen daher in einem nur für Sie zugänglichen abschließbaren Fach oder dergleichen aufbewahrt werden. Darüber hinaus ist die Nutzung der eigenen Drucker auf das notwendige Maß zu reduzieren. Seien Sie sich im Klaren, dass Netzwerkdrucker möglicherweise auch für andere sichtbar sind. Sichern Sie diese ebenso vor unberechtigtem Zugriff. Abschließend dürfen Firmendokumente nicht einfach ungeschreddert im Hausmüll landen. Diese sollten in jedem Fall bestmöglich nicht wiederherstellbar entsorgt werden.

Datenschutzvorfälle

Datenpannen und Angriffe auf die Integrität der IT können im häuslichen Bereich wenigstens genauso leicht vorkommen, wie im Unternehmen. Allerdings liegt die Kenntnisnahme dessen meist lediglich bei Ihnen. Es ist essentiell, dass Sie hiermit richtig umgehen und Vorfälle unverzüglich melden. Hierzu zählen die mögliche unberechtigte Kenntnisnahme Dritter, beispielsweise auch Familienangehörige, die sich bei kurzer Abwesenheit an Ihren Rechner setzen und möglicherweise dadurch Zugriff auf relevante

Daten haben. Ebenso aber auch die Feststellung eines Virus auf Ihrem Rechner. Trennen Sie dann unbedingt Ihre IT vom Internet und informieren Sie Ihre IT-Abteilung. Schließlich besteht immer die Gefahr einer Phishing-Attacke, woraus sich weitreichende Folgenden für die Integrität und Vertraulichkeit der Daten ergeben können. Leiten Sie verdächtige E-Mails keinesfalls weiter, auch nicht an Ihre IT-Abteilung.

Falls Ihnen irgendetwas Ungewöhnliches auffallen sollte, nehmen Sie bitte immer direkt Kontakt zu Ihrem Datenschutzbeauftragten und Ihrer IT-Abteilung auf. Dort wird das Risiko eingeschätzt und über weitere Maßnahmen entschieden.

Diese sind telefonisch erreichbar unter:

IT-Abteilung: _____

Datenschutzbeauftragter: _____

Vielen Dank, dass Sie sich für die Sicherheit im Unternehmen einsetzen. Befolgen Sie diese Schritte um Daten, Personen und damit auch das Unternehmen zu schützen.