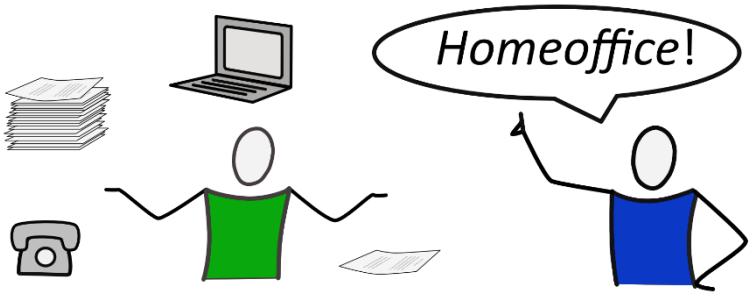
Datenschutz: Plötzlich im Homeoffice – und nun?

Im Zuge der Corona-Pandemie hat sich vieles im Alltagsleben sehr schnell verändert. Dazu gehört auch das Arbeiten von Zuhause (Homeoffice, Telearbeit). Üblicherweise ist die Einrichtung eines Heim-Arbeitsplatzes mit viel Vorbereitung verbunden, um zum Beispiel auch den Datenschutz am heimischen Arbeitsplatz in gleichem Maße wie im Büro zu gewährleisten.



Falls Sie sehr spontan ins Homeoffice wechseln mussten, haben wir einige einfache Regeln und Hinweise für den Umgang mit personenbezogenen Daten, die Sie auch sofort umsetzen können.

Vom Büro ins Homeoffice

Beim Wechsel ins Homeoffice nehmen Sie vermutlich Dokumente und IT-Geräte vom Arbeitsplatz mit nach Hause. Achten Sie dabei darauf, dass beispielsweise ihr Laptop nicht nur mit einem sicheren Passwort geschützt ist, sondern auch die Festplatte sowie externe Speichermedien verschlüsselt sind. Papierdokumente werden am besten in einem verschließbaren Behälter mitgenommen.

Und wie immer gilt: Lassen Sie Ihre Sachen nicht unbeaufsichtigt!

Arbeitsplatz im Homeoffice einrichten

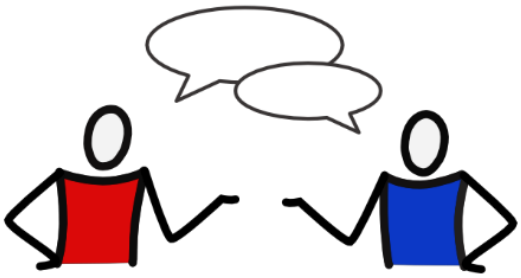
Achten Sie bei der Einrichtung ihres Arbeitsplatzes in den eigenen vier Wänden nicht nur darauf, dass Sie ungestört, angenehm und effektiv arbeiten können:

- Am besten ist ein Arbeitsplatz in einem eigenen Raum oder in einer eigenen Ecke. Wählen Sie den Platz so, dass andere nicht den Bildschirm sehen können – auch nicht durch ein Fenster. Eine Sichtschutzfolie für den Monitor kann dies unterstützen.

- Wenn Sie Ihren privaten Internet-Anschluss verwenden: Richten Sie Ihren Computer so ein, dass er mit dem privaten Netzwerk durch ein Kabel oder ein verschlüsseltes WLAN verbunden ist. Ihr WLAN sollte ohnehin so eingerichtet sein, dass man sich nur mit einem Passwort einwählen kann.
- Finden Sie einen geeigneten Platz, um Papier-Dokumente zu lagern. Dokumente mit personenbezogenen Daten müssen verschlossen aufbewahrt werden, am besten in einem verschlossenen Raum oder Behälter. Achten Sie auch darauf, dass Ihre Geräte und Speichermedien nicht zugänglich sind, wenn Sie den Raum verlassen, z. B. abends nach getaner Arbeit.

Nachdem Sie dies alles beachtet haben, überlegen Sie noch einmal selber, wo Risiken lauern können.

Mit Vorgesetzten und im Kollegium zu klären



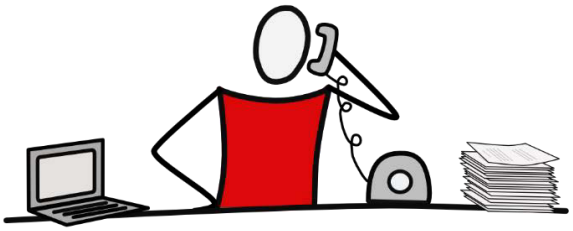
Der Arbeitsplatz zu Hause bringt einige Fragestellungen mit sich, die mit den Vorgesetzten und im Kollegium geklärt werden müssen. Üblicherweise werden die folgenden Punkte und noch mehr in einer Richtlinie oder Dienstvereinbarung geklärt; bei spontan eingerichteten Homeoffice-Arbeitsplätzen ist mindestens Folgendes zu beachten:

- Die grundlegende Frage, die Sie sich stellen sollten ist, ob Sie überhaupt dringend an Aufgaben mit personenbezogenen Daten arbeiten müssen. Wenn Sie zunächst an Aufgaben ohne Personenbezug und ohne andere sensible Daten arbeiten, können Sie sich an die neue Situation gewöhnen und Erfahrungen sammeln – dann gewinnen Sie auch Zeit für die Umsetzung dieser Regeln und Hinweise.
- Arbeiten Sie im Auftrag eines Kunden mit personenbezogenen Daten? Dann müssen Sie sicher sein, dass die Arbeit im Homeoffice nicht in der Vereinbarung über die Auftragsverarbeitung ausgeschlossen wird!
- Es ist sehr zu empfehlen, dass Sie vorrangig IT-Geräte Ihres Unternehmens bzw. Ihrer Behörde und nicht private Geräte nutzen. Es sollte Ansprechpersonen geben, falls technische Probleme auftauchen. Außerdem müssen die nötigen Sicherheitsmaßnahmen getroffen sein, z. B. das System ist auf aktuellem Stand (auf Updates achten!), Virenschutz und Firewall sind aktiv.
- In das Netzwerk Ihres Unternehmens bzw. Ihrer Behörde wählen Sie sich über eine sichere Verbindung (VPN) ein. Gegebenenfalls muss der Zugriff auf sensible Bereiche ausgeschlossen werden.
- Dokumente, an denen Sie arbeiten, und Ihre Arbeitsergebnisse speichern Sie am besten auf Datenträgern im Netz Ihres Unternehmens bzw. Ihrer Behörde. So kann auch die übliche Datensicherung (Backup) gewährleistet werden.
- Legen Sie gemeinsam fest, wie Sie untereinander und nach außen erreichbar sind und wie Sie Datenschutzrisiken vermeiden.
    - Sollen beispielsweise private Telefone verwendet werden, müssen Sie sicherstellen, dass automatisch gespeicherte Anrufkontakte regelmäßig gelöscht werden. Zumeist ist es sinnvoll, dass Ihre private Nummer bei Ihren Anrufen nicht übertragen wird, weil sonst Kundinnen und Kunden Ihre Privatnummer des Handys oder Ihres Haushalts auch in späteren Kontakten nutzen könnten. Achtung: Einige Telefonkonferenzsysteme funktionieren nur mit übertragener Rufnummer.

- Wenn Sie für die Kommunikation untereinander einen Messenger nutzen, sollte dieser für Zweier- und Gruppenunterhaltungen Ende-zu-Ende-Verschlüsselung gewährleisten. Achten Sie darauf, in Messenger-Kommunikationen keine sensiblen Informationen auszutauschen.

- Für den Fall eines Datenverlusts (z. B. Verlust von Papierunterlagen oder Datenträgern) oder eines Datenschutzverstoßes (z. B. Zugang von Unbefugten an den Computer) besteht eine Meldepflicht. Hier muss auch für das Arbeiten im Homeoffice klar sein, wem man dies unverzüglich mitteilen muss.

Beim Arbeiten im Homeoffice beachten

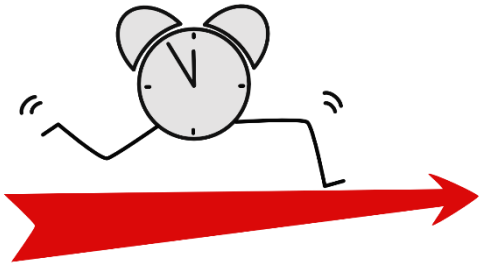


Bei der Arbeit im Homeoffice sollten Sie die gleichen Sicherheitsanforderungen wie an Ihrem Arbeitsplatz im Büro berücksichtigen. Im besten Fall sind solche allgemeinen Maßnahmen, die Mitarbeitende im Unternehmen oder in der Behörde umsetzen müssen, in Betriebs- bzw. Dienstanweisungen festgehalten. Ansonsten können Sie sich an folgenden Maßnahmen orientieren:

- Organisieren Sie Ihren Arbeitsplatz so, dass sich private und dienstliche Daten nicht mischen.
- Wenn Sie Ihren Arbeitsplatz kurzfristig verlassen, aktivieren Sie den Bildschirmschoner mit Kennwortschutz, damit niemand unberechtigt auf Ihre dienstlichen Daten zugreifen kann.
- Achten Sie beim Verlassen des Arbeitsplatzes darauf, dass Türen und – vor allem im Erdgeschoss – Fenster verschlossen bzw. geschlossen sind, um eine unbefugte Kenntnisnahme, einen Verlust oder eine Veränderung von Daten zu verhindern. Sollte dies in Ihrer häuslichen Umgebung nicht vollständig möglich sein, gehören zumindest Ihre Papierdokumente in einen verschlossenen Schreibtisch oder Schrank.
- Wenn Sie an einem dienstlichen Computer arbeiten, schließen Sie an diesem Gerät keine private Hardware (z. B. externe Festplatten oder USB-Sticks) an. So verringern Sie das Risiko, dass Schadsoftware Ihren Computer befallen und Ihre Daten kompromittiert werden. Falls der Computer doch infiziert wurde, müssen Sie dies schnellstens im Unternehmen oder in der Behörde melden – dafür müssen Sie die nötigen Kontaktinformationen (Telefon/E-Mail) griffbereit haben.
- Für den Fall, dass Sie Daten an einem **privaten** Computer verarbeiten **müssen**, achten Sie darauf, dass
  - Sie die dienstlichen Daten in einem verschlüsselten Bereich speichern. Bei der Einrichtung kann Ihnen Ihre IT-Abteilung weiterhelfen.
  - die Daten nach der Übertragung in das dienstliche Netz auf Ihrem privaten Gerät unwiederbringlich gelöscht wurden. Ein reines Verschieben in den Papierkorb mit dem entsprechenden „Leeren“ des Papierkorbs reicht nicht aus. Möglicherweise benötigen Sie zum sicheren Löschen besondere Tools – hierzu fragen Sie am besten Ihre IT-Abteilung.
- Wenn Sie Dokumente an Ihrem häuslichen Arbeitsplatz ausdrucken müssen, dann achten Sie darauf, dass Sie diese Dokumente unverzüglich aus dem Drucker entnehmen, damit andere Personen im Haushalt keine Kenntnis dieser Daten nehmen können. Achten Sie darauf, dass Sie, wenn Sie z. B. über VPN in Ihrem dienstlichen Netz arbeiten, keine Druckaufträge auf Drucker in Ihren Dienstgebäuden abschicken, da in diesem Fall unberechtigte Personen Einblick in diese Dokumente nehmen könnten.
- Werfen Sie dienstliche Papierdokumente nicht in Ihren privaten Papiermüll. In der Regel haben Unternehmen und Behörden genaue Richtlinien, wie Papiermüll entsorgt werden

muss. Sammeln Sie Ihren Papiermüll, lagern Sie ihn verschlossen und nehmen Sie ihn mit, wenn Sie wieder ins Dienstgebäude gehen. Entsorgen Sie den Papiermüll dann dort nach den geltenden Regeln.

- Wenn Sie am häuslichen Arbeitsplatz dienstlich telefonieren müssen, dann achten Sie darauf, dass Sie dafür einen ungestörten Bereich aufsuchen, damit andere Personen im Haushalt keine Kenntnis von Ihrem Telefonat nehmen können.



Wenn es länger als „kurzzeitig“ dauert

Mussten Sie sich sehr kurzfristig in den häuslichen Arbeitsbereich begeben, kann es sein, dass es in Ihrem Unternehmen bzw. in Ihrer Behörde noch kein Konzept für die Heimarbeit gibt. In dieser besonderen Situation müssen Sie, auch in Bezug auf den datenschutzkonformen Umgang mit Daten im häuslichen Bereich, versuchen, die Anforderungen mit Hilfe von mündlichen oder E-Mail-Anweisungen Ihrer Vorgesetzten oder durch die Berücksichtigung dieser Regeln umzusetzen.

Sollte sich jedoch eine unvorbereitete Homeoffice-Situation über einen längeren Zeitraum hinziehen, ist es notwendig, dass dafür in Ihrem Unternehmen bzw. in Ihrer Behörde ein schriftliches Konzept erstellt wird. In diesem Konzept müssen insbesondere die technischen und organisatorischen Maßnahmen beschrieben werden, um Daten sicher und datenschutzgerecht im Homeoffice verarbeiten zu können.

Quellen und weiterführende Informationen

- **„Telearbeit und Mobiles Arbeiten“**
  Information des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)
  Stand: Januar 2019, 20 Seiten, deutsch
  https://www.bfdi.bund.de/SharedDocs/Publikationen/Faltblaetter/Telearbeit.html

- **„Top Tips for Cybersecurity when Working Remotely“**
  Artikel der European Union Agency for Cybersecurity (ENISA)
  Stand: März 2020, englisch
  https://www.enisa.europa.eu/news/executive-news/top-tips-for-cybersecurity-when-working-remotely

- **„Home-Office? – Aber sicher!“**
  Information des Bundesamts für Sicherheit in der Informationstechnik (BSI)
  Stand: März 2020, 4 Seiten, deutsch
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.html

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Telefon: 0431 988-1200
E-Mail: mail@datenschutzzentrum.de