

Datenschutz und Datensicherheit im Homeoffice

Die aktuellen Maßnahmen zur Eindämmung der weiteren Ausbreitung von COVID-19 führen dazu, dass mehr Menschen als sonst nicht an ihrem normalen Arbeitsplatz arbeiten – im Homeoffice oder an anderen Orten außerhalb des normalen Büros. Im Folgenden finden Sie einige Hinweise zur Datensicherheit und zum Datenschutz bei der Arbeit außerhalb des Büros.

Geräte

- Achten Sie darauf, dass Geräte wie **USB-Sticks, Telefone, Laptops oder Tablets nicht verloren gehen** und dass niemand außer Ihnen dazu Zugang hat.
- Jedes Gerät sollte auf dem **aktuellen Stand** sein und über die **erforderlichen Sicherheitsupdates** verfügen. Achten Sie insbesondere auf **Aktualisierungen des Betriebssystems und von Antivirenprogrammen**.
- Verwenden Sie Ihren Computer oder Laptop an einem **sicheren Ort**, an dem Sie ihn im Auge behalten können und an dem möglichst keine unbefugten Personen den Bildschirm sehen können – vor allem, wenn Sie mit personenbezogenen Daten oder anderen vertraulichen Informationen arbeiten.
- Stellen Sie sicher, dass Ihre **Geräte ausgeschaltet oder gesperrt** und sorgfältig aufbewahrt werden, **wenn sie nicht in Gebrauch sind** oder Sie sie **unbeaufsichtigt** lassen müssen.
- Verwenden Sie **wirksame Zugriffskontrollen** (Multi-Faktor-Authentifizierung, starke Passwörter) und falls verfügbar **Verschlüsselung**, um den Zugriff auf vertrauliche Informationen zu verhindern und Folgerisiken bei Diebstahl oder Verlust zu vermeiden.
- **Im Fall von Diebstahl oder Verlust** sollten Sie dies **unverzüglich dem Arbeitgeber melden** und sofort Maßnahmen ergreifen, um möglichst eine **ferngesteuerte Speicherlöschung** in die Wege zu leiten.

E-Mails

- Halten Sie sich – falls vorhanden – an die internen **Vorgaben zur Nutzung von E-Mails innerhalb Ihres Unternehmens**.
- Verwenden Sie für arbeitsbezogene E-Mails, die personenbezogene oder vertrauliche Daten enthalten, möglichst **berufliche E-Mail-Konten**.
- Vermeiden Sie die Verwendung personenbezogener oder vertraulicher Daten in den Betreffzeilen.
- **Verschlüsseln Sie E-Mails oder angehängte Dokumente**, wenn sie personenbezogene oder vertrauliche Daten enthalten.
- Im Kontext von Covid-19 wurde bereits einem **Anstieg der Phishing-Versuche** festgestellt. Seien Sie aufmerksam und halten im Zweifelsfall Rücksprache, bevor Sie vertrauliche Daten wie Passwörter preisgeben.

Clouddienste

- Nutzen Sie nach Möglichkeit nur die **vertrauenswürdigen Netzwerke oder Cloud-Dienste Ihres Unternehmens** bzw. die Dienste, die für die Nutzung freigegeben wurden.
- Befolgen Sie die **internen Vorgaben bezüglich Cloud- oder Netzwerkzugang, Anmeldung und Datenaustausch**.

Aufzeichnungen auf Papier

- **Datenschutz** bezieht sich nicht nur auf elektronisch gespeicherte oder verarbeitete Daten, sondern auch auf **Daten**, die z.B. in **Papierform** vorliegen.
- Wenn Sie im Homeoffice an **Papierakten** arbeiten, **gewährleisten Sie die Sicherheit und Vertraulichkeit** dieser Aufzeichnungen, indem Sie
 - sie verschlossen aufbewahren, wenn sie nicht gebraucht werden,
 - sie sicher entsorgen (z.B. schreddern) bzw. sie bis zur sicheren Entsorgung am Dienstort aufbewahren und
 - sicherstellen, dass sie nicht verloren gehen oder gestohlen werden können.
- Bei Aufzeichnungen, die **besondere Kategorien persönlicher Daten** (z.B. Gesundheitsdaten) enthalten, muss besonders auf **Sicherheit und Vertraulichkeit** geachtet werden.

Videokonferenzen und Telefonate

- Führen Sie **dienstliche Telefonate und Videokonferenzen** so, dass Ihnen **niemand zuhören und bei Videokonferenzen zusehen** kann, also z. B. im Arbeitszimmer, nicht aber im Garten oder auf dem Balkon.
- Verwenden Sie für Telefonate – soweit vorhanden – ein **Diensthandy oder Diensttelefon**. Wenn Sie nicht über die Möglichkeit verfügen, Ihre Telefonate mit einem Dienstapparat zu führen, **anonymisieren Sie ggf. Ihre Rufnummer** und stellen Sie bei Herausgabe Ihrer Nummer klar, dass es sich um Ihre Privatnummer handelt und diese unter keinen Umständen weitergegeben werden darf.
- **Geben Sie ohne Rücksprache keine privaten Telefonnummern heraus**.
- Verwenden Sie für **Videokonferenzen** die von Ihrem Unternehmen **vorgegebenen Systeme und Apps** und beachten Sie die von Ihrem Unternehmen hierfür vorgegebenen Privatsphäre- und Datenschutzregelungen.