Merkblatt Datenschutz Mobile-Office

Gemeinde: *[...]*

Die Arbeit abseits des regulären Arbeitsplatzes stellt Mitarbeitende vor besondere Herausforderungen hinsichtlich Datenschutz und Datensicherheit. Die Berücksichtigung der folgenden Punkte unterstützt die Sicherheit bei der mobil-flexiblen Arbeit, auch beim Einsatz von privaten Geräten.

1. Dokumente in Papierform / Akten

- Nehmen Sie insbesondere keine Dokumente mit personenbezogenen Daten mit, wenn diese zur Aufgabenerfüllung nicht unbedingt notwendig sind.
- Sollten Sie dennoch Dokumente mitnehmen, sollten diese möglichst in einem geschlossenen und nicht einsehbaren Behältnis transportiert werden. Falls Dokumente auf elektronischen Datenträgern mitgenommen werden müssen, so gilt es diese gut zu schützen.
- Mitgeführte Papierdossiers und Ausdrucke müssen vor unberechtigtem Zugriff geschützt werden und sind in einem abschliessbaren Behältnis zu verwahren.
- Ausdrucke sowie die Nutzung von Büromaterialien sind ausschliesslich in der Arbeitszeit am regulären Arbeitsort durchzuführen.
- Entsorgen Sie mitgeführte, geschäftliche Dokumente bei Ihrer Rückkehr ins Büro sachgemäss und entsorgen Sie diese keinesfalls zu Hause.

2. Geschäftliche Informationen und Personendaten

- Alle geschäftlichen Informationen und Personendaten sind bei der mobil-flexiblen Arbeit zu schützen.
- Geschäftliche (interne und externe) Informationen und sensible Daten (z. B. Personendaten) müssen vor Einsicht durch Dritte geschützt werden, dies beinhaltet auch Familienmitglieder. Falls für die mobil-flexible Arbeit kein separater Raum zur Verfügung steht, muss der Arbeitsplatz so gewählt werden, dass kein direkter Blick auf den Bildschirm möglich ist.
- Bei der Arbeit im öffentlichen Raum (z. B. Bahn, Café, Parkanlagen, etc.) dürfen keine Arbeiten an Dokumenten mit sensiblen Daten vorgenommen werden (z. B. Personendaten). Zudem muss der Bildschirm vor dem direkten Einblick geschützt werden. Sofern das Gerät keinen Blickschutzfilter besitzt, sollen Bildschirmschutzfolien angebracht werden.
- Bei der Arbeit im öffentlichen Raum (z. B. Bahn, Café, etc.), sollten keine Telefongespräche geführt werden, die Rückschlüsse über den Inhalt der Arbeit und/oder Personen zulassen.
- Das Einwählen in öffentliche WLAN-Netze ist nicht gestattet. Für die Verbindung mit dem geschäftlichen Netzwerk darf ausschliesslich ein privates WLAN genutzt werden, das passwortgeschützt ist.
- Auf dem privaten Gerät darf die mobil-flexible Arbeit ausschliesslich auf der gesicherten Arbeitsoberfläche, getrennt von privaten Daten, stattfinden.
- Daten dürfen ausschliesslich in den dafür vorgesehenen Geschäftsablagen und nicht lokal auf den persönlichen Geräten oder externen Datenträgern gespeichert werden.

3. Kommunikationsmittel

- Private und geschäftliche E-Mails müssen auf dem privaten Gerät durch separate Apps/Software getrennt werden.
- Private E-Mail-Konten dürfen nicht für die geschäftliche Kommunikation genutzt werden.
- Der Arbeitgeber stellt den Mitarbeitenden die Videokonferenzlösung(en) ((XY)) zur Verfügung. Andere Tools dürfen nicht für geschäftliche Videokonferenzen verwendet werden.
- Private USB-Sticks und andere Datenträger dürfen nicht an die betriebseigenen Geräte angeschlossen werden.

4. Identifikation und Passwörter

- Starke Passwörter schützen Systeme und Daten vor dem Zugriff durch Unberechtigte. Auch private Geräte wie Smartphones oder Notebooks, auf denen geschäftliche Informationen gespeichert werden, müssen mit einem starken Passwort gesichert werden.
- Private Geräte, die Sie mit anderen Familienangehörigen teilen, müssen über ein eigenes Benutzerkonto, auf welches nur Sie Zugriff haben, verfügen.
- Passwörter dürfen nicht an Dritte weitergegeben werden.

5. Updates, Phishing und andere Bedrohungen

- Die Betriebssysteme und Programme auf privaten und betriebseigenen Geräten müssen immer auf dem aktuellen Stand gehalten werden. Hierfür sollen Updates regelmässig installiert werden.
- Verdächtige E-Mails sollten nicht geöffnet werden. Anhänge in Mails von unbekannten Absender*innen sollten nicht angeklickt werden. Im Zweifel ist die Absenderin oder der Absender per Telefon zu kontaktieren, damit sie oder er den Inhalt der E-Mail bestätigen kann. Bestehen weiterhin Zweifel ist der geschäftliche IT-Support sofort zu informieren.

6. Datenverlust

- Sollten Arbeitsmittel wie geschäftliche Dokumente oder IT-Geräte verloren gehen, ist dies den Vorgesetzten respektive dem IT-Support unverzüglich zu melden.