KANTON solothurn

Personalamt

Barfüssergasse 24
4509 Solothurn
Telefon +41 32 627 20 84

pa@fd.so.ch
https://so.ch

Merkblatt Datenschutz mobile Arbeit

Der Datenschutz und die Datensicherheit stellen Mitarbeitende bei der Arbeit abseits des regulären Arbeitsplatzes vor besondere Herausforderungen. Die Berücksichtigung der folgenden Punkte ist notwendig um die Sicherheit bei der mobilen Arbeit, insbesondere beim Einsatz von privaten Geräten, zu gewährleisten.

1. Geschäftliche Informationen und Personendaten

- Alle geschäftlichen Informationen und Personendaten sind bei der mobilen Arbeit zu schützen.
- Alle geschäftlichen Informationen und sensiblen Daten (bspw. Personendaten) müssen vor der Einsicht durch Dritte, inklusive vor Familienmitgliedern, geschützt werden. Dies beinhaltet die Einsicht auf den Bildschirm sowie auf physische Unterlagen.
- Falls für die mobile Arbeit kein separater Raum zur Verfügung steht, muss der Arbeitsplatz so gewählt werden, dass kein direkter Blick auf den Bildschirm und allfällige Unterlagen möglich ist.
- Beim Verlassen des Arbeitsplatzes ist immer die Bildschirmsperre zu aktivieren.
- Bei der Arbeit in öffentlichem Raum (z.B. Bahn, Café, Parkanlagen, etc.) dürfen keine Arbeiten an Dokumenten mit sensiblen Daten vorgenommen werden (z.B. Personendaten). Weiterhin müssen Bildschirm und Dokumente vor dem Einblick geschützt werden. Hierfür sollen Bildschirmschutzfolien angebracht werden, sofern das Gerät keinen Blickschutzfilter besitzt.
- Bei der Arbeit in öffentlichem Raum (z.B. Bahn, Café, Parkanlagen, etc.) und zu Hause, wenn Familienmitglieder mithören können, sollten keine Telefongespräche geführt werden, welche Rückschlüsse über den Inhalt der Arbeit und Personen zulassen.
- Es darf sich zum Zwecke der mobilen Arbeit nicht in öffentliche WLAN-Netze eingewählt werden. Für die Verbindung mit dem kantonalen Netzwerk darf ausschliesslich ein privates, mindestens WPA2 geschütztes WLAN oder die Sim Karte genutzt werden.
- Auf dem privaten Gerät darf die mobile Arbeit ausschliesslich via Remote Zugang auf der Kantonalen Umgebung, getrennt von privaten Daten, stattfinden (Stand, 1.4.2023).
- Daten dürfen ausschliesslich in den dafür vorgesehenen Geschäftsablagen und nicht lokal auf den persönlichen Geräten oder externen Datenträgern gespeichert werden.

2. Dokumente und Akten in Papierform oder auf elektronischen Datenträger

- Nehmen Sie insbesondere keine Dokumente mit personenbezogenen Daten mit, wenn diese zur Aufgabenerfüllung nicht unbedingt notwendig sind.
- Bei der Mitnahme von Dokumenten ist es wichtig, dass diese möglichst in einem geschlossenen und nicht einsehbaren Behältnis transportiert werden. Falls Dokumente auf elektronischen Datenträgern mitgenommen werden müssen, so ist darauf zu achten, dass diese geschützt sind (Passwortschutz zum Zugreifen auf Daten).
- Mitgeführte Papierdossiers und Ausdrucke müssen vor unberechtigtem Zugriff geschützt werden und sind in einem abschliessbaren Schrank, Pult, etc. zu verwahren.
- Ausdrucke und 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.

3. 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.
- Nutzen Sie unterschiedliche Passwörter für den geschäftlichen und den privaten Bereich.
- Private Geräte, die Sie mit anderen Familienangehörigen teilen, müssen über ein eigenes Benutzerkonto mit einem starken Passwort verfügen.
- Ihre Passwörter dürfen nicht an Dritte weitergegeben werden.

4. Kommunikationsmittel

- Private und geschäftliche E-Mails müssen auf dem privaten Gerät getrennt werden.
- Private E-Mail-Konten dürfen nicht für die geschäftliche Kommunikation genutzt werden.
- Sensiblen Daten dürfen nur geschützt, d.h. verschlüsselt versendet werden.
- Der Kanton stellt den Mitarbeitenden die Videokonferenzlösung MS-Teams (Stand, 1.4.2023) zur Verfügung. Sofern in Zusammenarbeit mit externen Personen weitere Kollaborationstools (z.B. Zoom, WebEx, etc.) zum Einsatz kommen, kann diesen Meetings als Gast beigetreten werden. Werden auf diesen Plattformen Daten ausgetauscht oder geteilt, obliegt es der Verantwortung der Sitzungsteilnehmenden, dabei alle Datenschutzvorgaben einzuhalten.
- Private USB-Sticks und andere Datenträger dürfen nicht an die betriebseigenen Geräte angeschlossen werden.

5. Videokonferenzen und Telefonieren

- Bleiben Sie während einer aktiven Video- oder Telefonkonferenz am Arbeitsplatz.
- Nutzen Sie dabei ein Headset oder einen Kopfhörer und telefonieren Sie nie über den Lautsprecher im Laptop oder im Smartphone.
- Schalten Sie das Mikrofon auf stumm und deaktivieren Sie die Kamera, wenn Sie diese nicht nutzen.

6. Updates, Phishing und andere Bedrohungen

- Die Betriebssysteme und Programme auf privaten (sofern für die Arbeit verwendet) und betriebseigenen Geräten müssen immer auf dem aktuellen Stand gehalten werden (regelmässige Überprüfung und Installation von Updates).
- Stellen Sie sicher, dass der Virenschutz installiert, aktiviert und aktualisiert ist.
- Aktivieren Sie die Client Firewall des Betriebssystems.
- Überprüfen Sie alle Sicherheitssysteme regelmässig und aktualisieren Sie diese vollständig, z.B. Datenschutz-Tools, Add-ons für Browser etc.
- Verdächtige E-Mails sollten nicht geöffnet, sondern gelöscht werden. Anhänge in Mails von unbekannten Absendern 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.

7. Datenverlust

- Sollten Arbeitsmittel wie Dokumente oder Geräte verloren gehen, ist dies den Vorgesetzten (Dokumente) und dem KICK (Geräte) zu melden.