Datenschutz für Nutzende des mobilen Arbeitens

Datenschutzvorkehrungen sind während des gelegentlichen ortsflexiblen Arbeitens zu Hause oder im Café ebenso einzuhalten wie bei der Arbeit im Büro. Die Gefahr von Datenschutzverstößen und der Preisgabe vertraulicher dienstlicher Informationen ist jedoch bei ortsflexiblem Arbeiten deutlich höher als im Betrieb oder am Tele-Heimarbeitsplatz.

Datenschutz-Tipps:

- Sie haben die Ihnen zur Verfügung gestellten Arbeitsmaterialien so einsetzen, dass Sicherheitsvorfälle vermieden werden können. Sicherheitsvorfälle betreffen den Verlust des Computers, dienstliche Unterlagen oder von Datenträgern, Systemstörungen oder die Kenntnisnahme von Informationen durch unberechtigte Dritte, unerlaubte Zugriffe oder den Befall mit Viren und anderer Schadsoftware. Der/die Arbeitnehmer*in ist verpflichtet, den Arbeitgeber unverzüglich über Sicherheitsvorfälle sowie Schäden am Gerät zu unterrichten.
- Sie sind bereits auf der Grundlage des geschlossenen Arbeitsvertrages zur Einhaltung der Datenschutzvorschriften, des Datengeheimnisses und zur Verschwiegenheit gegenüber Dritten über alle dienstlichen Daten verpflichtet. Diese Verpflichtung ist in besonderem Maße auch während der mobilen Arbeit zu berücksichtigen.
- Achten Sie darauf, daß Dritte keinen Zugriff auf Computer, dienstliche Unterlagen, Datenträger etc. haben oder Ihre Gespräche mithören können. Schützen Sie Ihren Computer vor der Einsichtnahme durch Dritte, indem Sie z.B. stets einen Blickschutzfilter verwenden.
- Der Internetanschluß muß über genügend Bandbreite verfügen, da eine schlechte Verbindung die Arbeit verlangsamen kann. Das ist inzwischen in vielen Cafés und Co-Working-Spaces kein Problem mehr, sollte aber getestet werden. Auch an Bahnhöfen oder Flughäfen ist die Infrastruktur generell vorhanden. Sollte sich der Arbeitsplatz abseits solcher Strukturen befinden, ist ein guter Datenplan unerläßlich. Auch hier fallen die Preise seit einiger Zeit. Aber Vorsicht:
- Aus Gründen des Datenschutzes und als Schutz gegen Hacker-Angriffe muß die Internetverbindung abgesichert werden.
- Wer viel telefonieren muß, sollte sich einen ruhigen Ort zum Arbeiten suchen. Nicht nur, damit er niemanden stört, sondern auch, damit vertrauliche Gespräche nicht mitgehört werden können.
- Es gilt die Clean Desk Regelung:
    - Bei kurzfristigem Verlassen vom Büro oder dem Homeoffice reichen das Aktivieren des Bildschirmschoners und Abschließen des Raumes.
    - Am Feierabend sind alle Unterlagen sicher zu verwahren und der Computer ist auszuschalten.
    - Im öffentlichen Raum sind selbst bei kurzfristigem Verlassen alle Unterlagen und Computer sicher zu verwahren.
- Beim Verlassen Ihres Platzes, auch nur für wenige Minuten haben Sie alles mitzunehmen. Dazu bieten sich Pilotenkoffer oder große Rucksäcke an. Oder durch Aufbewahrung der dienstlichen Unterlagen in einem verschließbaren Schrank oder Raum.
- Laptops und mobile Geräte dürfen nicht offen im Fahrzeug liegen, wenn Sie das Fahrzeug verlassen.
- Laptops und mobile Geräte dürfen über Nacht nicht in einem Fahrzeug gelassen werden.
- Entsorgen Sie dienstliche Unterlagen, Datenträger etc. ausschließlich im Betrieb.
- Achten Sie auf eine strikte Trennung von dienstlichen und privaten Arbeitsmitteln (keine private Nutzung der zur Verfügung gestellten IT-Ausstattung).

- Keine Verwendung privater oder nicht genehmigter Hard- und Software.
- Vorsicht bei öffentlich zugänglichen Internetanbindungen.

Organisatorische Maßnahmen

- ✓ Nachweisliche Schulung der Mitarbeiter die am mobilen Arbeiten teilnehmen in Datenschutzrecht und Datensicherheit
- ✓ Datenschutzverpflichtung der Mitarbeiter
- ✓ Keine Arbeit an vertraulichen Dokumenten in öffentlichen Räumen, wie z.B. im Cafés, Restaurants, öffentlichen Verkehrsmitteln, ...
- ✓ Mobile Geräte und Laptops dürfen niemals unbeaufsichtigt bleiben, sondern müssen stets mitgeführt werden.
- ✓ Wird nicht an den Geräten gearbeitet, muss der Bildschirmschoner aktiviert werden, um zu verhindern, dass unberechtigte Personen Einsicht auf die Dokumente, die auf dem Bildschirm angezeigt werden, nehmen können
- ✓ Im Hotel darf der Laptop nicht unbeaufsichtigt sein, bzw. muss im Safe aufbewahrt werden
- ✓ Der Rechner und die mobilen Geräte dürfen nicht offen in einem Fahrzeug liegen gelassen werden, wenn das Fahrzeug verlassen wird
- ✓ Es wurden Prozesse eingerichtet, um einen Verlust von Laptops und mobilen Geräten wie Handys und Tablets schnellst möglich zu melden.

Technische Maßnahmen

Laptop

- ✓ Passwortvergabe
  - Mindestlänge: 8 Zeichen
  - Mind. Ein Sonderzeichen
  - Anzahl der Fehleingaben 3
  - Mind. Ein Klein- und Großbuchstabe
  - Mind. Eine Ziffer
  - Ausschluss von Trivialpasswörtern
  - Wechselrhythmus 365 Tage
  - Passworthistorie
  - Regelmäßige Prüfung ob Zugangsdaten kompromittiert wurden (https://sec.hpi.uni-potsdam.de/ilc/search?lang=de)
  - Authentifikation mit Benutzername/Passwort
  - Zentrale Verwaltung von Benutzerrechten
- ✓ Eingeschränkte Benutzerrechte
- ✓ BIOS-Passwort ist aktiviert und nur der O-IT bekannt
- ✓ Festplattenverschlüsselung
- ✓ Einsatz von VPN-Technologie
- ✓ Zugang zum Internet nur über den Internetgateway der EKHN
- ✓ Gesicherte Nutzung von USB-Schnittstellen
- ✓ Einsatz von passwortgeschützten Bildschirmschonern
- ✓ Einsatz von Virenscannern
- ✓ Sicherheitsrelevante Softwareupdates und Virenpattern werden regelmäßig und automatisier eingespielt
- ✓ Soweit möglich ist auf den Netzwerklaufwerken zu arbeiten

- ✓ Daten sind soweit möglich auf den Netzwerklaufwerken zu sichern
- ✓ Daten die nicht mehr auf dem Laptop benötigt werden sind umgehend zu löschen
- ✓ Die Fernlöschung von mobilen Geräten ist aktiviert und kann im Falle des Verlusts des Geräts jederzeit durchgeführt werden