Datenschutzhinweise

FridoSpace
Co-Working in Waldshut

Arbeiten am Arbeitsplatz

Bei der Arbeit in geteilten Räumlichkeiten sollte man sich jederzeit bewusst sein, dass man zwar „zusammen arbeitet“, in dem Sinne, dass man zusammen in einem Raum, oder sogar an einem Tisch sitzt, aber eben nicht zusammenarbeitet. Daher ist jede/r Nutzer:in selbst für den eigenen Datenschutz verantwortlich. Folgende Hinweise sind zu beachten:

Sichtschutz: Wenn man in einem Raum oder gar an einem Tisch sitzt, bleibt es nicht aus, dass sich einem viele Möglichkeiten ergeben auch mal einen Blick auf den Monitor eines Nachbarn zu werfen. Ist dies der Fall, sind dort auch mit einer gewissen Wahrscheinlichkeit personenbezogene Daten oder andere vertrauliche Informationen zu sehen, die nicht für die Augen anderer gedacht sind.

Abhilfe kann hier eine geeignete Blickschutzfolie (IT-Grundschutzkompendium, CON.7.A4 Verwendung von Sichtschutz-Folien) schaffen. Durch eine solche reduziert sich der mögliche Einsichtswinkel von ca. 180 Grad auf bis zu ca. 60 Grad.

Unterlagen in Papierform: Auch diese sind in einer solchen Umgebung allzu leicht unerwünschten Blicken ausgesetzt. Das beste Mittel hiergegen stellt sicher eine soweit wie möglich papierlose Arbeitsweise dar. Lässt sich das Arbeiten mit Unterlagen in Papierform nicht vermeiden, sollte darauf geachtet werden wo die Unterlagen auf dem Tisch platziert werden und dass sie nach Möglichkeit immer abgedeckt oder sicher verstaut sind, wenn sie zeitweise nicht benötigt werden. Bestenfalls stehen abschließbare Rollcontainer und Aktenvernichtern oder Datenschutztonnen zur sicheren Vernichtung (IT-Grundschutzkompendium, SYS.4.1.A12 Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln) zur Verfügung.

Verlassen des Arbeitsplatzes

Verhalten bei Abwesenheit:. Sobald aber im Fridospace der „eigene“ Arbeitsplatz verlassen werden kann, gilt es folgendes zu berücksichtigen:

Es ist darauf zu achten, dass der Laptop bei nur kurzem Entfernen vom Arbeitsplatz durch eine Passwortsperre mit einem sicheren Passwort gesperrt wird (IT-Grundschutzkompendium ORP.4.A8 Regelung des Passwortgebrauchs), bzw. bei längerem Fernbleiben besser in einem Rollcontainer oder Schließfach zu verstauen ist, oder – soweit nicht vorhanden – mitgenommen wird. Außerdem ist natürlich darauf zu achten, dass alle Unterlagen bestenfalls in einem abschließbaren Rollcontainer sicher verstaut werden können. Datenträger sollten wenn überhaupt nur verschlüsselt zurück gelassen werden. Sicherer ist hier aber natürlich auch diese in einem Rollcontainer wegzuschließen.

Drucken und Telefonieren

Bei einer gemeinschaftlichen Nutzung von Arbeitsplätzen und Druckern drohen weitere Gefahren, dass vertrauliche Informationen in falsche Hände gelangen.

Die gemeinsame Nutzung von Netzwerkdruckern durch mehrere Personen, erschwert das Drucken von vertraulichen Dokumenten in hohem Maße. Beim Drucken ist in jedem Fall darauf zu achten, dass eine Pull-Printing-Lösung angeboten wird, so dass die Druckausgabe erst dann erfolgt, wenn man sich am Drucker authentifiziert hat (SYS.4.1.A15 Informationsschutz bei Druckern, Kopierern und Multifunktionsgeräten). Aber auch dann stellt sich die Frage nach den auf dem Gerät gespeicherten Druckdaten. Der Anbieter sollte hier die Datenspeicherung in geeigneter Weise verschlüsselten Form garantieren. Soweit es sich vermeiden lässt ist von einem Druck auf derlei gemeinschaftlich genutzten Druckern aber generell abzusehen.

Stellt sich noch die Frage nach unvermeidlichen Telefonanrufen während der Arbeit. Für das führen dienstlicher Telefonate bleibt einem letztlich keine andere Möglichkeit als sich aus der Hörweite anderer Co-Worker zu entfernen. Am besten gelingt einem das sicherlich in Telefonkabinen bzw. privaten Telefonräumen. Hier kommt es also zu einer Art Renaissance der guten alten Telefonzelle.

Nutzung des angebotenen WLANs

Eine Verschlüsselte Verbindung, etwa über VPN, ist unverzichtbar, wenn Sie sich in Co-Working Spaces und an Shared-Desk Arbeitsplätzen über das angebotene WLAN, mit Ihrem Unternehmensnetzwerk verbinden wollen (NET.2.2.A3 Absicherung der WLAN-Nutzung in unsicheren Umgebungen [IT-Betrieb]).

Für die allgemeine Nutzung des Internets empfiehlt es sich auf den Webseiten die Option „Immer HTTPS verwenden“ zu aktivieren. Zusätzlich empfiehlt es sich die Dateifreigabe über die Systemeinstellungen zu deaktivieren. Den besten Schutz bietet an dieser Stelle aber wohl das WLAN zu deaktivieren, wenn eine Internetverbindung nicht benötigt wird.