Handreichung Datenschutz und IT-Sicherheit zum mobilen Arbeiten an der Goethe-Universität

Beim mobilen Arbeiten ist ein verantwortungsvoller Umgang der Mitarbeitenden mit dienstlichen und personenbezogenen Daten besonders wichtig. Bei der Verarbeitung dieser Daten müssen die Anforderungen des Datenschutzes und der IT-Sicherheit beachtet und eingehalten werden. Details zu den notwendigen Maßnahmen finden Sie in der IT-Sicherheitsrichtlinie für die Johann Wolfgang Goethe-Universität Frankfurt am Main. Bei zentral verwalteten Rechnern muss durch die Systemverantwortlichen sichergestellt werden, dass bei der mobilen Arbeit dasselbe Sicherheitsniveau gewährleistet ist, wie bei der Arbeit vor Ort.
Um die Anforderungen des Datenschutzes und der IT-Sicherheit zu gewährleisten, enthält dieses Merkblatt ergänzende verpflichtende Regelungen, die beim mobilen Arbeiten eingehalten werden müssen. Das Merkblatt konkretisiert dabei die Anforderungen aus der „Dienstvereinbarung zur mobilen Arbeit“.

Arbeiten mit dienstlichen Daten und Geräten

Die dienstlichen Daten, mit denen Sie täglich arbeiten, sind wichtig und schützenswert. Nehmen Sie deshalb nur Unterlagen/Daten aus der Dienststelle mit an Ihren mobilen Arbeitsplatz, die Sie unbedingt benötigen.

Bitte stellen Sie sicher, dass:

- Sie ein Dienstgerät nutzen oder bei Nutzung eines privaten Endgerätes die Vorgaben der IT-Sicherheitsrichtlinie an Ihrem Endgerät umgesetzt haben.
- Sie Ihre dienstlichen Daten schützen, indem Sie andere Personen nicht auf Ihren Bildschirm schauen lassen, Sie Ihr dienstliches Gerät sperren, wenn Sie es (auch kurzzeitig) nicht benutzen und Sie Ihre dienstlichen Unterlagen sicher und verschlossen aufbewahren. Dies gilt sowohl zu Hause, als auch unterwegs.
- Sie Sichtschutzfolien verwenden (insbesondere bei Arbeiten im öffentlichen Raum), um unbefugte Einblicke auf Ihren Monitor zu verhindern. Die Anschaffung von Sichtschutzfolien hat in der Regel arbeitgeberseitig zu erfolgen, die Kosten hat die zuständige Einheit an der Goethe-Universität zu tragen.
- Sie Ihre Daten möglichst auf Ihrem Netzlaufwerk der Goethe-Universität und nicht lokal speichern. Lokale Speicherung dienstlicher personenbezogener Daten ist zu vermeiden bzw. auf das Minimum zu beschränken.
- Sie für den Austausch von Daten ausschließlich die Dienste der Universität nutzen.
- Sie keine dienstlichen Dokumente auf öffentlichen Druckern (z.B. Copyshop) ausdrucken.
- Sie vertrauliche Unterlagen nicht über den Hausmüll oder unterwegs entsorgen, sondern datenschutzgerecht in der Dienststelle.
- andere Personen nicht Ihre dienstlichen Geräte verwenden.
- Sie Ihre dienstlichen Unterlagen nicht offen herumliegen lassen.

- Sie keine dienstlichen Daten auf privaten, mobilen Speichermedien wie z.B. USB-Sticks, mobilen Festplatten oder Speicherkarten speichern.
- Sie keine USB-Sicks unbekannter Herkunft nutzen.
- Sie, im Falle der Notwendigkeit eines Cloudspeichers, die Hessenbox bzw. den von der Goethe-Universität betriebenen Clouddienst nutzen.
- Sie private und dienstliche Unterlagen nicht vermischen, sondern getrennt aufbewahren.
- Sie Ihren mobilen Arbeitsplatz sichern, sobald Sie ihn verlassen (etwa in einem Hotelzimmer durch Schließen von Fenster und Türen).
- Sie auf mobilen Endgeräten oder tragbaren Datenträger Daten, insbesondere sensible personenbezogene Daten, nur verschlüsselt speichern, so dass bei Verlust des Gerätes die Daten weiterhin geschützt sind.
- sofern die Installation zusätzlicher Software erforderlich ist, diese den Vorgaben der IT-Sicherheitsrichtlinie entspricht.
- der zu nutzende Benutzer Account im Allgemeinen keine Administrationsrechte besitzt.
- eine Nutzung von Sprachassistenten bei der mobilen Arbeit nicht stattfindet.
- alle verwendeten Programme, Tools und Systeme immer auf dem neuesten Stand gehalten sind.
- Sie ihr Gerät in öffentlich zugänglichen Bereichen nie unbeaufsichtigt lassen.
- Sie unterwegs unbedingt keine öffentlich zugänglichen USB-Aufladem̈oglichkeiten (Ladeterminals) nutzen.
- Sie einen Verlust oder Diebstahl unverzüglich Ihrer*m Vorgesetzten, der Abteilung Datenschutz und dem IT-Support melden.

Dienstliche Daten und Geräte transportieren

Schriftliche Notizen, Papierunterlagen und Ihre Endgeräte müssen verschlossen transportiert und weggeschlossen werden (zum Beispiel in einem verschließbaren Schrank oder Tresor), wenn Sie sie nicht verwenden. Ausdrucke mit personenbezogenen Daten sind nach Möglichkeit zu vermeiden. Papierunterlagen dürfen beim Transport nicht erhöhten Risikosituationen ausgesetzt werden (z. B. Rücksitz beim Einkaufen, Rucksack im Restaurant).

Mit dem Uni-Netz und dem Internet verbinden

Nutzen Sie bitte immer eine VPN-Verbindung. Nutzen Sie bei zentral verwalteten Rechnern den in Ihrem Bereich vorgegebenen VPN-Client und lassen Sie sich diesen gegebenenfalls von den zuständigen Administratoren einrichten. Eine Anleitung zur Einrichtung finden Sie auf den Webseiten des Hochschulrechenzentrums.

Bitte beachten Sie, wenn Sie mobil arbeiten, dass:

- Sie, wenn möglich, eine kabelgebundene LAN-Verbindung ins Internet nutzen.
- für die Verschlüsselung des WLANs an Ihrem Router mindestens WPA2 eingestellt ist.
- die Arbeit im öffentlichen Raum nur insoweit zulässig ist, wie die Arbeit an einem Rechner mit Sichtschutzfilter erfolgen kann. In öffentlichen Netzen muss notwendig das VPN verwendet werden und es darf nicht auf das vorhandene Netz zurückgegriffen werden.

Telefonieren und Besprechen

Auch bei Telefonaten und Videokonferenzen müssen Sie darauf achten, dass Unbefugte sensible Inhalte nicht mithören können. Insbesondere vertrauliche Inhalte sollten nicht in der Anwesenheit anderer Personen besprochen werden.
Bitte

- beachten Sie den oben genannten Hinweis, zur Nutzung von Sprachassistenten. Insbesondere vor Telefonaten und Videokonferenzen ist zu überprüfen, dass entsprechende Sprachassistenten deaktiviert bzw. nicht in der Nähe des Arbeitsplatzes sind.
- nutzen Sie für Videokonferenzen die von der Goethe-Universität bereitgestellten Dienste. Bei der Nutzung von Videokonferenzsystemen bei Dienstbesprechungen ist darauf zu achten, dass nur die dafür freigegebenen Videosysteme genutzt werden. Die jeweils gültige Regelung entnehmen Sie der Seite des SMT. Eine Ausnahme ist gegeben, wenn Externe die Nutzung anderer Videokonferenzsysteme zum Meeting vorgeben.
- beachten Sie die Regelungen zur Nutzung von Videokonferenzen sowie die allgemeinen Hinweise zum Datenschutz.
- achten Sie darauf, ohne ausdrückliche Erlaubnis keine personenbezogenen Daten von anderen Personen preiszugeben, wenn Sie von Externen zu einer Videokonferenz eingeladen werden.
- stellen Sie sicher, dass die mobile Arbeit, insbesondere virtuelle Videokonferenzen oder dienstliche Telefonate, nicht im Beisein Dritter erfolgt. Das gilt auch für Familienangehörige, ausgenommen Kleinkinder.
- unterlassen Sie die Teilnahme an Videokonferenzen in öffentlich zugängigen Stätten wie beispielsweise in Cafés und Zügen und führen Sie vertrauliche Telefonate nur in geschützten Umgebungen.
- verwenden Sie bei der Teilnahme an Videokonferenzen während des mobilen Arbeitens ein Headset.
- nutzen Sie für Email-Kommunikation ausschließlich die E-Mail-Systeme der Universität. Das Versenden dienstlicher E-Mails über private E-Mail-Accounts ist untersagt. Sie dürfen gemäß der IT-Sicherheitsrichtline dienstliche E-Mails nicht automatisiert an andere Provider weiterleiten.

Bitte wenden Sie sich bei Fragen an den für Sie zuständigen lokalen IT-Support oder an Ihre*n Vorgesetzte*n.