Datenschutz und Datensicherheit

Zielsetzung

Ziel dieser Dienstanweisung ist die Umsetzung datenschutzrechtlicher Vorgaben bei der Verarbeitung von personenbezogenen Daten auf mobilen Endgeräten sowie die Erfüllung von Sicherheitsanforderungen der Hochschule bei der Verarbeitung sonstiger Daten/Informationen.

Anwendungsbereich

Diese Regelung gilt für alle Beschäftigten der Berliner Hochschule für Technik (BHT) im Rahmen der Nutzung von mobilen Endgeräten (Handys, Smartphones, Laptops), insbesondere außerhalb der Räumlichkeiten der BHT.

Abweichungen zu dieser Arbeitsanweisung sind nur in Abstimmung mit der Hochschulleitung möglich.

Allgemeine Regelungen:

Es sind generell mindestens die gleichen Sicherheitsmaßnahmen wie bei den Geräten, die stationär verwendet werden, zu ergreifen. Hierzu zählen u. a. (nicht abschließende Aufzählung):

(1) Es werden nur Akten zum mobilen Arbeiten mitgenommen, die zwingend erforderlich sind. Es ist ein Verzeichnis der mitgeführten und zurückgebrachten Akten zu führen. Akten mit überwiegend personenbezogenen und äußerst sensiblen Daten dürfen nicht am Arbeitsplatz im mobilen Arbeiten bearbeitet werden. Dazu zählen insbesondere Personalakten, Bewerbungsunterlagen, Disziplinarangelegenheiten, Unterlagen zum Betrieblichen Eingliederungsmanagement und Studierendenakten.

(2) Vertrauliche Daten und Informationen sind - auch beim Transport zwischen dienstlichem und Arbeitsplatz im mobilen Arbeiten - so zu schützen, dass Dritte keine Einsicht nehmen können und ein unbefugter Zugriff auf die Daten wirksam verhindert wird. Der Transport der Akten erfolgt mit besonderer Sorgfalt, wenn möglich in verschlossenen Behältnissen.

(3) Familienangehörige und sonstige Dritte (Ausnahme: Arbeitsassistenzen) dürfen keinen Einblick in die Akten oder Dateien erhalten. Akten und Unterlagen sind verschlossen in einem Schrank oder Schrankteil aufzubewahren. Sofern Sie von zu Hause aus arbeiten und sichergestellt ist, dass diese Umgebung gegen Betreten von außen gesichert ist, genügt bei kurzfristiger Nicht-Nutzung zu Hause auch das Sperren des Bildschirmes, wenn Sie den Arbeitsraum, aber nicht die Wohnung verlassen. Sofern Sie allerdings nicht ausschließlich computerbasiert-, sondern zumindest auch papierbasiert zu Hause arbeiten und sich Dritte im Haus/der Wohnung befinden, sind die Akten auch bei kurzer Abwesenheit in einen Schrank einzuschließen oder der Raum abzuschließen. Beim Verlassen des Arbeitsplatzes an anderem Ort ist darauf zu achten, dass Türen und - vor allem im Erdgeschoss - Fenster verschlossen bzw. geschlossen sind.

(4) Mobile Rechner sind klein und handlich und somit leicht Gegenstand von Diebstahl. Auch stellen sie einen Wert dar, der potenzielle Diebe anlocken könnte. Daher sollten mobile Rechner niemals ungeschützt/unbeaufsichtigt herumliegen. Dies gilt auch für Hotelzimmer und Autos (das Verstecken und/oder Verschließen des Gerätes behindert zumindest Gelegenheitsdiebe).

(5) WLAN, Bluetooth und sonstige Kommunikationsfunktionen sind bei Nichtbenutzung auszuschalten.

(6) Bei Erforderlichkeit ist der Laptop der IT-Abteilung zu übergeben, so dass diese Wartungs- und Aktualisierungstätigkeiten durchführen können. Auch ein Remote-Zugang durch die IT-Abteilung kann ermöglicht werden.

(7) Die Arbeit erfolgt grundsätzlich auf einem dienstlichen Endgerät. Die Endgeräte sind mit Passwortschutz zu versehen. Der Zugriff auf die auch am dienstlichen Arbeitsplatz in der Dienststelle zugänglichen Daten erfolgt über einen gesicherten VPN-Zugang bzw. mindestens über den Remote-Desktop-Server. Sofern WLAN genutzt wird, darf der Aufbau dieser Verbindungen nur mit vertrauenswürdigem WLAN geschehen und hat manuell durch den Nutzer zu erfolgen (kein automatisches Wiederverbinden sobald das Gerät wieder in den Bereich des Hotspots zurückkehrt).

Die Dienststelle sorgt dafür, dass den Beschäftigten geeignete Datenträger im Netz der Berliner Hochschule für Technik (BHT) zur Verfügung stehen, auf denen zu bearbeitende Dokumente abgerufen und gespeichert werden.

(8) Sofern Daten lokal abgelegt werden müssen (beispielsweise durch das Arbeiten auf dem Laptop, der nicht am Netzwerk angeschlossen ist), sind die Daten eigenverantwortlich schnellstmöglich auf dem Server zu sichern.

(9) Beim Arbeiten an öffentlichen Plätzen (Flughafen, Bahnhof/Zug, Café etc.) ist darauf zu achten, dass keine Daten von Unbefugten eingesehen werden können. Dies kann durch das entsprechende Hinsetzen in wenig einsehbaren Bereichen und/oder durch die Nutzung von Sichtschutzfolien erreicht werden. Laptops sind ausschließlich als Handgepäck zu führen.

(10) Für dienstliche Video- oder Telefonkonferenzen sind die vom HRZ angebotenen Services zu nutzen.

(11) Nicht mehr benötigte Datenträger und Unterlagen sind zu löschen und/oder zu vernichten. Die Entsorgung von Unterlagen erfolgt ausschließlich in der Dienststelle.

(12) Folgende Ereignisse machen eine unverzügliche Meldung an den IT-Bereich erforderlich:

» verloren gegangene Geräte

» sicherheitsrelevante Ereignisse, wie z. B. unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, nicht autorisierte Zugriffe, Verdacht auf Missbrauch der eigenen Benutzerkennung usw.

» Verdacht auf Viren, Trojaner etc.

(13) Für den Fall eines Datenverlusts (z. B. Verlust von Papierunterlagen oder Datenträgern) oder eines Datenschutzverstoßes (z. B. Zugang von Unbefugten an den Computer) besteht eine Meldepflicht an die Aufsichtsbehörde. Der behördliche Datenschutzbeauftragte (datenschutz@bht-berlin.de) ist Ihr hochschulinterner Ansprechpartner im Rahmen des Meldeverfahrens.