Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Merkblatt des behördlichen Datenschutzbeauftragten

Datenschutz und IT-Sicherheit im Home-Office

Die wichtigste Regel lautet: Entnehmen Sie nur diejenigen dienstlichen Daten aus der Beschäftigungsstelle, die unbedingt für Ihre Arbeit erforderlich sind.

Verwenden Sie für alle IT-Dienste und Programm immer die Terminal-Server und das VPN.

1. Umgang mit Daten, insb. personenbezogenen Daten

1.1. Auch wenn Mitarbeitende an ihrem Heimarbeitsplatz tätig werden, sind Mitarbeiter/innen der HWR verpflichtet, alle Daten, Informationen und Unterlagen, auf die sie Zugriff haben, ausschließlich im Hoheitsbereich der HWR Berlin zu belassen. Betriebliche Daten, Informationen oder Unterlagen – insbesondere personenbezogene und sonstige vertrauliche Daten dürfen deshalb nicht an Dritte weitergegeben werden.

1.2. Daten, Informationen und Unterlagen der HWR dürfen nicht auf eigenen Speichermedien abgespeichert, unbefugt kopiert oder zu anderen als zu betrieblichen Zwecken genutzt werden.

1.3. Insbesondere bitten wir Sie sicherzustellen, dass

- Passwörter oder sonstige Zugangsmöglichkeiten zur dienstlichen EDV (z. B. Chipkarten) Dritten nicht mitgeteilt oder zugänglich gemacht werden, z. B. durch Notieren von Passwörtern oder Lagerung der Chipkarte (z.B. für Überweisungen) am Lesegerät.
- Dritten (z. B. Familienmitgliedern, sonstigen Mitbewohnern, Besuchern) kein Zugriff auf die betriebliche EDV und/oder betriebliche Unterlagen gewährt wird.
- betriebliche Daten nur auf Speichermedien der HWR Berlin gespeichert werden.
- Sicherheitsmaßnahmen nicht deaktiviert oder umgangen oder sonstige technische Veränderungen an den durch die HWR zur Verfügung gestellten Geräten vorgenommen werden. Software darf nur durch die IT-Abteilung installiert werden.
- eventuelle Ausdrucke mit vertraulichen Informationen (z. B. personenbezogenen Daten) sicher vernichtet werden, wenn sie nicht mehr benötigt werden (DIN 66399).

1.4. Alle Störungen oder Auffälligkeiten bei der EDV-Nutzung sind unverzüglich der IT-Abteilung unter der Mailadresse it-hotline@hwr-berlin.de zu melden.

1.5. Die private Nutzung, der für den Heimarbeitsplatz bereitgestellten betrieblichen Geräte bzw. Zugangsmöglichkeiten (insbesondere Computer), ist aus Gründen der Informationssicherheit (Viren, Schadsoftware wie Emotet) nicht zulässig.

1.6. Die Weiterleitung dienstlicher Emails / Dokumente an private Mailadressen ist zu unterlassen.

1.7. Sollte für das Abrufen von Emails kein VPN genutzt werden, so ist ein gesichertes (verschlüsseltes) WLAN zu nutzen.

1.8. Die HWR Berlin ist berechtigt, die Herausgabe sämtlicher betrieblicher Daten, Unterlagen und Akten einschließlich sämtlicher Kopien zu verlangen.

1.9. Die Dienstvereinbarung für Telearbeit ist weiterhin gültig. Wir bitten Sie, diese zu sichten. https://intranet.hwr-berlin.de/fileadmin/intranet/Dokumente/Personalwesen/Tele-Heimarbeit-Dienstvereinbarung.pdf

2. Sicherheitsmaßnahmen im Home-Office

2.1. Wenn verfügbar, soll als Heimarbeitsplatz in der Wohnung der Mitarbeitenden ein Raum genutzt werden, der abschließbar ist. Er soll bei Nichtnutzung durch die Mitarbeitenden abgeschlossen werden. Sind Gäste (auch Handwerker) in der Wohnung, sollte der Raum immer verschlossen sein. Der Mitarbeiter/die Mitarbeiterin ist verpflichtet, die Vertraulichkeit von Informationen und personenbezogenen Daten der HWR sicherzustellen.

2.2. Verlassen Mitarbeitende ihren Heimarbeitsplatz (und sei es nur kurz), muss sichergestellt sein, dass kein Dritter auf betriebliche Daten oder Akten zugreifen kann. Dies bedeutet insbesondere, dass

- der verwendete Computer gesperrt werden muss, so dass bei Rückkehr zumindest die Eingabe des Passwortes erforderlich ist – Sperren können Sie mit den Befehlen „Windows-Taste + L“.
- Fenster verschlossen sein müssen, außer bei kurzzeitiger Abwesenheit, während der ein Eindringen realistischer Weise ausgeschlossen werden kann.
- Papier-Akten eingeschlossen oder so weggeräumt werden, dass Dritte darauf keinen Zugriff haben.
- bei Verlassen der Wohnung ein gegebenenfalls genutztes Zugangsmedium (z. B. Chipkarte für Finanztransaktionen) vom Computer entfernt werden muss.

2.3. Admin-Zugänge sollten so wenig wie möglich von zu Hause genutzt werden.

2.4. Der Transport von Akten oder nicht elektronischen Dateien muss in verschlossenen Behältnissen erfolgen. Der Verlust ist unverzüglich beim Datenschutzbeauftragten anzuzeigen.

3. Zusätzliche Sicherheitsmaßnahmen im Mobile Office

Bei der Nutzung eines mobilen Arbeitsplatzes (Mobile Office) außerhalb der Wohnung der Mitarbeitenden gilt ergänzend:

3.1. Mitarbeitende dürfen den mobilen Arbeitsplatz außerhalb eines verschlossenen Raums nicht – auch nicht kurzzeitig – unbeaufsichtigt lassen, wenn nicht eine Aufsicht durch einen anderen Mitarbeitenden der HWR sichergestellt ist.

3.2. Bevor Mitarbeitende ihre direkte Aufmerksamkeit vom mobilen Arbeitsplatz entfernen, ist der Computer zu sperren und alle Zugangsmedien (z. B. Chipkarte) zu entfernen und sicher zu verwahren.

3.3. Der Transport von Akten oder nicht elektronischen Dateien muss in verschlossenen Behältnissen erfolgen.

4. Beendigung der Heimarbeitsplatz-Nutzung

4.1. Endet die Berechtigung des Mitarbeitenden zur Nutzung des Heimarbeitsplatzes nach dem SARS-CoV2-Notbetrieb, hat der Mitarbeitende unaufgefordert sämtliche betriebliche Zugangsmedien (z. B. Chipkarten), Datenträger und Akten (einschließlich Kopien) in die Hochschule zurückzubringen.

4.2. Mitarbeitende haben zudem die Abholung sämtlicher von der HWR Berlin bereitgestellter Arbeitsmittel durch von der HWR beauftragte Personen nach angemessener Ankündigungsfrist zu gewährleisten.

5. Hinweis auf rechtliche Folgen bei Verstößen

5.1. Die IT-Abteilung weist darauf hin, dass Verstöße gegen datenschutzrechtliche Normen (DSGVO, Berliner Datenschutzgesetz) arbeitsrechtliche Folgen (Ermahnung, Abmahnung, fristgerechte oder fristlose Kündigung) haben können und mit Geldbuße bedroht und/oder strafbar sein können (z. B. im Fall des unbefugten Kopierens von Daten nach Art. 83 DS-GVO, § 42 BDSG).

5.2. Die IT-Abteilung bittet Sie deshalb nicht fahrlässig mit den Geräten und den dort verarbeiteten Daten umzugehen und die Sicherheitsmaßnahmen zu treffen, die Sie an ihrem Arbeitsplatz an der HWR auch vornehmen würden.

6. Schulungsangebot IT-Sicherheit und Datenschutz

Das Schulungsangebot der HWR Berlin besteht aus einem Datenschutz- und IT-Sicherheitskurs.

Die Kurse sind unter moodle.hwr-berlin.de abrufbar. Sollten Sie noch nicht für den Kurs freigeschaltet sein, schreiben Sie bitte an das E-Learning-Team der HWR Berlin elearning@hwr-berlin.de.