Merkblatt Datenschutz und IT-Sicherheit im Home Office/Mobile Office (Telearbeit) während des SARS-CoV2-Notbetriebs

Die wichtigste Regel lautet, nur die dienstlichen analogen und digitalen Daten, die unbedingt erforderlich sind, aus der Beschäftigungsstelle zu entnehmen.

Für alle nicht von außerhalb der HWR Berlin erreichbaren Dienste verwenden Sie bitte das VPN, sofern Sie für den aktuellen Arbeitsvorgang darauf angewiesen sind, da dadurch der unberechtigte Zugang für Dritte erschwert wird. Um die begrenzten Kapazitäten zu schonen, beenden Sie die Verbindung nach Abschluss der Arbeiten bitte so schnell wie möglich wieder.

1. Umgang mit Daten, insb. personenbezogenen Daten

1.1. Auch wenn Mitarbeiter 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 sonst vertrauliche Daten – dürfen deshalb nicht an Dritte weitergegeben werden; sie müssen verhindern, dass solche Daten, Dritten zur Kenntnis gelangen (etwa durch Einsichtnahme am Bildschirm oder auf Ausdrucken). Daten, Informationen und Unterlagen der HWR sollen auch nicht auf eigenen Speichermedien abgespeichert, unbefugt kopiert oder zu anderen als betrieblichen Zwecken werden.

1.2. 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 HWR Berlin gespeichert werden. Sollten Sie gezwungen sein, dienstliche Daten kurzfristig auf privaten Geräten abzuspeichern, etwa weil die VPN-Verbindung zusammengebrochen ist, sind Sie verpflichtet, so rasch wie möglich eine ordnungsgemäße Speicherung auf HWR-Servern sicherzustellen und die Daten von Ihren privaten Geräten unbedingt und final wieder zu löschen; darüber hinaus ist es verboten, dienstliche Daten mit privaten Geräten zu verarbeiten (außer dienstlichen E-Mails und dem Netzlaufwerk per VPN)
- 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).
- Verwenden Sie möglichst die gleichen Produkte wie am dienstlichen Arbeitsplatz.
- Wählen Sie zur Nutzung von Tablets und Smartphones für den dienstlichen Gebrauch datenschutzgerechte Apps.

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

1.4. 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.

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

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

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

1.8. 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 des Mitarbeitenden ein Raum genutzt werden, der abschließbar ist. Er soll bei Nichtnutzung durch den Mitarbeiter abgeschlossen werden. Hat der Mitarbeiter Gäste (auch Handwerker) in seiner Wohnung, sollte der Raum verschlossen sein. Halten sich Dritte am Heimarbeitsplatz auf (z. B. Handwerker oder Kinder die hier arbeiten müssen), sollte der Mitarbeitende sie im Auge behalten.

Soweit dies während des SARS-CoV2-Notbetriebs nicht möglich ist, ist der Mitarbeiter/die Mitarbeiterin verpflichtet, die Vertraulichkeit von HWR-Daten, -Informationen und –Unterlagen anderweitig sicherzustellen.

2.2. Verlässt der Mitarbeiter seinen 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 (z. B. 10. Stock und keine Möglichkeit, aus der Nachbarwohnung herüberzuklettern);
- bei Nutzung von Papier-Akten eingeschlossen oder so weggeräumt werden, dass Dritte darauf nicht ohne Weiteres Zugriff haben; dies gilt nur dann nicht, wenn der Mitarbeiter alleine zu Hause ist und seinen Heimarbeitsplatz nur kurzzeitig verlässt;
- bei Verlassen der Wohnung ein gegebenenfalls genutztes Zugangsmedium (z. B. Chipkarte für Finanztransaktionen) vom Computer entfernt werden muss und bei Nutzung von Papier-Akten diese eingeschlossen oder sicher weggeräumt werden müssen.

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

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

3. Zusätzliche Sicherheitsmaßnahmen im Mobile Office

Bei der Nutzung eines mobilen Arbeitsplatzes (Mobile Office) außerhalb der Wohnung des Mitarbeiters gilt ergänzend zu den Regelungen in 2:

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

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

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

4. Beendigung der Heimarbeitsplatz-Nutzung

4.1. Endet die Berechtigung des Mitarbeiters zur Nutzung des Heimarbeitsplatzes nach dem SARS-CoV2-Notbetrieb oder das Arbeitsverhältnis endet oder der Mitarbeiter wird unwiderruflich von der Pflicht zur Arbeitsleistung freigestellt, hat der Mitarbeiter unaufgefordert sämtliche betrieblichen Zugangsmedien (z. B. Chipkarten), Datenträger und Akten (einschließlich Kopien) in den Betrieb zurückzubringen und dem Vorgesetzten zu übergeben.

4.2. Der Mitarbeiter hat 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 unternehmen würden.

5.3. Uns ist klar, dass es sich aktuell um eine Sondersituation handelt, in der wir alle uns im Rahmen des Möglichen um flexible Lösungen für so viele Fragen bemühen. Bitte helfen Sie uns dabei, auch in dieser Phase die datenschutzrechtlichen Anforderungen zu erfüllen.

6. Schulungsangebot IT-Sicherheit und Datenschutz

Sollten Sie sich nicht sicher sein, welche weiteren Datenschutz und IT-Sicherheitsmaßnahmen Sie unternehmen müssen, können Sie die angebotenen Online-Schulungen der HWR in Moodle durchlaufen. Wir raten Ihnen dazu.

Die Kurse sind unter moodle.hwr-berlin.de abrufbar. Sollten Sie noch nicht für den Kurs freigeschaltet sein, können Sie dies mit einer Mail an das E-Learning-Team der HWR elearning@hwr-berlin.de tun.