Merkblatt

**zum Datenschutz und zur Informationssicherheit
bei Mobiler Arbeit für Beschäftigte der Technischen Universität Chemnitz
vom 11. Mai 2022[1]**

Das Merkblatt zum Datenschutz und zur Informationssicherheit bei Mobiler Arbeit für Beschäftigte der Technischen Universität Chemnitz vom 11. Mai 2022 dient als nachweisbare Erläuterung der datenschutzrechtlichen Bestimmungen und Risiken im Sinne von § 8 Abs. 3 S. 1 Dienstvereinbarung zur Mobilen Arbeit.

Über darüberhinausgehende Fortbildungsmaßnahmen zum Umgang mit datenschutzrechtlichen Themen, welche Ihren Arbeitsbereich betreffen könnten, informiert Sie das Dezernat Personal, Sachgebiet 2.2.1 Personalentwicklung (Ausbildung, Fort- und Weiterbildung).

Die Technische Universität Chemnitz ist als datenschutzrechtlich Verantwortliche verpflichtet, geeignete technische und personelle/organisatorische Schutzmaßnahmen und Kontrollmöglichkeiten zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und eine unbefugte Nutzung der IT-Systeme bzw. einen unberechtigten Zugriff auf Informationen auszuschließen. Vorbenannte Schutzmaßnahmen schließen u. a. die in § 7 der Datenschutzleitlinie der Technischen Universität Chemnitz vom 19. Juni 2019 genannten Schutzziele ein.

Um die vermeidbaren Risiken – z. B. unbefugter Zugang oder Zugriff auf Datenverarbeitungsanlagen, Datenmissbrauch/-verlust, Integritätsverlust – möglichst auszuschließen, sollten entsprechend des Schutzbedarfes der verarbeiteten Daten („normal“, „hoch“, „sehr hoch“; vgl. Anlage 4 der Dienstvereinbarung zur Mobilen Arbeit) im Rahmen der Mobilen Arbeit hinreichende Schutzmaßnahmen getroffen werden. Darüberhinausgehend wird auf die Regelungen und Anweisungen zur Mobilen Arbeit in der o. g. Dienstvereinbarung Bezug genommen.

Eine Verarbeitung von Daten mit einem sehr hohen Schutzbedarf (z. B. Beschäftigtendaten, Sozialdaten, Prüfungsdaten, Daten unter besonderer Geheimhaltungs-/Vertraulichkeitsverpflichtung (u. a. § 203 StGB), Daten im Sinne von Art. 9 Abs. 1 bzw. Art. 10 DSGVO) während der Mobilen Arbeit ist nur am häuslichen Arbeitsplatz und unter Einhaltung besonderer Schutzmaßnahmen (risikobasierter Ansatz) zulässig.

Zur eigenständigen Überprüfung der technischen und organisatorischen Schutzmaßnahmen am häuslichen Arbeitsplatz stellt der Datenschutzbeauftragte der TU Chemnitz auf seiner Webseite (https://www.tu-chemnitz.de/rektorat/dsb/vorlagen.html#dokumentation) eine Checkliste zur Verfügung und steht darüber hinausgehend jederzeit, insbesondere auch in Zweifelsfällen und bei Rückfragen, für eine Abstimmung bzw. Beratung zur Verfügung.

[1] Aus Gründen der besseren Lesbarkeit wird im Folgenden in der Regel das generische Maskulinum verwendet. Sämtliche Personenbezeichnungen gelten aber selbstverständlich für alle Geschlechter.

1. Infrastrukturelle Risiken

Gerade die Ortsunabhängigkeit der Mobilen Arbeit ist es, die besonders erhöhte Risiken für den Datenschutz und die Informationssicherheit in sich birgt, da der mobile Arbeitsplatz nicht in dem Umfang gegen Bedrohungen der Datensicherheit geschützt ist wie die Arbeitsplätze an der Technischen Universität Chemnitz selbst. Um dieses Risiko zu minimieren sollte soweit möglich ein ortsgebundener Arbeitsplatz und/oder zusätzliche Sicherungsmaßnahmen in Abhängigkeit des Schutzbedarfes der Daten gewählt werden, z. B.:

- sorgfältige Auswahl geeigneter mobiler Arbeitsplätze: z. B. gesondertes (Arbeits-)Zimmer, zumindest abschließbar/abtrennbar von sonstigen Räumlichkeiten, keine Mobile Arbeit an unsicheren Orten, z. B. wenn unbefugter Zugriff nicht ausschließbar, keine hinreichenden Verschlussmöglichkeiten bzw. Strom-/Netzwerkversorgung, Gefahr des Mithörens beim Freisprechen in Kraftfahrzeugen,
- physische Zugangs-/Zugriffskontrolle auch bei nur vorübergehender Nichtbenutzung, z. B. besondere Schließzylinder, Zusatzschlösser, Riegel, gegebenenfalls besonderen Sicherungsschutz für einstiegsgefährdete Türen oder Fenster u. a. im Keller-/Erdgeschoss, kein unbeaufsichtigtes Aufhalten von unberechtigten Personen (gilt auch für Familienangehörige), gegebenenfalls anderweitige, wenn physisch nicht möglich: z. B. Beaufsichtigung durch interne Mitarbeitende in Besprechungs-, Veranstaltungs-, Schulungs-, Konferenzräumen,
- aufgeräumter Arbeitsplatz: z. B. Verschluss/Sicherung im Schreibtisch, Schrank auch bei nur kurzzeitigem Verlassen,
- Berücksichtigung von Ergonomie, Sicherheit und Gesundheitsschutz: z. B. ausreichend Platz für Möbel und Bildschirmarbeitsplatz; Anordnung der Arbeitsmittel mit möglichst geringer Belastung für jeweilige Arbeitsaufgabe; Stuhl (Rückenlehne, Sitzhöhe, Sitzfläche), Tisch, Bildschirm, Tastatur individuell einstellbar; regelbare Raumtemperatur und ausreichende Lüftungsmöglichkeiten; Abschirmung gegenüber Lärmquellen (Möglichkeit zum ungestörten Arbeiten); Tageslicht sowie ausreichend künstliche Beleuchtung; Sichtschutz(-folien) (z. B. Beobachtung durch Fenster, Blick über die Schultern, Aufzeichnung durch Videokameras); Vermeidung von störenden Blendungen, Reflexionen, Spiegelungen (u.a. Bildschirm im rechten Winkel zum Fenster) und Anschlüsse für Telefon/Strom,
- physische Sicherung der IT-Systeme auch bei Nichtbenutzung: z. B. stabile Unterlagen, nicht zu feuchtes, zu kaltes oder zu warmes Betriebsklima, frühzeitiges Informieren über Verhalten im Notfall (z. B. Brandfall), Diebstahlschutz (z. B. Kabelschloss), kein unbeaufsichtigtes Zurücklassen (z. B. sichtbar in Fahrzeugen),
- besondere Vorsicht vor Social Engineering Angriffen, z. B. kein Austausch vertraulicher Informationen, strenge Identitätsprüfung.

2. Besondere Risiken während des Verarbeitungsvorganges (z. B. Transport, Aufbewahrung etc.)

Auch während des Verarbeitungsvorganges entstehen aufgrund der Ortsunabhängigkeit der Mobilen Arbeit besondere Risiken in bereits oben genannter Art und Weise, die mittels geeigneter und dem Schutzbedarf angemessener Maßnahmen minimiert werden sollten, z. B.:

- Aufbewahrung in verschlossenen Behältnissen bzw. abschließbaren Schränken, u. a. Dokumente/Arbeitsunterlagen, digitale Datenträger, mobilen Endgeräten einschließlich Laptops und Geräte zur Herstellung einer Einwahlverbindung (z. B. Token-Generator),
- ausreichend dimensionierte, abschließbare Staumöglichkeiten, z. B. Rollcontainer, Schränke, Tresore, Schreibtische,
- Schlösser sollten Angriffen mit von jedermann herzustellenden oder einfach zu erwerbenden Schließmitteln standhalten (z. B. Büroklammern, Dietrichen etc.), inkl. keiner leichten Umgehungsmöglichkeit (z. B. Entfernen von Rückwänden),
- zentrale Datenverarbeitung auf Servern der Technischen Universität Chemnitz: insbesondere unverzügliche zentrale (keine externe, mobile) Sicherung, keine Ausdrucke, frühestmögliche Löschung, insbesondere für temporäre Dateien, Datenminimierung,
- persönlicher Datentransport auf kürzestem Weg in verschlossenen Behältnissen bzw. hinreichende Verschlüsselung,
- gegebenenfalls Sicherungskopie vor Transport (sofern zulässig),
- keine E-Mail-Weiterleitung auf private E-Mail-Postfächer,
- vorherige Prüfung auf Schadsoftware bei Nutzung externer Datenträger.

3. Risiken bei der Entsorgung/Vernichtung

Die besonderen Risiken insbesondere des unbefugten Zuganges/Zugriffes auf Daten im Zusammenhang mit der Entsorgung/Vernichtung während der Mobilen Arbeit sollten durch hinreichende und angemessene Schutzmaßnahmen minimiert werden, z. B.:

- grundsätzliche Unzulässigkeit der Entsorgung/Vernichtung von Daten am mobilen Arbeitsplatz, es sei denn, besondere Entsorgungseinrichtungen wurden durch die Technische Universität Chemnitz zur Verfügung gestellt,
- Entsorgung ausschließlich mittels zur Verfügung gestellter Arbeitsmittel am dienstlichen Arbeitsplatz,
- Sammlung/Rücktransport von Entsorgungsgut: hinreichenden Verwahr- und Transportschutz im oben genannten Sinne.

4. Risiken beim mobilen Einsatz von Datenverarbeitungssystemen

Der ortsungebundene Einsatz von Datenverarbeitungssystemen birgt das besondere Risiko in sich, dass beispielsweise Unbefugte darauf zugreifen oder das System aufgrund des Betreibens im Rahmen einer unsicheren Umgebung anderweitig kompromittiert wird, so dass besondere Schutzmaßnahmen unter Beachtung des Schutzbedarfes der betroffenen Daten erforderlich sind, z. B.:

- sofern möglich: Einsatz von zur Verfügung gestellten und zentral konfigurierten Datenverarbeitungssystemen, u. a. Verwaltung, Wartung, Weitergabe und Entsorgung durch Universitätsrechenzentrum der Technischen Universität Chemnitz (URZ),
- komplette zwangsweise Verschlüsselung der lokalen Datenbestände,
- keine Privat- bzw. Dritt-Nutzung der dienstlich zur Verfügung gestellten Datenverarbeitungssysteme,
- keine verändernden Zugriffe auf Betriebssystemebene (grundsätzlich keine Administrationsrechte),
- keine Manipulationen an der Hardware, gegebenenfalls Versiegelung/Verplombung des Gehäuses,
- Zugriffsschutz mittels Benutzerkennung/Login-Passwort (Passwortrichtlinie: u. a. Geheimhaltung, Komplexitätsanforderungen),
- sofern verfügbar: Zwei-Faktor-Authentifizierung (z. B. Token- bzw. Chipkarten-Authentifizierungen),
- Zugriffsschutz auch bei kurzzeitiger Unterbrechung, z. B. passwortgeschützte Tastatur-/Bildschirmsperre über „Windows-Taste + L“,
- fremde IT-Systeme (z. B. Internet-Café, fremder Büroraum, WLAN-Hotspot) gelten grundsätzlich als unsicher, eigene Sicherungsmaßnahmen erforderlich, z. B. Löschen temporärer Daten, Cachelöschung, keine Nutzung von Auto-Vervollständigungsfunktionen, Verschlüsselung mittels Verbindungsaufbau über Virtual Private Network (VPN).

5. Risiken beim Eintreten sicherheitsrelevanter Vorkommnisse

Sicherheitsrelevante Vorkommnisse (z. B. Verlust von Dokumenten, dienstlich eingesetzten IT-Systemen oder Datenträgern; Verlust von Daten über Hacker-, Phishing-Angriffe oder Schadsoftware, u. a. bei unbefugter Weitergabe/Offenlegung der URZ-Nutzerdaten) können – wenn nicht rechtzeitig und angemessen reagiert wird – einen materiellen oder immateriellen Schaden nach sich ziehen, so dass u. a. dem Risiko von Informationsdefiziten bei der Mobilen Arbeit mit angemessenen Schutzmaßnahmen vorgebeugt werden sollte, z. B.:

- unverzügliche Meldung beim Dienstvorgesetzen, soweit erforderlich beim URZ und IT-Sicherheitsbeauftragten,
- unverzügliche Meldung von Verletzungen des Schutzes personenbezogener Daten an den Datenschutzbeauftragten der Technischen Universität Chemnitz (Meldeformular: https://www.tu-chemnitz.de/rektorat/dsb/vorlagen.html#dokumentation),
- unverzügliches Ändern von Zugangsdaten betroffener IT-Systeme, gegebenenfalls Sperrung/Löschung betroffener IT-Systeme,
- gegebenenfalls erneute positive Evaluierung wiederaufgefundener verlorengegangener Geräte.