Dienstvereinbarung

zwischen der

Technischen Universität Chemnitz

vertreten durch den Rektor

und dem

Personalrat der Technischen Universität Chemnitz

vertreten durch den Vorsitzenden

zur

Mobilen Arbeit

Präambel[1]

Mobile Arbeit bezeichnet das Arbeiten außerhalb der Dienststelle. Die Beschäftigten erledigen ihre Arbeit von anderen Orten aus ggf. mit Hilfe elektronischer Geräte über jeweils zur Verfügung stehende Kommunikationsnetze.
Mobile Arbeit soll im Interesse von Dienststelle und Beschäftigten Möglichkeiten zur Flexibilisierung der Arbeitsorganisation schaffen. Dies soll dazu beitragen, Motivation und Arbeitszufriedenheit zu steigern und dadurch einen positiven Effekt auf die Arbeitsproduktivität und -qualität zu bewirken.

Mobile Arbeit dient vorrangig folgenden Zielen:

- bessere Vereinbarkeit von Beruf und Familie durch stärkere individuelle Arbeitsorganisation,
- Integration von Menschen mit Schwerbehinderung,
- Wiedereingliederung, z. B. nach längerer Krankheit, und damit der positiven Beeinflussung von Fehlzeiten,
- Steigerung der Attraktivität der Dienststelle als Arbeitgeber,
- Sicherung des Verbleibs und der Gewinnung von qualifizierten Beschäftigten,
- konzentrierter, ablenkungsfreier Tätigkeit, z. B. in Hochleistungsphasen.

§ 1 Geltungsbereich

Diese Dienstvereinbarung gilt für alle Beschäftigten der TU Chemnitz.

§ 2 Begriffsbestimmung

(1) Unter Mobiler Arbeit ist die Erfüllung von arbeitsvertraglich geschuldeter Leistung außerhalb der Dienststelle zu verstehen, sofern es sich nicht um Dienstreisen handelt.

[1] Aus Gründen der Vereinfachung und besseren Lesbarkeit, wird in der vorliegenden Dienstvereinbarung in der Regel das generische Maskulinum verwendet. Sämtliche Personenbezeichnungen gelten unabhängig davon aber gleichermaßen für alle Geschlechter.

(2) Die Arbeit am häuslichen Arbeitsplatz (Homeoffice) wird als Sonderform der Mobilen Arbeit betrachtet.

(3) Bei Mobiler Arbeit handelt es sich nicht um Heimarbeit im Sinne des Heimarbeitsgesetzes und nicht um Telearbeit im Sinne der Arbeitsstättenverordnung. Rufbereitschaft gilt nicht als Mobile Arbeit im Sinne dieser Vereinbarung, für sie gelten spezielle Bedingungen.

(4) Mobile Arbeit wird alternierend ausgeübt, sodass die geschuldete Arbeitsleistung, entsprechend der getroffenen Vereinbarung, sowohl in der Dienststelle als auch außerhalb der Dienststelle erbracht wird.

(5) Entsprechend der Dienstvereinbarung wird zwischen regelmäßiger (§ 5) und kurzzeitiger Mobiler Arbeit (§ 6) unterschieden.

(6) Die individuelle Gestaltung der Mobilen Arbeit wird gemäß § 5 in einer schriftlichen Vereinbarung (Anlage 1) geregelt. Es sind die Hinweise gemäß Anlagen 2 - 4 zu beachten.

§ 3 Voraussetzungen

(1) Die dem Beschäftigten übertragenen Tätigkeiten müssen sich für Mobile Arbeit eignen. Grundsätzlich sind solche Tätigkeiten geeignet, die eigenständig und eigenverantwortlich durchführbar sind und die ohne Beeinträchtigung des Dienstbetriebes bei eingeschränktem, unmittelbarem Kontakt der Teilnehmer zur Dienststelle verlagert werden können. Ebenso muss der Beschäftigte für Mobile Arbeit persönlich geeignet sein, u. a. verantwortungsbewusst, selbstmotiviert, strukturiert und hinreichend geschult und sensibilisiert im sicheren Umgang mit Informationstechnik und (personenbezogenen) Daten sein.

(2) In der Probezeit ist Mobile Arbeit in der Regel nicht zugelassen.

(3) Für Auszubildende ist in der Regel Mobile Arbeit ausgeschlossen. Im Ausnahmefall kann nach Zustimmung des Ausbilders und der Ausbildungsleitung von kurzfristiger Mobiler Arbeit Gebrauch gemacht werden.

(4) Im Rahmen der Mobilen Arbeit sind die datenschutzrechtlichen Bestimmungen einzuhalten. Vor Aufnahme der Mobilen Arbeit ist mit dem Fachvorgesetzten der Schutzbedarf der zu bearbeitenden Daten zu bestimmen. Tätigkeiten, die auf Grund ihrer Einstufung besonders vertraulich (Schutzbedarf „sehr hoch“) zu behandeln sind, dürfen außerhalb der Dienststelle nur im Homeoffice (häuslicher Arbeitsplatz) unter Beachtung erhöhter Anforderungen zum Datenschutz ausgeführt werden. Änderungen der Adresse des Homeoffice sind unverzüglich anzuzeigen.

(5) Die Inanspruchnahme der Mobilen Arbeit darf nicht zur Überlastung der übrigen Beschäftigten in der Organisationseinheit führen.

§ 4 Bedingungen

(1) Das Dienst- bzw. Arbeitsverhältnis bleibt unberührt. Lediglich die Präsenzpflicht in der Dienststelle wird für die Dauer der Verlagerung des Arbeitsplatzes verändert.

(2) Bestehende Regelungen wie beispielsweise Dienstvereinbarungen gelten unverändert oder zumindest sinngemäß weiter, soweit sie ihrem Sinn nach anwendbar bleiben und nicht in dieser Dienstvereinbarung ausdrücklich etwas anderes vereinbart ist. Die Dienstvereinbarung zur Arbeitszeitordnung in der jeweils geltenden Fassung findet für die

Teilnehmer der Mobilen Arbeit (ausgenommen Regelungen zur Funktionszeit) Anwendung. Dienst im Rahmen der Mobilen Arbeit an Sonn- und Feiertagen sowie an sonstigen dienstfreien Werktagen bedarf der Anordnung oder Einwilligung durch die Dienststelle.

(3) Ein Rechtsanspruch auf Teilnahme an Mobiler Arbeit besteht nicht.

(4) Mobiles Arbeiten während des Urlaubs und einer Krankheit (Arbeitsunfähigkeit) ist untersagt.

(5) Mobile Arbeit darf sich für den Beschäftigten nicht nachteilig auf den beruflichen Werdegang auswirken und in der dienstlichen Beurteilung keine negative Bewertung oder ähnliche Nachteile nach sich ziehen. Ebenso wenig dürfen den nicht an Mobiler Arbeit teilnehmenden Beschäftigten solche Nachteile entstehen.

(6) Der Arbeitsplatz in der Dienststelle bleibt während der Mobilen Arbeit erhalten.

§ 5 Regelmäßige Mobile Arbeit

(1) Regelmäßige Mobile Arbeit ist durch den Beschäftigten formlos beim Fachvorgesetzten zu beantragen.

(2) Soweit die Voraussetzungen nach § 3 und § 4 erfüllt sind, ist zwischen dem Fachvorgesetzten und dem Beschäftigten innerhalb von drei Wochen nach Antragstellung eine individuelle schriftliche Vereinbarung zu schließen, in der die Einzelheiten geregelt werden (siehe Anlage 1). Die Vereinbarung ist zeitlich zu befristen. Eine Verlängerung ist auf Antrag möglich.

(3) Die Lage, Dauer und Verteilung der Arbeitszeit auf den Arbeitsplatz in der Dienststelle und dem außerhalb der Dienststelle befindlichen Arbeitsplatz sind zwischen der Dienststelle und den Beschäftigten individuell in der Vereinbarung (Anlage 1) festzulegen. Mindestens 60 % der geschuldeten Arbeitsleistung sind in der Regel am Arbeitsplatz in der Dienststelle zu erbringen.

(4) Die Vereinbarung ist vom Fachvorgesetzten als Kopie/Scan nach beidseitiger Unterzeichnung zur Kenntnis und Ablage in der Personalakte an die E-Mail-Adresse „mobile_arbeit@verwaltung.tu-chemnitz.de“ zu senden.

(5) Beabsichtigt der Fachvorgesetzte einen Antrag auf regelmäßige Mobile Arbeit abzulehnen, sind das Dezernat Personal über die o. g. E-Mail-Adresse und über dieses der jeweilige Dienstvorgesetzte unverzüglich, jedoch spätestens innerhalb drei Wochen nach Antragstellung zu informieren und die Ablehnung substantiiert zu begründen. Das Dezernat Personal leitet umgehend ein Mitbestimmungsverfahren analog § 80 Abs. 1 Nr. 17 SächsPersVG ein.

(6) Mobile Arbeit endet zum vereinbarten Zeitpunkt oder automatisch mit der Beendigung des zugrundeliegenden Dienst- bzw. Arbeitsverhältnisses.

(7) Die Dienststelle ist berechtigt, die Vereinbarung gemäß Abs. 2 aus wichtigem Grund vorzeitig zu beenden. Ein wichtiger Grund ist insbesondere anzunehmen, wenn eine der in § 3 und § 4 genannten Voraussetzungen entfallen ist oder der Beschäftigte gegen die Dienstvereinbarung oder die darauf beruhende Vereinbarung gemäß Abs. 2 verstößt. Bei einer vorzeitigen Beendigung aus Gründen, die nicht vom Beschäftigten zu vertreten sind, sollen dem Beschäftigten vier Wochen zur Umstellung auf die veränderten Gegebenheiten eingeräumt werden. Darüber hinaus hat der Beschäftigte das Recht, die

gemäß Abs. 2 abgeschlossene Vereinbarung aus wichtigem Grund mit einer Frist von vier Wochen zu kündigen und an den Arbeitsplatz in der Dienststelle zurückzukehren.

(8) Dem Beschäftigten dürfen durch die Ausübung seines Kündigungsrechts keine Nachteile entstehen.

§ 6 Kurzzeitige Mobile Arbeit

(1) Bei kurzzeitiger Mobiler Arbeit handelt es sich um einen Ausnahmefall, der situativ und nicht zu regelmäßigen Zeiten und in festgelegtem Umfang eintritt.

(2) Die kurzzeitige Mobile Arbeit darf drei Tage hintereinander nicht überschreiten und soll nicht öfter als zweimal pro Monat zur Anwendung kommen.

(3) Die kurzzeitige Mobile Arbeit wird formlos zwischen Beschäftigtem und Fachvorgesetztem vereinbart. Eine Vereinbarung nach § 5 ist dabei nicht notwendig. Eine mündliche Absprache ist durch den Fachvorgesetzten per E-Mail zu bestätigen. Im Übrigen gelten die Bestimmungen dieser Dienstvereinbarung.

§ 7 Organisation Mobiler Arbeit

(1) Bei dringender dienstlicher Notwendigkeit kann der Fachvorgesetzte unter Berücksichtigung der Vereinbarung mit dem Beschäftigten eine Anwesenheit am dienstlichen Arbeitsplatz anordnen. Hierdurch entstehende Wegezeiten gelten als Arbeitszeit, die Wegekosten werden nicht erstattet. Die Belange des Beschäftigten sind zu berücksichtigen.

(2) Eine Bereitstellung der erforderlichen Arbeits- und Verbrauchsmittel durch die und auf Kosten der Dienststelle wird in der individuellen Vereinbarung gemäß Anlage 1 geregelt.

(3) Bei der Nutzung von dienststelleneigener Technik obliegt deren Wartung der Dienststelle und ist bei Bedarf in der Dienststelle vorzulegen. Für die Nutzung der bereitgestellten Arbeits- und Verbrauchsmittel gelten die gleichen Regeln wie am Arbeitsplatz in der Dienststelle.

(4) Bei Ausfällen und Störungen der genutzten Technik während der vereinbarten Arbeitszeit erfolgt keine Arbeitsunterbrechung. Ausfälle und Störungen der genutzten Technik sind unverzüglich dem Fachvorgesetzten zu melden sowie die Möglichkeiten einer anderweitigen Erledigung von Dienstaufgaben ohne Technik abzustimmen.

(5) Für Mobile Arbeit gelten die gleichen Antrags-, Anzeige- und Meldepflichten wie am Arbeitsplatz in der Dienststelle (z. B. bei Urlaub, Krankheit, Arbeitsbefreiung usw.).

(6) Bei Bedarf stellt der Beschäftigte einen häuslichen Arbeitsplatz kostenfrei zur Verfügung. Die Betriebskosten des häuslichen Arbeitsplatzes werden nicht erstattet.

(7) Die Nutzung privater Arbeitsmittel erfolgt auf eigenes Risiko. Es können keine Ansprüche (z. B. Abnutzung, Reparatur) geltend gemacht werden.

(8) Fahrtkosten zwischen dem Mobilen Arbeitsplatz und dem Arbeitsplatz in der Dienststelle werden nicht erstattet. Bei Dienstreisen, die nicht von der Dienststelle aus angetreten werden, wird als Bezugspunkt die Wohnung im Sinne von § 2 Abs. 3 SächsRKG zugrunde gelegt.

(9) Beschäftigte mit Behinderungen, die für ihre Arbeit technische Hilfen benötigen, werden von der Dienststelle zur Umsetzung der Mobilen Arbeit unterstützt. Konkrete Maßnahmen werden in der individuellen Vereinbarung gemäß Anlage 1 geregelt.

(10) Die Dienststelle stellt sicher, dass Beschäftigte mit Mobiler Arbeit über betriebliche Vorgänge und Bekanntmachungen, Weiterbildungsmaßnahmen sowie über sonstige dienststelleninterne Informationen rechtzeitig und umfassend unterrichtet werden. Dienstberatungen etc. sollen so terminiert werden, dass Beschäftigte mit Mobiler Arbeit teilnehmen können. Diese haben außerdem das Recht, an allen Versammlungen, Besprechungen, Fortbildungen, Gemeinschaftsveranstaltungen etc. teilzunehmen.

(11) Dem Beschäftigten stehen auch in Mobiler Arbeit sämtliche betrieblichen Maßnahmen der Gesundheitsfürsorge offen.

(12) Der Beschäftigte ist vor Abschluss der Vereinbarung über den gesetzlichen Unfallversicherungsschutz aufzuklären.

§ 8 Datenschutz und Informationssicherheit

(1) Die für die Dienststelle gültigen gesetzlichen und rechtlichen Bestimmungen sowie Ordnungen und Richtlinien zum Datenschutz und zur Informationssicherheit in den jeweils gültigen Fassungen finden auch für Mobile Arbeit uneingeschränkt Anwendung.

(2) Dienstliche Daten und Informationen in jeder Form sind auch am Mobilen Arbeitsplatz vor dem unberechtigten Zugriff Dritter zu schützen und sicher zu verwahren.

(3) Vor Aufnahme von Mobiler Arbeit sind dem Beschäftigten die datenschutzrechtlichen Bestimmungen und Risiken durch die Dienststelle nachweislich zur Kenntnis zu geben (siehe Anlagen 2 – 4). Beschäftigte mit Teilnahme an Mobiler Arbeit werden durch die Dienststelle über entsprechende Fortbildungsmaßnahmen zu Datenschutz und Informationssicherheit, welche ihren Arbeitsbereich betreffen könnten, informiert. Soweit erforderlich, sollen sie daran teilnehmen.

(4) Die Nutzung privater Geräte ist ausschließlich zur Verarbeitung von Daten mit dem Schutzbedarf „normal“ gemäß Anlage 4 zugelassen. Die Nutzung privater Geräte zur Verarbeitung von Daten mit Schutzbedarf „hoch“ und „sehr hoch“ ist unzulässig und ausgeschlossen. Für den Fall des Einsatzes privater Geräte hat der Beschäftigte sicherzustellen, dass die getroffenen Maßnahmen der IT-Sicherheit dem Stand der Technik entsprechen und ein ausreichender technisch-organisatorischer Datenschutz gewährleistet ist.

§ 9 Haftung

(1) Die Haftung des Beschäftigten in Mobiler Arbeit richtet sich nach den geltenden gesetzlichen und tariflichen Bestimmungen.

(2) Vor der Geltendmachung von Ersatzansprüchen gegen einen Beschäftigten ist ein Mitbestimmungsverfahren gemäß § 80 Abs. 1 Nr. 15 SächsPersVG einzuleiten.

§ 10 Besondere Rechte

Die Beteiligungs- und Informationsrechte der Personalvertretung und, soweit betroffen, der Schwerbehindertenvertretung und der Frauenbeauftragten bleiben unberührt.

§ 11 Schlussbestimmungen

(1) Die Dienstvereinbarung tritt zum 01.01.2023 in Kraft. Zugleich verliert die Dienstvereinbarung zur Mobilen Arbeit vom 29.07.2019 ihre Gültigkeit.

(2) Sollten einzelne Bestimmungen dieser Dienstvereinbarung unwirksam sein oder werden, so wird dadurch die Wirksamkeit der übrigen Bestimmungen nicht berührt. Für einen solchen Fall verpflichten sich beide Seiten, eine wirksame Regelung zu treffen, die dem Zweck der unwirksamen Regelung möglichst nahekommt.

(3) Bezüglich der Kündigung dieser Dienstvereinbarung gilt § 84 Abs. 3 SächsPersVG; eine Nachwirkung entsprechend § 84 Abs. 4 SächsPersVG wird ausdrücklich vereinbart. Unabhängig davon wird in zwei Jahren die Dienstvereinbarung evaluiert und ggf. angepasst.

(4) Die Möglichkeit der Vertragsparteien, die Dienstvereinbarung jederzeit in beiderseitigem Einvernehmen zu verändern, bleibt unberührt. Bestehende Vereinbarungen gemäß § 5 Abs. 2 bleiben bei einer Kündigung der Dienstvereinbarung unberührt.

Chemnitz, den 06.10.2022

gez. Prof. Dr. Gerd Strohmeier	gez. Frank Hohaus
Rektor	Vorsitzender des Personalrates

Anlagen

Anlage 1: Vereinbarung zur Mobilen Arbeit

Anlage 2: Kurzüberblick zum Datenschutz und zur Informationssicherheit bei Mobiler Arbeit für Beschäftigte der Technischen Universität Chemnitz

Anlage 3: Merkblatt zum Datenschutz und zur Informationssicherheit bei Mobiler Arbeit für Beschäftigte der Technischen Universität Chemnitz

Anlage 4: Feststellung des Schutzbedarfes der zu verarbeitenden Informationen bei Mobiler Arbeit für Beschäftigte der Technischen Universität Chemnitz

Vereinbarung gemäß § 5 Abs. 2 der Dienstvereinbarung zur Mobilen Arbeit

(Auszufüllen durch die/den Beschäftigte/n und die/den Fachvorgesetzte/n)

Zwischen der

Technischen Universität Chemnitz

und

Name, Vorname: _____

wohnhaft in: _____

Struktureinheit: _____

Fachvorgesetzte/r: _____

wird Folgendes vereinbart:

§ 1 Grundlage

Grundlage dieser Vereinbarung ist die Dienstvereinbarung an der Technischen Universität Chemnitz zur Mobilen Arbeit vom 06.10. 2022.

§ 2 Laufzeit

Die Mobile Arbeit wird mit der/dem Beschäftigten für den Zeitraum

vom _____ bis zum _____ vereinbart.

§ 3 Aufgabenstellung

Während der Mobilen Arbeit werden folgende Tätigkeiten ausgeführt, die gemäß dem Daten-/Informationsschutz in eine der Kategorien nach Anlage 4 der Dienstvereinbarung eingeordnet werden:

Tätigkeiten	Schutzbedarf der Tätigkeit N – normal H – hoch SH – sehr hoch		
	N	H	SH
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐
	☐	☐	☐

§ 4 Arbeitszeit

(1) Die durchschnittliche regelmäßige wöchentliche Arbeitszeit beträgt _____ Stunden, davon werden in der Regel _____ Stunden in Mobiler Arbeit erbracht.

(2) Die Arbeitstage an denen Mobile Arbeit erbracht wird, werden zwischen der/dem Beschäftigten und der/dem Fachvorgesetzen abgestimmt:

☐ feste Wochentage: _____ ☐ flexibel: _____

(3) Zur Erreichbarkeit am Mobilen Arbeitsplatz werden mit der/dem Beschäftigten folgende (feste) Kommunikationszeiten innerhalb der täglichen Arbeitszeit vereinbart:

☐ flexible / ☐ feste Tage	von	bis

(4) Die Erfassung der Arbeitszeit am Mobilen Arbeitsplatz erfolgt entsprechend den allgemeinen Regelungen und Vereinbarungen zur Arbeitszeiterfassung (vgl. Dienstvereinbarung zur Arbeitszeitordnung).

§ 5 Arbeitsort, Arbeitsplatz

☐ Die/der Beschäftigte ist frei in der Wahl des Arbeitsortes.

☐ Es wird ein fester Arbeitsplatz (Homeoffice) außerhalb der Dienststelle vereinbart (zwingend notwendig für Tätigkeiten mit sehr hohem Schutzbedarf).
Adresse:

(Eine Änderung dieser Adresse ist der/dem Fachvorgesetzten unverzüglich anzuzeigen.)

Die/der Beschäftigte hat sicherzustellen, dass der Arbeitsort und der Arbeitsplatz den gesetzlichen Anforderungen hinsichtlich Arbeits-, Gesundheits- und Daten-/Informationsschutz entspricht und die geltenden Sicherheits- und Ergonomiestandards erfüllt.

§ 6 Arbeits- und Verbrauchsmittel

Die Dienststelle stellt der/dem Beschäftigten folgende Arbeits-/Verbrauchsmittel bzw. technische Hilfsmittel im Sinne von § 7 Abs. 9 der Dienstvereinbarung zur Verfügung:

- _____
- _____
- _____
- _____
- _____
- _____

Die/der Beschäftigte stellt folgende Arbeitsmittel unentgeltlich zur Verfügung:

- _____
- _____
- _____
- _____
- _____
- _____

§ 7 Daten- und Informationsschutz

(1) Die/der Beschäftigte verpflichtet sich zur strikten Einhaltung des Datenschutzes und gewährleistet den Schutz von dienstlichen Unterlagen am Mobilen Arbeitsplatz.

(2) Der Schutz sensibler Daten durch Passwörter bzw. eine Verschlüsselung wird durch die Dienststelle gewährleistet und durch die/den Beschäftigte/n umgesetzt.

(3) Sicherheitssoftware für den Schutz vor Viren etc. wird durch die Dienststelle bereitgestellt.

(4) Dienstliche Unterlagen und Datenträger dürfen nur in der Dienststelle entsorgt werden, es sei denn, besondere Entsorgungseinrichtungen wurden durch die Dienststelle zur Verfügung gestellt.

(5) Im Falle der Nutzung von selbst administrierten mobilen IT-Geräten versichert die/der Beschäftigte mit ihrer/seiner Unterschrift, dass diese Geräte die Anforderungen der Dienstvereinbarung Mobile Arbeit erfüllen.

(6) Der unterzeichnete „Kurzüberblick zum Datenschutz und zur Informationssicherheit bei Mobiler Arbeit für Beschäftigte der Technischen Universität Chemnitz“ ist Bestandteil dieser Vereinbarung.

§ 8 Änderung der Vereinbarung

Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform.

_____ , den _____ _____ , den _____

_____ _____
Fachvorgesetzte/r Beschäftigte/r

Verlängerung:

Diese Vereinbarung vom _____ wird verlängert bis _____

_____, den _____ _____, den _____

_____ _____
Fachvorgesetzte/r Beschäftigte/r

(Kopie/Scan an mobile_arbeit@verwaltung.tu-chemnitz.de für Ablage in der Personalakte)

Anlage: - Merkblatt zum Versicherungsschutz bei Mobiler Arbeit

- Kurzüberblick zum Datenschutz und zur Informationssicherheit bei Mobiler Arbeit für Beschäftigte der Technischen Universität Chemnitz

Information an Dezernat 2:

Gemäß § 5 Abs. 4 ist die unterzeichnete Vereinbarung und Anlage vom Fachvorgesetzten als Kopie/Scan nach beidseitiger Unterzeichnung zur Kenntnis und Ablage in der Personalakte an die E-Mail-Adresse

mobile_arbeit@verwaltung.tu-chemnitz.de

zu senden.

Kurzüberblick zum Datenschutz und zur Informationssicherheit bei Mobiler Arbeit für Beschäftigte der Technischen Universität Chemnitz vom 21. November 2022[1]

DATENSCHUTZ während der Mobilen Arbeit

Die Verarbeitung dienstlicher Informationen/Daten im Rahmen der Mobilen Arbeit ist auf das **ERFORDERLICHE MASS ZU BESCHRÄNKEN**. Nicht mehr benötigte Informationen/Daten sind unverzüglich an die Dienststelle zurückzuführen.

Dienstliche Informationen/Daten dürfen nur in **HINREICHEND SICHEREN UND GEEIGNETEN BEHÄLTNISSEN** zwischen der Dienststelle und dem Mobilen Arbeitsplatz transportiert werden. Das Transportrisiko ist geeignet zu begrenzen (bspw. unmittelbarer Weg ohne Zwischenstopps).

Der Mobile Arbeitsbereich sollte **ABSCHLIESSBAR** bzw. zumindest **ABTRENNBAR** und für Unberechtigte nicht einsehbar gestaltet sein und hinreichende **VERSCHLUSS- UND VERSTAUMÖGLICHKEITEN** bieten („aufgeräumter Arbeitsplatz“), so dass unberechtigte Personen (gilt auch für Familienangehörige) keinerlei Zugang oder Zugriff auf dienstliche Informationen/Daten (gilt bspw. auch für das unberechtigte Mithören von Telefonaten, Videokonferenzen) erhalten können (Vertraulichkeit).

Der Mobile Arbeitsplatz ist unter **WAHRUNG DES GESUNDHEITSSCHUTZES UND DER ARBEITSSICHERHEIT** zu gestalten, um mögliche Fehlerrisiken bei der Informations-/Datenverarbeitung zu minimieren (bspw. hinreichende Beleuchtung, Belüftung).

Um einen Verlust von Informationen/Daten möglichst ausschließen zu können, ist auf eine hinreichende **PHYSISCHE SICHERHEIT** u. a. der IT-Systeme zu achten (bspw. Diebstahlschutz).

Dienstliche Informationen/Daten werden grundsätzlich über **GEEIGNETE ENTSORGUNGSEINRICHTUNGEN AM DIENSTLICHEN ARBEITSPLATZ** und nicht im privaten Hausmüll entsorgt und bis dahin sicher verwahrt und transportiert.

Werden **BESONDERS SCHÜTZENSWERTE INFORMATIONEN/DATEN** (z. B. Beschäftigten-, Prüfungs-, Gesundheitsdaten) verarbeitet, sind regelmäßig **BESONDERE SCHUTZMASSNAHMEN** erforderlich (bspw. Einzeldatenverschlüsselung, Zwei-Faktor-Authentifizierung).

SICHERHEITSRELEVANTE VORKOMMNISSE UND DATENSCHUTZVERLETZUNGEN (bspw. Verlust von Informationen/Daten, Phishing-Angriffe) sind dem Fachvorgesetzten **UNVERZÜGLICH ZU MELDEN**, welcher gegebenenfalls weitere Meldungen an das URZ, den Datenschutzbeauftragten der TU Chemnitz etc. veranlasst.

Kontakt: https://www.tu-chemnitz.de/rektorat/dsb/ | Datenschutzbeauftragter der TU Chemnitz

Informationen/Empfehlungen des Datenschutzbeauftragten:
https://www.tu-chemnitz.de/rektorat/dsb/vorlagen.html#dokumentation

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

INFORMATIONSSICHERHEIT während der Mobilen Arbeit

Die **TU CHEMNITZ TRÄGT DIE VERANTWORTUNG FÜR DIE DIENSTLICH BEREITGESTELLTE UND FREIGEGEBENE / ADMINISTRIERTE HARD- UND SOFTWARE**, welche nicht privat und nicht durch unberechtigte Dritte genutzt werden darf. Veränderungen oder Manipulationen sind grundsätzlich unzulässig. Eine **SICHERE VERWAHRUNG** ist zu gewährleisten, ein Verlust ist unverzüglich zu melden.

Die **NUTZUNG PRIVATER HARD- UND SOFTWARE** erfolgt freiwillig, eigenverantwortlich und auf eigenes Risiko (**PERSÖNLICHES HAFTUNGSRISIKO**) und sollte deshalb nur ausnahmsweise und nur bei einem normalen Schutzbedarf der betroffenen Daten/Informationen unter Wahrung einer hinreichenden Datentrennung (dienstlich vs. privat) erfolgen. **EIN SUPPORT DURCH DIE TU CHEMNITZ FINDET NICHT STATT.** Installieren Sie wenn möglich und lizenzrechtlich zulässig die kostenfrei von der TU Chemnitz zur Verfügung gestellte Virenschutzsoftware.

Installierte **SOFTWARE** (u. a. Betriebssystem, Virenschutzsoftware) muss regelmäßig auf **SICHERHEITSUPDATES** überprüft werden. Verfügbare Updates sind unverzüglich (möglichst automatisiert) zu installieren.

Bei regulären Tätigkeiten sind **KEINE ADMINISTRATIONSBERECHTIGUNGEN** zu nutzen.

Die **WEITERLEITUNG DIENSTLICHER E-MAILS** an private E-Mail-Accounts ist **UNZULÄSSIG**.

Auch bei kurzzeitiger Arbeitsunterbrechung ist ein **HINREICHENDER ZUGRIFFSSCHUTZ** sicherzustellen (bspw. passwortgeschützte Tastatur-/Bildschirmsperre, Security-Token).

Es sollten ausschließlich **SICHERE UND EINMALIGE PASSWÖRTER** verwendet werden (mindestens acht Stellen aus allen vier Zeichenklassen), welche vertraulich zu behandeln sind. **WIR FRAGEN SIE NIEMALS NACH IHREM PASSWORT!**

Grundsätzlich sollten von der TU Chemnitz zur Verfügung gestellte und **ZENTRAL KONFIGURIERTE DATENVERARBEITUNGSSYSTEME ÜBER EINE VPN-VERBINDUNG** der TU Chemnitz genutzt werden (u. a. TUCcloud, AFS-Verzeichnisse, BigBlueButton der TU Chemnitz).

FREMDE IT-SYSTEME (z. B. WLAN-Hotspot am Bahnhof, Flughafen) gelten grundsätzlich als **UNSICHER** und erfordern eigene Sicherungsmaßnahmen (bspw. VPN, SSH, HTTPS).

MOBILE DATENBESTÄNDE sollten zwangsweise und hinreichend **VERSCHLÜSSELT** sein. Gleichwohl ist die **VERFÜGBARKEIT UND WIEDERHERSTELLBARKEIT** zu gewährleisten. Fremde Datenträger sollten vor der Verwendung u. a. auf Schadsoftware geprüft werden.

Machen Sie sich bewusst, dass gerade während der Mobilen Arbeit die **GEFAHR SOG. SOCIAL ENGINEERING ANGRIFFE** besonders hoch ist. Auf einen **SORGSAMEN UMGANG** sollte geachtet werden (bspw. bei Downloads, Verlinkungen, Telefonanrufen, privaten Gesprächen).

Kontakt: *support@hrz.tu-chemnitz.de* | URZ-Nutzerservice

Informationen/Empfehlungen des URZ: *https://www.tu-chemnitz.de/urz/desktop/mobil/*

BESTÄTIGUNG DER KENNTNISNAHME / EINWILLIGUNGSERKLÄRUNG

Die Beschäftigten sind auch während der Mobilen Arbeit dazu verpflichtet und tragen hierfür die Verantwortung, sich an die geltenden Vorschriften betreffend den Datenschutz und die Informationssicherheit zu halten. Ausführlichere Hinweise entnehmen Sie bitte dem „Merkblatt zum Datenschutz und zur Informationssicherheit bei Mobiler Arbeit für Beschäftigte der Technischen Universität Chemnitz vom 21. November 2022“ (Anlage 3 der Dienstvereinbarung zur Mobilen Arbeit) sowie den einschlägigen Empfehlungen u. a. des Datenschutzbeauftragten der TU Chemnitz und des Universitätsrechenzentrums, insbesondere zu den Anforderungen an mobile Geräte.

Der „Kurzüberblick zum Datenschutz und zur Informationssicherheit bei Mobiler Arbeit für Beschäftigte der Technischen Universität Chemnitz vom 21. November 2022“ ist mir heute überreicht und von mir zur Kenntnis genommen worden. Darüber hinausgehend versichere ich, dass ich auch die von der Dienststelle zur Verfügung gestellten ausführlichen Hinweise betreffend den Datenschutz und die Informationssicherheit bei Mobiler Arbeit in der jeweils aktuell gültigen Fassung zur Kenntnis genommen habe und zukünftig nehmen werde sowie diese beachte.

Datum	Unterschrift Beschäftigte/r

Merkblatt

**zum Datenschutz und zur Informationssicherheit
bei Mobiler Arbeit für Beschäftigte der Technischen Universität Chemnitz
vom 15. November 2022[1]**

Das Merkblatt zum Datenschutz und zur Informationssicherheit bei Mobiler Arbeit für Beschäftigte der Technischen Universität Chemnitz vom 15. November 2022 dient als nachweisbare Erläuterung der datenschutzrechtlichen Bestimmungen und Risiken im Sinne von § 8 Abs. 3 S. 1 Dienstvereinbarung zur Mobilen Arbeit.

Über darüber hinausgehende 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. Darüber hinausgehend 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 Fachvorgesetzten, 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.

Feststellung des Schutzbedarfes der zu verarbeitenden Informationen bei Mobiler Arbeit für Beschäftigte der Technischen Universität Chemnitz vom 15. November 2022[1]

Gemäß § 3 Abs. 4 der Dienstvereinbarung zur Mobilen Arbeit müssen Beschäftigte vor Aufnahme der Mobilen Arbeit mit dem Fachvorgesetzten den Schutzbedarf der während der Mobilen Arbeit zu verarbeitenden Informationen bestimmen, um ein angemessenes Schutzniveau auch während der Mobilen Arbeit sicherstellen zu können. Der Fachvorgesetzte trägt die Verantwortung dafür, dass bei der Klassifizierung die erforderliche Sorgfalt angewandt worden ist. Die vorliegende beispielhafte, nicht abschließende Aufzählung soll hierbei unterstützen, ersetzt jedoch keine Klassifizierung im Einzelfall, welche von der vorliegenden Einstufung gemessen an den Schutzzielen (Vertraulichkeit, Verfügbarkeit, Integrität) auch abweichen kann. Ist eine Zuordnung nicht eindeutig möglich, sollte der jeweils höhere Schutzbedarf zugrunde gelegt werden. Der Datenschutzbeauftragte der TU Chemnitz steht jederzeit, insbesondere auch in Zweifelsfällen, für eine Abstimmung bzw. Beratung und Unterstützung bei der Informationsklassifizierung zur Verfügung.

NORMALER SCHUTZBEDARF

„normal“: … Auswirkungen bei unzureichendem Schutz begrenzt und überschaubar

- öffentliches Vorlesungsverzeichnis, Lehrveranstaltungsplanung etc.
- Lehrmaterialien für Lehrveranstaltungen
- Vor-/Nachbereitung von Lehrveranstaltungen
- öffentliche Telefon-/Adressverzeichnisse
- dienstliche Kontaktdaten von Beschäftigten
- öffentliche Mitteilungen, bspw. Pressemitteilungen, Veranstaltungen, Newsletter
- Werbematerialien, z. B. Flyer, Broschüren, Aushänge, Plakate etc.
- Webseiteninhalte, Soziale Medien (ohne Zugriffsbeschränkungen) etc.
- öffentliche Beratungen, Tagungen etc.
- Recherchearbeiten in öffentlichen Datenbanken, bspw. Bibliothekssystem

HOHER SCHUTZBEDARF

„hoch“: … Auswirkungen bei unzureichendem Schutz beträchtlich, erheblich

- interne (Kontakt-)Verzeichnisse, Datenbanken
- Telefon- und E-Mail-Kommunikation (abhängig von Inhalt, Gesprächsteilnehmern etc.)
- interne Beratungen
- Forschungsdaten (einzelfallabhängig)
- Verwaltungstätigkeiten, u. a. Rechnungsbearbeitung, Zahlungsanweisungen, Abrechnungen, Haushalt, Mittelverwaltung, Kontenabfragen etc.
- Studierendenverwaltung, u. a. Matrikelnummer, Anmelde-/Anwesenheitslisten, Lernplattform
- technische Daten, u. a. Gebäude-/Raumdaten, Bauplanung, Netzwerkpläne, Konfigurationseinstellungen etc.
- Projektantragsstellung, Projektberichte etc.

SEHR HOHER SCHUTZBEDARF

„sehr hoch“: … Auswirkungen bei unzureichendem Schutz bedrohlich, katastrophal

- Personaldaten, u. a. Gehalts-/Bezüge-/Reisekostenabrechnung, Arbeitszeugnisse, Personalnummer, Arbeitszeitnachweise etc.
- Sozialdaten (Sozialgeheimnis)
- Prüfungsdaten, insbes. Prüfungsergebnisse
- besondere Kategorien personenbezogener Daten (Art. 9, 10 DSGVO), insbes. Gesundheitsdaten, biometrische Daten, Straftaten etc.
- besondere Geheimhaltungs-/Vertraulichkeitsverpflichtung, bspw. § 203 StGB, § 3 TTDSG
- Betriebs-, Geschäfts-, Dienst-, Berufs- und/oder Amtsgeheimnisse etc.
- nicht-öffentliche Beratungen, Gremiensitzungen
- Forschungsdaten (einzelfallabhängig)

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