UNIVERSITÄT
HEIDELBERG
ZUKUNFT
SEIT 1386

# EMPFEHLUNGEN UND ERLÄUTERUNGEN ZUR DIENSTVEREINBARUNG TELEARBEIT
AN DER UNIVERSITÄT HEIDELBERG

**1. Haben Mitarbeitende ein Recht auf Telearbeit?**
Universitäres Leben und Arbeiten erfordern sowohl eine akademische Präsenzkultur als auch moderne Arbeitsplätze und Arbeitsformen. Zur Erhöhung der Motivation und Zufriedenheit der Mitarbeiterinnen und Mitarbeiter wird Telearbeit als Möglichkeit der räumlichen und zeitlichen Flexibilisierung der Arbeitsorganisation genutzt. Der direkte persönliche Austausch in allen Bereichen der Universität ermöglicht eine bestmögliche Kommunikation. Ein grundsätzliches Recht auf Telearbeit besteht nicht. Bei der Entscheidung über einen Antrag sind besondere Umstände der jeweiligen Antragstellenden zu berücksichtigen, wie das Vorliegen einer Schwerbehinderung oder von Familien- oder Pflegeaufgaben.

Wenn Telearbeit vereinbart wurde, stehen die dienstlichen Belange im Bedarfsfall im Vordergrund.

**2. Verantwortlichkeit für die Telearbeitsvereinbarungen**
Die Entscheidungsfindung und die Vereinbarung der individuellen Regelungen über Telearbeit finden generell in der jeweiligen Einrichtung statt. Die Einrichtungsleitung kann die Verantwortung für den Abschluss der Telearbeitsvereinbarung schriftlich auf die verantwortlichen Führungskräfte delegieren. Um Rechtssicherheit zu erreichen, ist die in der Einrichtung unterzeichnete Telearbeitsvereinbarung an das Personaldezernat zu übersenden. Eine zusätzliche Genehmigung durch das Personaldezernat ist nicht erforderlich.

**3. Geltungsbereich der Dienstvereinbarung Telearbeit**
Die Regelungen der Dienstvereinbarung gelten für alle Beschäftigten der Universität Heidelberg mit Ausnahme jener, für die das Universitätsklinikum Heidelberg die Personalverwaltung vornimmt.

Beschäftigte, die mit der jeweiligen Einrichtungsleitung oder der verantwortlichen Führungskraft eine Vereinbarung zur Telearbeit abgeschlossen haben, können in den verschiedenen Telearbeitsmodellen arbeiten. Bereits vor Geltung der aktuellen Dienstvereinbarung abgeschlossene Telearbeitsvereinbarungen behalten für den vereinbarten Zeitraum ihre Gültigkeit.

**4. Formen bzw. Modelle sowie Umfang der Telearbeit**
Telearbeit wird an der Universität Heidelberg alternierend angeboten. Das bedeutet, dass Beschäftigte ihre individuelle Arbeitszeit teilweise in der Dienststelle und teilweise an einem festgelegten Telearbeitsplatz erbringen können. Es werden dazu schriftliche Vereinbarungen mit der Einrichtungsleitung, bzw. sofern an diese delegiert, mit der verantwortlichen Führungskraft abgeschlossen (im Weiteren vereinfachend: die Führungskraft). Dies ist für zwei Formen der Telearbeit möglich:

a) Die Hauptform ist die **„Reguläre Telearbeit“**. Sofern die dienstlichen Tätigkeiten und der Dienstbetrieb dies zulassen, können Anteile der regulären Arbeitszeit an festgelegten Tagen oder Teilen von Tagen in Telearbeit geleistet werden. Die Dienststelle empfiehlt, dass seitens der/dem für die Entscheidung über den Umfang der Gewährung der Telearbeit Verantwortlichen in der Regel bis zu 40% der individuellen Wochenarbeitszeit der Beschäftigten für die Aufgabenerledigung in Telearbeit als angemessen erachtet werden. Die Geltungsdauer der Telearbeitsvereinbarung beträgt bis zu einem Jahr und kann, sofern die

Voraussetzungen weiterhin gegeben sind, nach Ende der jeweiligen Vertragslaufzeit jeweils um wiederum ein Jahr verlängert werden.

b) Die alternative Form ist die **„Vorübergehende Telearbeit“**. Sie soll eine größtmögliche Flexibilität für die Beschäftigten und die Führungskräfte ermöglichen, um aufgrund kurzfristiger Bedarfe einen oder mehrere Telearbeitstage oder Teile von Arbeitstagen kurzfristig und auf direktem Zuruf vereinbaren zu können. Die Vereinbarung zur Vorübergehenden Telearbeit umfasst in der Regel 24 Telearbeitstage pro Kalenderjahr − dies sollte üblicherweise nicht überschritten werden. Auch bei dieser Form der Telearbeit beträgt die Geltungsdauer der Telearbeitsvereinbarung bis zu einem Jahr, mit der Option der Verlängerung um jeweils ein weiteres Jahr.

In der Telearbeitsvereinbarung wird ein Rahmen festgelegt, der bedarfsbezogen definiert wird. Dabei wird vereinbart, an welchen Wochentagen und an wie vielen Tagen im gesamten Jahr in „Vorübergehender Telearbeit“ gearbeitet werden kann und wie die konkrete Kommunikation zur Inanspruchnahme der Telearbeitsoption aussehen soll (z.B. per E-Mail, per E-Mail mit Rückantwort durch die Führungskraft oder telefonisch). Die „Vorübergehende Telearbeit“ kann für sich alleine oder zusätzlich zur „Regulären Telearbeit“ in einer zweiten Telearbeitsvereinbarung vereinbart werden.

### 5. Geltungsdauer der Telearbeitsvereinbarung

Jede Telearbeitsvereinbarung gilt längstens für ein Jahr. Den konkreten Umfang der „Regulären“ wie „Vorübergehenden Telearbeit“ legen die jeweilige Führungskraft und die betreffenden Beschäftigten individuell fest. Dabei trägt die Führungskraft die Verantwortung, dass für die Telearbeit die dienstlichen Belange vollumfänglich berücksichtigt werden.

Insbesondere bei der „Vorübergehenden Telearbeit“ ist zu beachten: Um eine größtmögliche Flexibilität zu schaffen und somit einen oder mehrere Telearbeitstage kurzfristig und auf direkten Zuruf zu vereinbaren, ist es angeraten, einen weiten Zeitrahmen in der Telearbeitsvereinbarung zu spannen.

Beispiel: Der Zeitrahmen kann von montags ab 6.00 Uhr bis freitags um 21.00 Uhr festgelegt werden, innerhalb dessen optional in „Vorübergehender Telearbeit“ gearbeitet werden kann. Die Inanspruchnahme erfolgt auf vereinbarten Zuruf, bspw. könnte dies per Telefon oder E-Mail geschehen. Der Modus, wie dies konkret vereinbart werden kann, wird in der Rahmenvereinbarung „Vorübergehende Telearbeit“ gemeinsam schriftlich festgelegt. Die Telearbeit kann auch für Teile eines Arbeitstages vereinbart bzw. in Anspruch genommen werden.

Die „Reguläre Telearbeit“ hat gegenüber der „Vorübergehenden Telearbeit“ den Vorteil, dass die Anwesenheitszeiten für das Kollegium meist berechenbarer sind.

### 6. Entscheidungsfindung: Vereinbarungsprozess und Kriterien

Die **Entscheidung** über das Arbeiten in Telearbeit sowie über die damit verbundenen Detailfragen trifft die Einrichtungsleitung bzw. die von ihr beauftragte Führungskraft für die Universität Heidelberg. Diese Befugnis kann im Einzelfall oder generell, befristet oder unbefristet auf Führungskräfte der jeweiligen Einrichtung delegiert werden.

Bei **Interesse an Telearbeit** wenden sich die Beschäftigten an die verantwortliche Führungskraft. Zunächst haben beide anhand der Dienstvereinbarung Telearbeit der Universität Heidelberg zu prüfen, ob die Arbeitsaufgaben der/ des anfragenden Beschäftigten in definierbaren Anteilen ohne qualitative und quantitative Abstriche telearbeitsfähig sind und ob die oder der Beschäftigte die persönlichen Voraussetzungen für Telearbeit mitbringt. Die Vorgesetzten prüfen, ob Telearbeit in die Abläufe und Organisation des Arbeitsbereiches passt. Sie tragen die Verantwortung dafür, dass der universitären Gemeinschaft durch das Arbeiten in Telearbeit keine Nachteile entstehen, sowohl mit Blick auf die Aufgabenerledigung als auch mit Blick auf die Zusammenarbeit mit den Kolleginnen und Kollegen, die in Präsenz arbeiten.

In einem Mitarbeiterinnen- bzw. Mitarbeitergespräch ist zu klären, ob die Rahmenbedingungen für das Arbeiten in Telearbeit passend sind und ob das Umfeld der Beschäftigten ein erfolgreiches Arbeiten am heimischen Arbeitsplatz ermöglichen würde.

Die für die Telearbeit vorgesehenen Dienstaufgaben müssen eigenständig, eigenverantwortlich und ohne nennenswerten zeitlichen Mehraufwand durchführbar und die übliche Erreichbarkeit muss wie im Rahmen der Tätigkeit am universitären Arbeitsplatz gegeben und sichergestellt sein.

### 7. Mitarbeiterinnen- bzw. Mitarbeitergespräch

Vor dem erstmaligen Abschluss einer Vereinbarung zur Telearbeit wie auch vor jeder Verlängerung der Telearbeit führen die jeweiligen Beschäftigten und ihre Führungskraft zeitnah nach Beantragung ein Mitarbeitergespräch, bei dem die Rahmenbedingungen zur Umsetzung einer gelingenden Telearbeit zentraler Gegenstand sind.

Zusätzlich sind die Themen Arbeitsschutz, Datenschutz und Informationssicherheit Gegenstand der Gespräche. Die Unterlagen zum Themenbereich Arbeitsschutz sind unter dem folgenden Link abrufbar: https://www.uni-heidelberg.de/universitaet/beschaeftigte/service/sicherheit/arbeitsstaetten/homeoffice.html

Auf der Website stehen zwei Dokumente zur Verfügung: Die „Gefährdungsbeurteilung zur Dienstvereinbarung Telearbeit“ ist vor Aufnahme der Telearbeit gemeinsam auszufüllen. Das Vorgehen ist dort beschrieben. Mit dem Dokument „Sicheres Arbeiten im Homeoffice“ machen sich die Führungskraft und die Beschäftigten in der Vorbereitung des Gesprächs vertraut.

Die gemeinsame Unterlage „Handreichung Datenschutz und IT-Sicherheit i. R. d. Telearbeit“ findet sich im Anhang dieser Anleitung. Mit ihr machen sich die Führungskraft und die Beschäftigten ebenfalls in der Vorbereitung des Gesprächs vertraut.

### 8. Erstellung der Vereinbarung für das Arbeiten in Telearbeit

Für beide Formen der Telearbeit stehen zu verwendende Formulare zur Telearbeitsvereinbarung auf der Webseite für die Telearbeit an der Universität Heidelberg zum Download bereit: https://www.uni-heidelberg.de/de/beschaeftigte-in-wissenschaft-verwaltung-und-technik/attraktive-rahmenbedingungen/telearbeit (zugangsgeschützt über Uni-ID)

Die Telearbeitsvereinbarung tritt bei Nutzung der vorgegebenen Formulare mit der beiderseitigen Unterschrift zum vereinbarten Termin in Kraft. Die rückerbetenen Mehrfertigungen werden von der Führungskraft an die personalverwaltende Stelle gesendet, wo sie aus versicherungsrechtlichen Gründen in die Personalakte der bzw. des jeweiligen Beschäftigten verfügt werden.

In der Telearbeitsvereinbarung legen Beschäftigte und Führungskräfte gemeinsam die wesentlichen Rahmenbedingungen der Tätigkeiten in Telearbeit fest:

a) Umfang der Telearbeit
b) Ggf. Arbeitsinhalte
c) Arbeitszeiten
d) Erreichbarkeit
e) Bei „Vorübergehender Telearbeit“: Modus, wie Telearbeitstage kurzfristig vereinbart werden sollen, z.B. per E-Mail-Kommunikation oder per Telefonat

Die Telearbeitsvereinbarungen stellen Nebenabreden zum Arbeitsvertrag dar und dürfen daher ausschließlich mittels den von der personalverwaltenden Stelle bereitgestellten aktuellen Mustern und ausschließlich unter den Voraussetzungen und im Rahmen der Dienstvereinbarung Telearbeit abgeschlossen werden.

In den Telearbeitsvereinbarungen sind zwei Erklärungen enthalten, deren Bestätigung zwingend für die Genehmigung des Arbeitens in Telearbeit sind:

a) **Erklärung über den Erhalt von Informationsmaterialien zu Arbeitsschutz, Informationssicherheit und Datenschutz (§ 4 Abs. 2 c) DV)**. Mit den „Informationsmaterialien zum Arbeitsschutz, zur Informationssicherheit und zum Datenschutz“ müssen sich die Führungskraft und die Beschäftigten vor dem Gespräch intensiv vertraut machen. Die Beschäftigten können diese Materialien zum Mitarbeitergespräch mitbringen und offene Fragen ansprechen. Etwaige Unsicherheiten können im Rahmen einer Beratung durch die Stabsstelle Datenschutz, die Abteilung Arbeitssicherheit sowie das IT-Sicherheitsteam des

Universitätsrechenzentrums aufgelöst werden. Beratung zu diesen Themen steht unter folgenden Kontaktdaten zur Verfügung:
Datenschutzbezogene Fragestellungen: datenschutz@uni-heidelberg.de
Informationssicherheits- bzw. IT-Sicherheitsbezogene Fragestellungen: it-sicherheit@urz.uni-heidelberg.de
Arbeitssicherheitsrechtliche Fragestellungen: sicherheit@zuv.uni-heidelberg.de

b) **Erklärung über die Erfüllung der erforderlichen Bedingungen zur Telearbeit am eigenen Telearbeitsplatz (§ 4 Abs. 3 DV)**. Mit der Erklärung über die Erfüllung der erforderlichen Bedingungen zur Telearbeit am eigenen Telearbeitsplatz (§ 4 Abs. 3 DV) bestätigen die Beschäftigten schriftlich, dass die Einhaltung der Voraussetzungen zur Telearbeit, wie sie in der Dienstvereinbarung in § 4 geregelt und als zwingend erforderlich zur Vergabe eines Telearbeitsplatzes vorgegeben sind, auch tatsächlich eingehalten werden. Das sind Regularien hinsichtlich der Ausstattung des Telearbeitsplatzes, den Anforderungen des Arbeitsschutzes, der Einhaltung der Vorgaben des Datenschutzes und der Informationssicherheit sowie der Absicherung von Zutritts- und Kontrollrechten zum heimischen Arbeitsplatz.

## 9. Beteiligungsrechte und -pflichten bei Ablehnung von Telearbeit

Sollten nach Abwägung aller Fakten und gegebenen Bedingungen der Anfrage nach Telearbeit eine Ablehnung oder Einschränkung beabsichtigt sein, so teilt die verantwortliche Führungskraft dies der bzw. dem jeweiligen Beschäftigten zeitnah schriftlich oder mündlich nebst Begründung und nach § 76 Abs. 3 LPVG einem Hinweis auf die Möglichkeit der Einbindung des Personalrats mit. Auf Antrag der bzw. des Beschäftigten kann der Personalrat gemäß § 75 Abs. 3 Ziff. 4 LPVG beteiligt werden.

Bei einer bzw. einem Beschäftigten mit Schwerbehinderung bzw. Gleichgestellten wird die Schwerbehindertenvertretung gemäß § 178 Absatz 2 SGB IX unverzüglich und umfassend von der verantwortlichen Führungskraft über die vorgesehene Ablehnung unterrichtet und vor einer Entscheidung angehört.

Bei einer bzw. einem Beschäftigten mit Familien- oder Pflegeaufgaben wird die Beauftragte für Chancengleichheit gemäß § 30 Absatz 5 ChancenG unverzüglich und umfassend von der verantwortlichen Führungskraft über die vorgesehene Ablehnung unterrichtet und vor einer Entscheidung angehört.

## 10. Aufkündigung der Telearbeitsvereinbarung

Grundsätzlich kann die Telearbeitsvereinbarung durch jede Partei mit einer Frist von vier Wochen zum Monatsende ordentlich schriftlich gekündigt werden. Eine Aufhebung im gegenseitigen Einvernehmen ist jederzeit möglich. Ein Abdruck des Kündigungsschreibens ist an die personalverwaltende Stelle zu übermitteln, es reicht ein Scan dessen.

Liegen wichtige Gründe vor, insbesondere, wenn sich die zuvor abgefragten Voraussetzungen für den Telearbeitsplatz bei den Beschäftigten nicht mehr einhalten lassen, kann die Telearbeitsvereinbarung von jeder Partei auch kurzfristig gekündigt werden. Dafür sind allerdings belegbare Gründe notwendig. Das ist beispielsweise dann der Fall, wenn die zuvor von den Beschäftigten schriftlich bestätigten Voraussetzungen hinsichtlich der Ausstattung des Telearbeitsplatzes, der Anforderungen des Arbeitsschutzes, der Einhaltung der Vorgaben des Datenschutzes und der Informationssicherheit sowie der Absicherung von Zutritts- und Kontrollrechten zum heimischen Arbeitsplatz nicht mehr vollständig gegeben sind (gemäß § 4 der DV). Dann ist die Telearbeitsvereinbarung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist zu kündigen.

Ist die Kündigung erfolgt, sind die Beschäftigten verpflichtet, ihre Tätigkeiten wieder in Präsenz zu erbringen. Die Führungskraft hat dazu die Bedingungen herzustellen, die die erneute Präsenztätigkeit ermöglichen.

Bei Beschäftigten mit Schwerbehinderung oder diesen gleichgestellten Beschäftigten, ist die Schwerbehindertenvertretung vor der Kündigung der Telearbeitsvereinbarung durch die Führungskraft einzubinden.

Im Fall der Kündigung der Telearbeitsvereinbarung durch die Führungskraft weist die Führungskraft die bzw. den Beschäftigten auf die Möglichkeit hin, den Personalrat einzubinden. Die Einbindung erfolgt dann durch die

Beschäftigten selbst. Sofern der Personalrat beteiligt wird, wird die Kündigung erst mit Abschluss des Beteiligungsverfahrens wirksam.

**11. Verantwortung der Führungskräfte**

Die Führungskräfte tragen für ihre jeweiligen Bereiche die Verantwortung und haben die Eignung der Beschäftigten und ihrer Arbeitsaufgaben für eine mögliche Telearbeit zu bewerten. Sie stellen im Verlauf der Telearbeit regelmäßig anhand der Arbeitsergebnisse und der Feedbacks fest, ob die gleiche Arbeitsleistung wie in Präsenz erbracht wird. Zudem, ob die dienstlichen Voraussetzungen für Telearbeit weiterhin gegeben sind oder nachzusteuern ist, auch ob die Eignung der jeweiligen Beschäftigten und deren Arbeitsaufgaben für Telearbeit fortgesetzt gegeben ist. Können eventuelle Schwierigkeiten auch durch Gespräche nicht gelöst werden, so umfasst die Steuerungspflicht Maßnahmen bis hin zur Rückführung des jeweiligen Arbeitsverhältnisses in ein zukünftiges Arbeiten vermehrt oder ausschließlich in Präsenz.

Den Führungskräften obliegt die Organisation und die Führung der Mitarbeitergespräche. Für die Erfassung der Arbeitszeit gelten die einschlägigen Regelungen der jeweiligen Einrichtung der Universität.

**12. Arbeitsmittel**

Den Telearbeitsplatz statten die Beschäftigten mit arbeitsschutzkonformen Einrichtungsgegenständen wie Möbeln und Beleuchtungskörpern selbst aus. Sie sorgen dabei für eine angepasste Trennung von beruflicher und privater Sphäre für die Tätigkeit in Telearbeit. Die IT-Mittel und -Gerätschaften, die zur Erfüllung der dienstlichen Tätigkeiten am Telearbeitsplatz benötigt werden, stellt wiederum die Einrichtung der bzw. des Beschäftigten. Private Geräte dürfen nach der Übergangsfrist ab dem 01.01.2023 nicht mehr verwendet werden. Ausgenommen sind die Internetverbindung, der Router bzw. die Firewall sowie die Telefonie-Geräte. Dafür sind zu gewährleisten:

a) Stabile Internetverbindung, die ein problemloses Arbeiten einschließlich Teilnahme an Videokonferenzen gewährleistet
b) Kabelgebundene und/oder kabellose Netzwerkverbindung einschließlich eines Routers mit aktuellem Softwarestand und aktivierter Firewall
c) Telefonverbindung über Festnetz oder Mobilfunk, um die Erreichbarkeit während vereinbarter Erreichbarkeitszeiten zu gewährleisten

Die Installation der für die Telearbeit erforderlichen Software und die im Zusammenhang mit der Telearbeit benötigte Gerätebetreuung wird durch die IT-Beauftragten der eigenen Einrichtung oder durch qualifizierte Personen sichergestellt, die von diesen beauftragt wurden. Das gesamte Vorgehen zu Transport und Installation ist den Beschäftigten von eben genannten Beauftragten zu erläutern. Für Einrichtungen, deren IT durch das Universitätsrechenzentrum betreut wird, obliegt diese Verpflichtung dem Universitätsrechenzentrum.

Es sind grundsätzlich die individuellen Vorgehensweisen in der jeweiligen Einrichtung zu berücksichtigen. Bei Unklarheiten ist eine Verbindung mit den IT-Beauftragten der jeweiligen Einrichtung aufzunehmen.

**13. Verlängerung der Telearbeitsvereinbarung**

Die Telearbeitsvereinbarungen gelten in beiden Formen längstens für ein Jahr. Sofern die Voraussetzungen weiterhin gegeben sind, kann die Telearbeitsvereinbarung jeweils um ein weiteres Jahr verlängert werden. Hierfür wird mit entsprechendem Vorlauf erneut ein Mitarbeiterinnen- bzw. Mitarbeitergespräch geführt. Sollte seitens der Beschäftigten kein Interesse an der Verlängerung der Telearbeit bestehen, so läuft sie mit Ablauf der vereinbarten Laufzeit aus, die Arbeitsleistung ist anschließend vollumfänglich wieder in Präsenz zu erbringen.

Für eine Verlängerung ist zu prüfen und durch die Beschäftigten erneut zu bestätigen, ob die erforderlichen Voraussetzungen zur erfolgreichen Durchführung von Telearbeit gemäß § 4 der Dienstvereinbarung weiterhin vorliegen. Auch nachträgliche Änderungen der individuellen regelmäßigen Arbeitszeit sind zu berücksichtigen.

# ANLAGE
# HANDREICHUNG DATENSCHUTZ UND IT-SICHERHEIT I.R.D. TELEARBEIT

Für Ihre Tätigkeit in Telearbeit gelten grundsätzlich die gleichen Datenschutz- und IT-Sicherheitsanforderungen wie an Ihrem Arbeitsplatz in der Universität. Um sicherzustellen, dass durch die Telearbeit kein höheres / erhöhtes Risiko für den Schutz personenbezogener Daten sowie für die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen entsteht, sind die nachfolgenden Maßnahmen zu beachten.

**1. Telearbeitsplatz**

Achten Sie bei der Einrichtung und Nutzung Ihres Telearbeitsplatzes auf die folgenden datenschutz- und IT-sicherheitsbezogenen Aspekte:

- Am besten geeignet ist ein Arbeitsplatz in einem eigenen Raum oder in einem gesonderten Bereich in Ihrer Wohnung. Wählen Sie diesen so, dass andere den Bildschirm nicht einsehen können, auch nicht durch ein Fenster. Sofern keine entsprechende Platzierung des Bildschirms erfolgen kann, ist auf diesem eine Sichtschutzfolie anzubringen.
- Finden Sie einen geeigneten Platz, um Papierdokumente so aufzubewahren, dass diese nicht von unbefugten Dritten, einschließlich Familienangehörigen, sonstigen Mitbewohner*innen oder Besucher*innen, eingesehen oder zugegriffen werden können.
- Schließen Sie beim Verlassen des Arbeitsplatzes die Türen und – vor allem im Erdgeschoss – die Fenster, um eine unbefugte Kenntnisnahme, einen Verlust oder eine Veränderung von Daten zu verhindern.

**2. Dienstliche Daten, Informationen und Unterlagen**

Ihr Umgang mit dienstlichen Daten, Informationen und Unterlagen sowie die richtige Organisation Ihres Telearbeitsplatzes trägt wesentlich zum Schutz dieser bei. Beachten Sie hierzu die folgenden Maßnahmen:

- Dienstliche Daten dürfen nicht an Dritte weitergegeben oder für andere als dienstliche Zwecke verwendet werden.
- Organisieren Sie Ihren Arbeitsplatz so, dass sich private und dienstliche Daten nicht mischen.
- Dienstliche Daten dürfen nicht auf privaten Geräten oder universitätsfremden Clouddiensten, sondern ausschließlich auf den von der Universität zugelassenen Geräten und/oder IT-Systemen oder Verbünden, wie den universitären Dateiservern oder der heiBOX, gespeichert oder verarbeitet werden. Im Rahmen von Forschungsprojekten sind, für das jeweilige Forschungsprojekt, die von einer dritten Forschungseinrichtung bereitgestellten Datenspeicher ebenso zulässig.
- Speichern Sie Dokumente, an denen Sie arbeiten, sowie Ihre Arbeitsergebnisse regelmäßig auf Datenträgern bzw. Servern im Netz der Universität, da dadurch die Datensicherung (Backup) gewährleistet wird.
- Dienstliche Daten oder Informationen dürfen Sie nur verschlüsselt übermitteln. Bei E-Mails genügt in der Regel die bei einer Nutzung von universitären E-Mail-Adressen standardmäßig gegebene Transportverschlüsselung. Eine Inhaltsverschlüsselung, wie bei E-Mails mittels S/MIME oder vergleichbarem Standard, ist ausschließlich bei einem erhöhten Schutzbedarf der Daten erforderlich. Das für einen inhaltsverschlüsselten E-Mail-Versand erforderliche Zertifikat können Sie beim URZ beantragen. https://www.urz.uni-heidelberg.de/de/service-katalog/it-sicherheit/smime-zertifikate-fuer-e-mail-kommunikation
  Bei Fragen bezüglich der Kategorisierung der Schutzbedürftigkeit von Daten ist der Vorgesetzte einzubeziehen.

**3. Papierunterlagen, Akten und Datenträger**

Beim Wechsel in Telearbeit ist es oftmals erforderlich, Dokumente und IT-Geräte vom Arbeitsplatz mit nach Hause zu nehmen. Dies dürfen Sie allerdings nur dann tun, wenn es zwingend erforderlich ist.

Sofern keine Mehrfertigung von Unterlagen vorhanden oder Mehrfertigungen nicht mit vergleichsweise geringem Aufwand wiederbeschaffbar sind, dürfen Sie in der Telearbeit nur mit Kopien und nicht mit Originaldokumenten, -akten und -datenträgern arbeiten.

Hinsichtlich Papierunterlagen, Akten und Datenträgern sind die folgenden Punkte zu beachten:

**Transport:** Papierdokumente transportieren Sie in einem verschließbaren Behältnis. Die Festplatte bzw. SSD Ihres Laptops sowie ggf. alle weiteren externen Speichermedien müssen verschlüsselt sein. Die Verschlüsselungstechnologie muss so gewählt werden, dass der Datenzugriff durch den alleinigen Besitz des Geräts bzw. Speichermediums nicht möglich ist.
Während des Transports ist es erforderlich, dass Dokumente und IT-Geräte immer unter Beaufsichtigung stehen. Achten Sie darauf, Papierunterlagen, Akten und Datenträgern keinen erhöhten Risiken, wie z.B. durch die Mitnahme bei Einkäufen, auszusetzen.

**Ablage/Aufbewahrung:** Papierunterlagen, Akten und Datenträger dürfen nicht offen und freizugänglich herumliegen. Sie müssen verschlossen in einem geeigneten Behältnis (z.B. Aktenschrank, Rollcontainer) aufbewahrt werden, sobald diese nicht mehr für den jeweils in Telearbeit ausgeführten Arbeitsvorgang erforderlich sind oder die tägliche Telearbeitszeit beendet ist.

**Entsorgung:** Werfen Sie dienstliche Papierdokumente keinesfalls in Ihren privaten Papiermüll. Sammeln Sie Ihren dienstlichen Papiermüll, lagern Sie diesen verschlossen und entsorgen Sie diesen, wenn Sie wieder ins Dienstgebäude gehen, dort in den von der Universität bereitgestellten und dafür vorgesehenen Datenschutzcontainern.

**Umgang mit Benutzerkennungen, Passwörtern u.ä.:** Benutzerkennungen, Passwörter oder sonstige Zugangssicherungsmaßnahmen zu dienstlichen IT-Systemen oder IT-Verbünden sind so aufzubewahren, dass sich niemand Zugang dazu verschaffen kann. Insbesondere dürfen keine Notizzettel unter der Tastatur oder am Bildschirm kleben und die Zugangsinformationen auch niemandem mitgeteilt werden. Bei der Wahl von Passwörtern ist die Passwortrichtlinie des URZ zu beachten.
https://www.urz.uni-heidelberg.de/de/service-katalog/identity-management/passwort-policy

### 4. IT-Mittel, Gerätschaften und Systeme

**Keine Nutzung durch Unbefugte:** Die von der Universität für die Telearbeit zur Verfügung gestellten IT-Mittel und Gerätschaften dürfen nicht durch Unbefugte, einschließlich Familienangehörigen, sonstigen Mitbewohnerinnen/Mitbewohnern oder Besucherinnen/Besuchern des Telearbeitsplatzes, benutzt werden.

**Anschluss privater Geräte:** Um auszuschließen, dass Schadsoftwares Ihren Computer befallen und Ihre Daten kompromittieren, dürfen Sie an einen dienstlichen Computer grundsätzlich keine privaten Speichermedien (z.B. externe Festplatten oder USB-Sticks) anschließen. Falls der Computer dennoch infiziert wurde, müssen Sie dies schnellstmöglich an Ihren IT-Beauftragten sowie die Servicegruppe IT-Sicherheit des URZ melden.

**Zugang:** Der Zugang zu IT-Systemen erfolgt immer über eine Benutzerkennung und ein Passwort, das der Passwortrichtrichtlinie des URZ entspricht. Eine PIN ist insbesondere nur bei dienstlichen Smartphones und Tablets zulässig, jedoch sind auch auf diesen Geräten komplexere Passwörter zu bevorzugen.

**Bildschirmsperre:** Schützen Sie Ihren Bildschirm durch einen automatischen Bildschirmschoner mit Kennworteingabe und sperren Sie den Bildschirm bei jedem Verlassen Ihres Telearbeitsplatzes, damit niemand unberechtigt auf Ihre dienstlichen Daten zugreifen kann.

### 5. Nutzung von Druckern und Scannern

Die Nutzung von Druckern und Scannern ist am Telearbeitsplatz nur dann zulässig, wenn dringende dienstliche Gründe dies erfordern und der Ausdruck bzw. Scan nicht am nächsten Präsenztag durchgeführt werden kann, weil dies den Erfolg des Arbeitsvorgangs beeinträchtigen würde. Drucker bzw. Scanner müssen kabelgebunden oder kabellos, jedoch mindestens mit WPA2 und einem mindestens 16-stelligen Passwort verschlüsselt, angebunden sein.

Sofern Sie am Telearbeitsplatz drucken müssen, beachten Sie die folgenden Punkte:

**Drucken am Telearbeitsplatz:** Entnehmen Sie am Telearbeitsplatz ausgedruckte Dokumente unverzüglich aus dem Drucker, damit andere Personen im Haushalt keine Kenntnis von diesen Daten nehmen können.

**Drucken bei Nutzung des VPN:** Achten Sie darauf, dass Sie, wenn Sie z.B. über VPN im Netz der Universität arbeiten, keine Druckaufträge auf Drucker in Dienstgebäuden abschicken, soweit der Druck der Aufträge nicht durch eine berechtigte Person überwacht und der Druck damit unmittelbar entgegengenommen werden kann, da sonst unberechtigte Personen Einblick in diese Dokumente nehmen könnten.

**Drucken sensibler Daten:** Wenn Sie mit vertraulichen oder sensiblen Daten arbeiten, die personenbezogene Daten beinhalten, dürfen diese nicht am Telearbeitsplatz ausgedruckt werden.

### 6. Telefonate

Wenn Sie am Telearbeitsplatz dienstlich telefonieren, achten Sie insbesondere auf folgendes:

— Suchen Sie einen ungestörten Bereich auf, damit andere Personen im Haushalt keine Kenntnis von Ihrem Telefonat nehmen können. Balkone, Terrassen oder Gärten sind dafür regelmäßig ungeeignet.
— Denken Sie bei Telefonaten auch daran, geöffnete Fenster zu schließen und ggf. im Hintergrund laufende Videokonferenzen bzw. Telefonate zu beenden.

### 7. Videokonferenzen

Bitte verwenden Sie für Videokonferenzen ausschließlich die vom URZ für den jeweiligen Einsatzzweck empfohlenen Videokonferenzsysteme. Schützen Sie den Zugang zu Videokonferenzräumen über Passwörter oder individuelle Einladungslinks. Ansonsten gelten für Videokonferenzen dieselben Erfordernisse wie für Telefonate (s.o.).

### 8. E-Mails

Wenn Sie dienstliche E-Mails versenden oder empfangen, dann benutzen Sie dafür bitte ausschließlich Ihre dienstlichen E-Mail-Adressen bzw. die dienstlich bereitgestellten E-Mail-Systeme oder Postfächer. Leiten Sie ihre dienstlichen E-Mails keinesfalls an eine private E-Mail-Adresse weiter.
Sollten Sie E-Mails versenden, die besonders sensible personenbezogene Daten enthalten, insbesondere Daten gemäß Art. 9 Abs. 1 DS-GVO, wie z.B. Gesundheitsdaten, dürfen Sie diese ausschließlich inhaltsverschlüsselt mittels S/MIME oder vergleichbarem Standard versenden.

### 9. Messenger

Sofern Sie dienstlich auf Messengerdienste zurückgreifen, nutzen Sie nur Messengerdienste, die auf universitätseigenen Servern gehostet werden, wie heiCHAT. Alle anderen Messengerdienste, die nicht von der Universität gehostet oder bereitgestellt werden, wie z.B. WhatsApp, Facebook, Threema oder Telegram, dürfen nicht verwendet werden.

### 10. Digitale sprachgesteuerte Assistenten und Smart-Home-Geräte

Ebenfalls nicht erlaubt ist der Einsatz digitaler sprachgesteuerter Assistenten, wie Google Assistent, Amazon Echo, Siri, Alexa, Cortana, Bixby, und HiVoice. In akustischer Reichweite Ihres Telearbeitsplatzes dürfen sich keine privaten Geräte oder IT-Systeme befinden, die entsprechende Dienste in Betrieb sind. Dasselbe gilt für sprachgesteuerte Smart-Home-Geräte. Bitte beachten Sie dabei, dass diese Dienste grundsätzlich dauerhaft mithören, um die Aktivierungswörter für den jeweiligen Dienst („Hey Siri“, „Ok, Google“, etc.) zu erkennen. Daher sind alle privaten Geräte mit entsprechend aktivierten Diensten außer Hörreichweite des Telearbeitsplatzes aufzubewahren.

### 11. Sicherheitsmaßnahmen und technische Veränderungen

Es ist unzulässig, die Sicherheitsmaßnahmen zu umgehen bzw. zu deaktivieren oder die zur Verfügung gestellten Geräte ohne Genehmigung technisch zu verändern.

**12. Internetzugang**

Wenn Sie Ihren privaten Internet-Anschluss verwenden:

— Richten Sie Ihren Computer so ein, dass er mit Ihrem privaten Netzwerk durch ein Kabel oder ein verschlüsseltes WLAN (mind. WPA2, 16-stelliges Passwort) verbunden ist.
— Für den für die Telearbeit erforderlichen Internetzugang benötigen Sie einen Router mit Firewallfunktion / Paketfilter und/oder eine gesonderte Firewall, die regelmäßig aktualisiert wird. Die vom Internetserviceprovider bereitgestellten Geräte sind, solange diese noch Updates vom Hersteller erhalten, in der Regel ausreichend.

**13. Verbindung zum Universitätsnetzwerk**

Wählen Sie sich in das Netzwerk der Universität über eine sichere Verbindung mit Hilfe einer von der Universität bereitgestellten VPN-Verbindung ein und übertragen Sie nur über diese Verbindung Daten an die Universität.
https://www.urz.uni-heidelberg.de/de/service-katalog/netzwerk/vpn-virtual-private-network

**14. Maßnahmen gegen Daten- oder Passwortdiebstahl**

Ergreifen Sie Maßnahmen, um sich vor Passwortdiebstahl zu schützen, indem Sie

— die Adressleiste im Browser überprüfen,
— Hyperlinks aus zweifelhaften Nachrichten und Dokumenten heraus nicht öffnen,
— keine Anhänge von verdächtigten E-Mails öffnen,
— bei der Eingabe von Zugangsdaten wachsam sind,
— jede Online-Session durch ein reguläres Log-Out und nicht nur durch Schließen des Browserfensters beenden.

**15. Beratung zum Datenschutz und zur Informationssicherheit**

Wenn Sie Beratung zum Datenschutz bzw. zur Informationssicherheit benötigen, können Sie sich unter datenschutz@uni-heidelberg.de an die/den behördlichen Datenschutzbeauftragten und unter it-sicherheit@urz.uni-heidelberg.de an die Servicegruppe IT-Sicherheit am URZ wenden.