



Anlage 1 der Dienstvereinbarung zur Telearbeit am heimischen Arbeitsplatz
Stand: 11.07.2016

Bitte senden Sie Ihren Antrag an die
Universität Hohenheim
Personalabteilung (APO)

Antrag auf Einrichtung oder Verlängerung eines Heimarbeitplatzes

Die Universität Hohenheim bietet ihren Beschäftigten zur individuellen Flexibilisierung des Beschäftigungsverhältnisses die Möglichkeit dienstliche oder arbeitsvertragliche Tätigkeit am heimischen Arbeitsplatz („Telearbeit“) zu erbringen. Den Rahmen hierfür hat sie gemeinsam mit dem Personalrat in der Dienstvereinbarung zur Telearbeit am heimischen Arbeitsplatz festgelegt.

Die Vereinbarung von Telearbeit kann ausschließlich in einer schriftlichen Vereinbarung zwischen dem Beschäftigten und der Universität erfolgen. Zur Prüfung der Voraussetzungen für die Vereinbarung von Telearbeit ist ein Antrag mit den nachfolgend anzugebenden Informationen erforderlich. Um festzustellen, ob Ihre Tätigkeit für Telearbeit geeignet ist, ist die Stellungnahme Ihres Vorgesetzten auf Ihrem Antrag erforderlich. Zu den weiteren Voraussetzungen der Vereinbarung von Telearbeit gehört Ihre Bestätigung, dass Ihr Heimarbeitsplatz geeignet ist und dass Sie die in der Anlage 2 zur Dienstvereinbarung vorgeschriebenen Maßnahmen umsetzen werden. Im Rahmen ihrer Aufgaben erhalten der Personalrat, die Beauftragte für Chancengleichheit bzw. die Gleichstellungsbeauftragte sowie ggf. die Schwerbehindertenvertretung die Gelegenheit zur Stellungnahme.

Die Universität verarbeitet die mit diesem Formular erhobenen personenbezogenen Daten auf Grundlage von § 36 Abs. 1 Landesdatenschutzgesetz sowie der Dienstvereinbarung zur Telearbeit am heimischen Arbeitsplatz. Sie haben das Recht, bei der Universität Hohenheim Auskunft über die zu Ihrer Person gespeicherten Daten zu verlangen und diese Daten bei Fehlern berichtigen zu lassen. Bitte wenden Sie sich in diesen Fällen an die Universität Hohenheim, Abteilung Personal und Organisation, Schloss Hohenheim 1, 70599 Stuttgart.

Persönliche Angaben:

Name: _____

Vorname: _____

Einrichtung: _____

Einrichtungsnummer: _____

Beschäftigungsumfang: _____

Ich beantrage die Einrichtung eines Heimarbeitsplatzes im Umfang von _____ Stunden pro Woche (Telearbeit soll höchstens 50 % Ihres individuellen Beschäftigungsumfangs betragen) im Zeitraum von (i.d.R. nicht länger als 12 Monate):

Beginn: _____

Ende: _____

Die Arbeitszeit am Heimarbeitsplatz soll folgendermaßen erfolgen:

Ich bestätige, dass der Heimarbeitsplatz für die Erbringung von Telearbeit geeignet ist und dass ich die in Anlage 2 zur Dienstvereinbarung zur Telearbeit am heimischen Arbeitsplatz festgelegten Maßnahmen vollständig umsetzen werde.

Datum, Unterschrift des Beschäftigten

Stellungnahme des Dienstvorgesetzten

Ich habe geprüft, ob die Einrichtung des Heimarbeitsplatzes dienstlichen Interessen zuwiderlaufen würde:

Mit der Einrichtung des Heimarbeitsplatzes sowie der Verteilung der Arbeitszeit am Heimarbeitsplatz bin ich einverstanden.

Mit der Einrichtung des Heimarbeitsplatzes bin ich grundsätzlich einverstanden, jedoch erhebe ich gegen den beantragten Umfang bzw. die Verteilung der Arbeitszeit am Heimarbeitsplatz folgende Einwände:

Der Einrichtung des Heimarbeitsplatzes stehen folgende dienstliche Belange entgegen:

Datum, Unterschrift des Dienstvorgesetzten

Maßnahmen des Datenschutzes und der IT-Sicherheit nach § 8 Abs. 1 der Dienstvereinbarung zur Telearbeit am heimischen Arbeitsplatz

Nach § 8 Abs. 1 der Dienstvereinbarung zur Telearbeit am heimischen Arbeitsplatz haben die Universität und der Personalrat nachfolgend die von den Beschäftigten am Heimarbeitsplatz umzusetzenden Maßnahmen des Datenschutzes und der IT-Sicherheit festgelegt.

§ 1 Regeln für den Umgang mit vertraulichen Unterlagen

- (1) Alle Informationen (elektronische Daten und Unterlagen) sind am Heimarbeitsplatz stets so aufzubewahren, dass andere Personen (einschließlich Familienangehörige, Mitbewohner, Gäste) nicht darauf zugreifen oder deren Inhalt zur Kenntnis nehmen können. Hierzu gehört beispielsweise die verschlossene Aufbewahrung der Unterlagen außerhalb der Nutzungszeit in Schubladen, Schänken usw.
- (2) Beim Transport von Unterlagen zwischen Universität und Heimarbeitsplatz muss stets sichergestellt sein, dass diese nicht abhandenkommen oder beschädigt werden. Dies kann beispielsweise durch eine ausreichend stabile und verschlossene Tasche gewährleistet werden. Durchsichtige Plastiktüten sind aber ungeeignet, weil Unbefugte den Inhalt zur Kenntnis nehmen könnten.
- (3) Dienstliche Unterlagen sind ausschließlich an der Dienststelle datenschutzgerecht zu vernichten – nicht jedoch am Heimarbeitsplatz.
- (4) Von außen erreichbare Einstiegsmöglichkeiten in die Wohnung sind beim Verlassen des Heimarbeitsplatzes zu verschließen, dies betrifft insbesondere nach außen gehende Türen und Fenster.

§ 2 Regeln für die Nutzung von IT-Geräten (Computer, Zubehör, Netzwerkgeräte, usw.)

- (1) Sensible oder personenbezogene Daten sind so weit wie möglich nicht auf dem Arbeitsplatzrechner oder mobilen Datenträgern sondern auf den Serversystemen der Universität Hohenheim zu speichern.
- (2) IT-Geräte, mobile Datenträger und Unterlagen sind gegen unbefugte Nutzung und Einsicht zu schützen. Hierzu gehört beispielsweise beim Verlassen des Arbeitsplatzes das Sperren oder Herunterfahren des PCs oder das Einschließen mobiler Datenträger und Unterlagen.
- (3) Kabellose Eingabegeräte (Funkmaus, Funktastatur, usw.) dürfen nicht verwendet werden.
- (4) Personenbezogene Daten dürfen nicht mit privaten Geräten (z.B. Drucker) verarbeitet werden.
- (5) Bei Eingaben über die Tastatur ist die unbefugte Kenntnisnahme vertraulicher Informationen, wie z.B. Passwörter, zu verhindern.
- (6) Geben Sie keine Passwörter an Dritte weiter, auch nicht an Angehörige oder Mitglieder der Universität Hohenheim. Soweit für Urlaub und Krankheit interne Regelungen gelten, sind diese zu beachten.

- (7) Änderungen an Hardware und Software der zur Verfügung gestellten IT-Einrichtungen dürfen nur mit Genehmigung des Vorgesetzten erfolgen.

§ 4 Umgang mit mobilen Datenträgern (USB-Stick, CD, DVD, usw.)

- (1) Auf mobilen Datenträgern dürfen personenbezogene Daten nur in ausreichend verschlüsselter Form gespeichert werden.
- (2) Mobile Datenträger sind sorgfältig zu behandeln und gegen unbefugte Zugriffe zu schützen.

§ 5 Regeln zur Sicherheit bei der Datenübertragung, insbesondere beim E-Mailversand

- (1) Personenbezogene Daten dürfen per E-Mail nur verschlüsselt versendet werden. Neben der E-Mailverschlüsselung mit S/MIME¹ besteht die Möglichkeit, die zu versendenden Daten in einer verschlüsselten Datei (als Anlage) der E-Mail anzuhängen. Das Passwort oder der Schlüssel der zu versendenden Datei darf nicht per E-Mail versendet werden; ein alternativer Übertragungsweg ist zwingend erforderlich, z.B. Fax, Telefon, Brief. Folgende Anwendungen können zur Verschlüsselung einzelner Dateien verwendet werden:
- a. VeraCrypt ab Version 1.17
 - b. Truecrypt Version 7.1a
 - c. Word, Excel, Powerpoint ab Version 2003, Passwortlänge mindestens 12 Zeichen aus jeweils mindestens einem Zeichen der Zeichengruppen Buchstaben, Zahlen, Sonderzeichen
- (2) Die von Ihnen genutzten IT-Geräte dürfen am Heimarbeitsplatz nur verwendet werden, wenn dabei der vom KIM bereitgestellte VPN-Dienst aktiv ist. Dies gilt insbesondere während jeder Datenverbindung.

§ 6 Regeln für den Notfall

- (1) Vorfälle, die die Vertraulichkeit oder Sicherheit zu schützender Daten beeinträchtigt haben oder gefährden könnten, sind dem Vorgesetzten unverzüglich zu melden.
- (2) Unerklärliche Veränderungen an Hard- oder Software sind dem Administrator, dem KIM oder dem IT-Sicherheitsbeauftragten unverzüglich zu melden.

Sie erreichen das KIM im Notfall wie folgt:

IT-Service-Desk
Garbenstr. 30 | Bio 1 | 1. UG
70599 Stuttgart

Telefon: +49 711/459-24444

E-Mail: kim-it@uni-hohenheim.de

¹ Ansprechpartner für Zertifikate (S/MIME) im KIM sind Herr Buchfink und Herr Bücheler.



Vordruck für Stellungnahmen zur Telearbeit am heimischen Arbeitsplatz
Stand des Vordrucks: 11.07.2016

Stellungnahme zum Antrag auf Einrichtung oder Verlängerung eines Heimarbeitsplatzes

Stellungnahme

- des Personalrats
- der Schwerbehindertenvertretung
- der Beauftragten für Chancengleichheit
- der Gleichstellungsbeauftragten

Diese Stellungnahme bezieht sich auf folgenden Antrag auf Einrichtung oder Verlängerung eines Heimarbeitsplatzes:

Name des Beschäftigten _____

Vorname des Beschäftigten: _____

Einrichtung: _____

Einrichtungsnummer: _____

Antragsdatum: _____

- Der Einrichtung des Heimarbeitsplatzes wird wie beantragt zugestimmt.
- Folgende Einwände werden erhoben:

Datum, Unterschrift



Vordruck für Stellungnahmen zur Telearbeit am heimischen Arbeitsplatz
Stand des Vordrucks: 11.07.2016

Stellungnahme zum Antrag auf Einrichtung oder Verlängerung eines Heimarbeitsplatzes

Stellungnahme

- des Personalrats
- der Schwerbehindertenvertretung
- der Beauftragten für Chancengleichheit
- der Gleichstellungsbeauftragten

Diese Stellungnahme bezieht sich auf folgenden Antrag auf Einrichtung oder Verlängerung eines Heimarbeitsplatzes:

Name des Beschäftigten _____

Vorname des Beschäftigten: _____

Einrichtung: _____

Einrichtungsnummer: _____

Antragsdatum: _____

- Der Einrichtung des Heimarbeitsplatzes wird wie beantragt zugestimmt.
- Folgende Einwände werden erhoben:

Datum, Unterschrift



Vordruck zur technischen Realisierung eines Heimarbeitsplatzes
Stand des Vordrucks: 11.07.2016

Vordruck zur technischen Realisierung eines Heimarbeitsplatzes

Nach § 9 der Dienstvereinbarung zur Telearbeit am heimischen Arbeitsplatz ist für die Einrichtung des Heimarbeitsplatzes und die Bereitstellung der zum Einsatz kommenden IT-Geräte und Datenträger die Einrichtung des Beschäftigten zuständig; im Falle der zentral gemanagten PC-Arbeitsplätze ist es das Kommunikations-, Informations- und Medienzentrum.

Abhängig von der Art der Telearbeit sind technische und organisatorische Maßnahmen umzusetzen, um eine Einhaltung der Vorschriften des Landesdatenschutzgesetzes sicherzustellen. Die Festlegung dieser Maßnahmen erfolgt durch die jeweilige Einrichtung in Abstimmung mit dem IT-Sicherheitsbeauftragten und dem Projektmanager Datenschutz.

Die im Folgenden beschriebenen Maßnahmen beziehen sich auf folgenden Heimarbeitsplatz:

Name des Beschäftigten _____
Vorname des Beschäftigten: _____
Einrichtung: _____
Einrichtungsnummer: _____

Ansprechpartner für die Sicherheit der am Heimarbeitsplatz eingesetzten IT-Systeme ist:

Name _____
Vorname: _____
Einrichtung: _____
Einrichtungsnummer: _____
Telefon: _____
E-Mail: _____

Am Heimarbeitsplatz werden folgende IT-Systeme der Universität eingesetzt (Beschreibung der Hard- und Software):

... [bitte ausführlich darstellen]

Die sichere Einbindung der eingesetzten IT-Systeme in den IT-Verbund der Universität wird durch folgende Maßnahmen gewährleistet:

... [bitte ausführlich darstellen]

Datum, Unterschrift

Stellungnahme des IT-Sicherheitsbeauftragten:

- Den beschriebenen Maßnahmen wird wie dargestellt zugestimmt.
- Folgende Einwände werden erhoben:

Datum, Unterschrift

Stellungnahme des Projektmanagers Datenschutz:

- Den beschriebenen Maßnahmen wird wie dargestellt zugestimmt.
- Folgende Einwände werden erhoben:

Datum, Unterschrift