Anlage 2

Konzept zum mobilen Arbeiten und zum Einsatz privater Hard- und Software

- Datenschutz- und Informationssicherheitsaspekte beim mobilen Arbeiten -

Inhaltsverzeichnis

1 Einleitung 1
2 Grundsätze 2
2.1 Datenschutz- und Informationssicherheitsziele 2
2.2 Datenkategorien 3
2.3 Datenspeicherung 3
3 Varianten von mobilem Arbeiten und technische Umsetzung 3
3.1 Arbeitsumgebung und Schutz für unberechtigten Einblicken 4
3.2 Sicher konfigurierte Geräte 4
3.3 Sicherung von Geräten und Daten 5
3.4 Gesicherte Netzanbindungen 6
3.5 Kommunikation beim mobilen Arbeiten 6
3.6 Datenspeicherung und Datenverarbeitung 8
3.7 Verwendung schriftlicher Unterlagen und Drucken 10
3.8 E-Mail auf privaten Geräten 10
4 Risikoanalyse und Entscheidung über mögliche Formen mobilen Arbeitens 10
5 Hinweise zum Einsatz privater Hard- und Software 11
5.1 Sichere Konfiguration und sichere Nutzung 11
5.2 Aufbewahrung und Zugriffe 13
6 Verarbeitung personenbezogener Daten 13
6.1 Elektronisch gespeicherte Daten 13
6.2 Papierakten 14
7 Quellenangaben 14

1 Einleitung

Die Georg-August-Universität Göttingen und die Universitätsmedizin Göttingen[1] wollen Universitätsangehörigen das mobile Arbeiten, dass während der Corona-Pandemie vermehrt genutzt wurde, auch nach Ende der Pandemie ermöglichen, soweit dies im Rahmen der Arbeitsorganisation und Aufgabenerfüllung möglich ist. Dieses Konzept geht davon aus, dass Bedingungen für einen gewollten Einsatz von mobilem Arbeiten beschrieben werden. Dadurch ergeben sich andere Aspekte als in Konzepten bei Ausbruch der Corona-Pandemie, die durch Notmaßnahmen durch Home-Office-Zwang während der Pandemie geprägt waren.

Dieses Konzept gibt Rahmenbedingungen für mobiles Arbeiten aus Sicht des Datenschutzes und der Informationssicherheit vor. Um ein angemessenes Datenschutz- und Informationssicherheitsniveau gewährleisten zu können, werden in diesem Konzept

[1] Im Folgenden wird die Bezeichnung Stiftungsuniversität verwendet, wenn Universität und Universitätsmedizin gemeinsam gemeint sind.

verschiedene Maßnahmen dargestellt und bezüglich dem mit diesen Maßnahmen erreichten Sicherheitsniveau bewertet. Unter welchen Bedingungen ein mobiles Arbeiten abhängig von Aufgaben und Arbeitsbedingungen und unter Abwägung von Chancen und Risiken mit Blick auf Datenschutz und Informationssicherheit genehmigt wird, sollte individuell risikoabhängig bewertet werden. Grundsätze dazu erläutert Kapitel 5.

Da mobiles Arbeiten zum Teil auch unter Einsatz privater Rechner erfolgt, legt dieses Konzept auch Rahmenbedingungen für den Einsatz privater Hard- und Software aus Sicht des Datenschutzes und der Informationssicherheit vor. Der Einsatz von privaten Rechnern wird häufig auch mit dem Begriff „Bring Your Own Device“ (BYOD) verbunden. Insofern stellt dieses Dokument auch ein BYOD-Konzept dar. Dabei ist aber nicht daran gedacht, dass Angehörigen oder Mitgliedern der Stiftungsuniversität private Geräte finanziert oder bezuschusst werden, wie dies in Zusammenhang mit BYOD in der Literatur auch diskutiert wird. Die nachstehenden Regelungen geben einen Rahmen vor, der auch auf den Einsatz privater Hard- und Software in Räumen und auf dem Gelände der Stiftungsuniversität anzuwenden ist.

Die Informationssicherheitsrichtlinie der Stiftungsuniversität [1] gibt in verschiedenen Maßnahmen (z.B. A. 16 Datenspeicherung und A.18 Nutzung privater Hard- und Software) Regeln vor, von denen nur im Rahmen von spezifischen Informationssicherheitskonzepten abgewichen werden darf. Dieses Konzept legt einen Rahmen fest, auf dessen Basis zuständige Leitungen über solche Abweichungen entscheiden können. Genehmigungen können sich auf dieses Konzept beziehen, wobei auf Basis von Schutzbedarfsfeststellung und Risikobewertung aus den hier dargestellten Möglichkeiten die geeigneten ausgewählt und vorgegeben werden können.

Weitere technische Anleitungen zum mobilen Arbeiten stellen die IT-Dienstleister zur Verfügung (z.B. Anleitung der GWDG zum mobilen Arbeiten [2]).

Auch im mobilen Arbeiten sind die für den IT-Einsatz geltenden Regelungen, insbesondere die Informationssicherheitsrichtlinie der Stiftungsuniversität [1], die für die eingesetzten Nutzungskonten geltenden Nutzungsordnungen wie auch Regelungen für einzelne IT-Systeme im vollen Umfang einzuhalten.

2 Grundsätze

2.1 Datenschutz- und Informationssicherheitsziele

Ziel des Datenschutzes ist primär der Schutz von Persönlichkeitsrechten beim Umgang mit personenbezogenen Daten. Neben der Aufrechterhaltung der Vertraulichkeit solcher Daten, müssen auch Transparenz für Betroffene durch Information über die Verarbeitung sowie Berichtigungs-, Sperr- und Löschrechte umgesetzt werden. Hier ergeben sich Probleme bei der Datenverarbeitung in einer Umgebung außerhalb der Diensträume sowie auf privaten Rechnern oder in der Public Cloud.

Die Informationssicherheit will Vertraulichkeit, Integrität und Verfügbarkeit von Informationen (Daten) und informationsverarbeitenden Systemen gewährleisten. Auch hier er-

geben sich Probleme für die Gewährleistung der Erreichung dieser Ziele, sobald Informationen auf Systemen oder in Umgebungen verarbeitet werden, auf die die Stiftungsuniversität keinen oder nur eingeschränkten Einfluss hat.

2.2 Datenkategorien

Im Folgenden wird auf verschiedene Arten von Daten (oder Informationen) Bezug genommen. Die verwendeten Begriffe werden nachstehend erläutert:

- Dienstliche Daten sind jegliche Daten, die im Rahmen von Dienstgeschäften anfallen.
- Personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person … beziehen“ (z. B. Studierendendaten, Personaldaten, Patientendaten).
- Schützenswerte Daten werden als Begrifflichkeit in der Informationssicherheitsrichtlinie der Stiftungsuniversität definiert als
    - personenbezogene Daten,
    - Unternehmensdaten (z.B. Finanzdaten, vertrauliche interne Informationen/Protokolle),
    - Patente sowie
    - im Einzelfall weitere Daten, die von einer IT-Anwenderin oder einem IT-Anwender als schützenswerte Daten eingestuft wurden (z.B. Forschungsergebnisse).

2.3 Datenspeicherung

Dienstliche Daten sollten, um die oben genannten Ziele gemäß Abschnitt 2.1 zu erreichen, nach Möglichkeit auf zentralen Speichersystemen der Stiftungsuniversität gespeichert werden. Schützenswerte Daten müssen besonders gesichert und auf zentralen Systemen der Stiftungsuniversität gespeichert werden. Die Informationssicherheitsrichtlinie der Stiftungsuniversität gibt dies daher auch grundsätzlich vor und erlaubt Ausnahmen im Rahmen von spezifischen Informationssicherheitskonzepten unter Berücksichtigung von Schutzbedarf und Risiken einer Abweichung. Solche Konzepte sind von der zuständigen Leitung gemäß Informationssicherheitsrichtlinie zu beschließen und dem ISB zur Stellungnahme vorzulegen.

3 Varianten von mobilem Arbeiten und technische Umsetzung

Mobiles Arbeiten findet in Bezug auf Ort und Ausstattung unter unterschiedlichen Umständen statt. Bezüglich des Ortes wird im Weiteren unterschieden zwischen Arbeiten in häuslicher Umgebung (Home-Office) und Arbeiten in variabler Umgebung (z.B. auf Dienstreisen), bezüglich der Ausstattung zwischen dem mobilen Arbeiten mit von der Stiftungsuniversität bereitgestellter Ausstattung und dem Einsatz privater Komponenten.

Ergänzend ist für das BYOD-Szenario der Einsatz privater Komponenten für dienstliche Tätigkeiten in der Stiftungsuniversität zu betrachten.

Anlage 2

Welche Varianten mobilen Arbeitens für Angehörige der Stiftungsuniversität unter welchen technischen Bedingungen ermöglicht werden sollen, muss von den Aufgaben des Angehörigen, den technischen und organisatorischen Möglichkeiten und den durch die Aufgaben bedingten Risiken für Datenschutz und Informationssicherheit abhängig gemacht werden.

Nachstehend werden Umsetzungsvarianten und Maßnahmen dargestellt und ihre Eignung im Hinblick auf Schutzbedarf und Risiken bewertet.

3.1 Arbeitsumgebung und Schutz für unberechtigten Einblicken

Datenschutz und Informationssicherheit fordern eine geeignete Arbeitsumgebung, in der verhindert wird, dass Personen unberechtigt Einblick in Daten, Informationen und Unterlagen nehmen können. Am Arbeitsplatz in der Stiftungsuniversität kann der Arbeitgeber eine geeignete Umgebung sicherstellen. Beim mobilen Arbeiten sind die mobil Arbeitenden verpflichtet, sicherzustellen, dass keine Personen unberechtigt Einblick in nicht öffentliche Daten nehmen.

Daraus ergeben sich folgende Anforderungen:

- Lassen Sie ihren Rechner nicht unbeaufsichtigt stehen, ohne den Bildschirm zu sperren.
- Richten Sie in einer häuslichen Umgebung den Arbeitsplatz so ein, dass andere Personen keinen Einblick in Bildschirm oder auf Tastatureingaben haben. Dazu sollten Sie vorzugsweise in einem allein genutzten Arbeitszimmer arbeiten.
- Wenn Sie unterwegs, z.B. auf Reisen oder in Tagungen arbeiten und andere Personen Sie umgeben, stellen Sie sicher, dass andere Personen keinen Einblick in vertrauliche Daten nehmen können.

    - Beim Arbeiten in öffentlichen Bereichen sollte ihr Rechner mit einer Bildschirmschutzfolie ausgestattet sein, so dass eine Einsichtnahme auf die Bildschirminhalte nur aus einem sehr engen Betrachtungswinkel möglich ist.
    - Beim Arbeiten in öffentlichen Bereichen sollten Sie vertrauliche Daten gar nicht oder nur in begründeten Notsituationen bearbeiten.

3.2 Sicher konfigurierte Geräte

Die beim mobilen Arbeiten genutzten Geräte, insbesondere Arbeitsplatzrechner, müssen sicher konfiguriert werden.

Vorzugsweise kommt beim mobilen Arbeiten ein dienstlich zur Verfügung gestelltes Gerät zum Einsatz, das vom zuständigen IT-Personal der Stiftungsuniversität sicher konfiguriert ist und bei dem durch die Konfiguration sichergestellt ist, dass die Sicherheit auch durch automatische Aktualisierung von Software und Sicherheitssystem (z.B. Signaturen von Virenscannern) aufrechterhalten wird.

Anlage 2

Kann kein dienstliches Gerät bereitgestellt werden und sollen deshalb private Geräte zum mobilen Arbeiten eingesetzt werden, so müssen die jeweiligen mobil arbeitenden Personen selbst eine sichere Konfiguration der privaten Geräte sicherstellen. Anforderungen hierzu sind im Abschnitt 5 aufgeführt.

3.3 Sicherung von Geräten und Daten

Beim mobilen Arbeiten besteht ein erhöhtes Risiko, dass die eingesetzten Geräte verloren gehen (z.B. durch Diebstahl) oder beschädigt werden, sodass sich erhöhte Risiken für Vertraulichkeit und Verfügbarkeit ergeben.

Beim mobilen Arbeiten eingesetzte Geräte müssen angemessen gegen Verlust geschützt werden.

- Lassen Sie unterwegs (z.B. auf Dienstreisen) die Geräte nicht unbeaufsichtigt.
- Verwahren Sie die Geräte (insbesondere in Hotelzimmern) sicher.

Besondere Probleme können sich bei Auslandsreisen ergeben:

- Informieren Sie sich über besondere Gefahren bei Auslandsreisen und verwenden Sie in Ländern, in denen die Gefahr besteht das staatliche Stellen (z.B. Geheimdienste) Zugriff auf ihre Geräte erlangen, nur gesonderte Rechner, die keine schützenswerten Daten enthalten und die nach Rückkehr komplett bereinigt werden können.

Auch in häuslicher Umgebung muss das Gerät geschützt werden:

- Verwahren Sie auch in häuslicher Umgebung dienstliche Geräte sicher, sodass auch Haushaltangehörige oder Besucher weder absichtlich noch versehentlich Geräte beschädigen oder auf diese zugreifen können.

Wenn ein Gerät verloren geht oder beschädigt wird, sind Datensicherungen wichtig:

- Stellen Sie sicher, dass von allen Daten eine Sicherung existiert oder speichern Sie alle Daten gar nicht auf dem mobilen Gerät, sondern auf den zentralen Servern der Stiftungsuniversität.

Geht ein mobiles Gerät verloren, so ist dies auch ein Datenschutz- und Informationssicherheitsvorfall, aus dem sich Meldepflichten und andere rechtliche Konsequenzen ergeben können.

- Melden Sie den Verlust von dienstlichen Geräten aber auch von privaten Geräten, auf denen sich dienstliche Daten befinden unverzüglich.

Anlage 2

3.4 Gesicherte Netzanbindungen

Beim mobilen Arbeiten wird in der Regel über das Internet auf Dienste und Computersysteme der Stiftungsuniversität zugegriffen. Zugriffe über Netzwerke sollten immer (also auch innerhalb des Universitätsnetzes) über verschlüsselte Kommunikationswege erfolgen, damit ein Abhören des Netzverkehrs unmöglich ist. Beim Zugriff über das Internet ist eine Verschlüsselung immer zwingend sicherzustellen. Dazu bestehen verschiedene Möglichkeiten:

- Die bevorzugte und empfohlene Möglichkeit ist der Zugriff auf das Universitätsnetz über eine VPN-Verbindung. VPN steht für Virtual Private Network. Dabei wird ein verschlüsselter Tunnel zwischen dem mobilen Gerät und dem Universitätsnetz aufgebaut, sodass alle Datenübertragungen unabhängig von der verwendeten Anwendung auf dem Weg durch das Internet sicher verschlüsselt werden und abhörsicher sind. Über einen solchen Tunnel wird auch der Zugriff auf Dienste ermöglicht, die über das Internet nicht erreichbar sind. Software für den Aufbau einer VPN-Verbindung sowie Zugangsberechtigungen mit Benutzername und Password und ggf. zusätzlich über ein Hardware-Token werden von der GWDG für die Universität und von G3-7 für die UMG bereitgestellt.
- Muss beim mobilen Arbeiten nur auf Dienste der Stiftungsuniversität zugegriffen werden, die grundsätzlich auch aus dem Internet erreichbar sind, kann auf diese auch ohne die Nutzung eines VPN-Tunnels zugegriffen werden. Solche Dienste bieten inhärent eine Verschlüsselung der Verbindung und somit eine Abhörsicherheit an.
- Auf Verschlüsselung ist insbesondere dann zu achten, wenn unterwegs in öffentlichen WLANs (Hotspots) gearbeitet wird, da in diesen der WLAN-Verkehr meist unverschlüsselt übertragen wird und in der Umgebung relativ leicht ein Abhören möglich wäre.

3.5 Kommunikation beim mobilen Arbeiten

Moderne Kommunikationsmethoden wie E-Mail, Messenger, Videokonferenzen kommen schon im Büro vermehrt zum Einsatz. Beim mobilen Arbeiten bekommen diese besondere Bedeutung. Auch beim Einsatz von Telefonie sind zusätzliche Aspekte beim mobilen Arbeiten zu berücksichtigen.

Beim Einsatz von E-Mail muss sichergestellt werden, dass auch im Home-Office nur die dienstliche E-Mail-Adresse für dienstliche Kommunikation verwendet wird:

- Leiten Sie nie dienstliche E-Mails an ihre private E-Mail-Adresse weiter.
- Beantworten Sie dienstliche Anfragen nie über ihre private E-Mail-Adresse.

Der Einsatz eines Messenger wie z.B. WhatsApp kann unter Datenschutz-Aspekten problematisch sein:

Anlage 2

- Verwenden Sie für dienstliche Kommunikation keine privaten Messenger-Konten. Dienstlich steht in der Stiftungsuniversität i.d.R. nur Rocket Chat zur Verfügung. Aber auch Rocket Chat dürfen Sie nicht für den Austausch personenbezogener Daten verwenden!

Für Videokonferenzen stellt die Stiftungsuniversität zwei Systeme zur Verfügung. Das Videokonferenzsystem BigBlueButton (BBB) wird auf dem Campus von der GWDG betrieben. Mit diesem System können Anforderungen des Datenschutzes in vollem Umfang erfüllt werden.

Für Konferenzen mit sehr vielen Teilnehmern ist BBB jedoch nicht leistungsfähig genug. Als Alternative wird daher auch die kommerzielle Lösung Zoom angeboten. Der Dienst des Anbieters Zoom wird über Server des Anbieters angeboten. Zoom unterliegt als U.S-amerikanischer Anbieter dem Recht der USA. Damit kann Zoom aktuell nicht die Anforderungen des europäischen Datenschutzrechts erfüllen.[2]

- Verwenden Sie für Videokonferenzen, soweit nicht technische Gründe wie eine sehr hohe Teilnehmerzahl (mehr als 200) dagegensprechen, BBB als Videokonferenzsystem.
- Für Videokonferenzen, in denen über personenbezogene oder andere schützenswerte Informationen gesprochen wird oder in denen solche Daten präsentiert oder ausgetauscht werden, darf die Zoom nicht eingesetzt werden[3].

In Videokonferenzsystemen ist eine Videoaufzeichnung oder die Abspeicherung von Inhalten z.B. in Chats möglich. Hier ist zu beachten:

- Beteiligte an der Kommunikation müssen informiert sein und ihre Zustimmung bekunden, wenn eine Aufzeichnung oder Speicherung von Daten vorgenommen wird.
- Wird in Videokonferenzen über personenbezogene oder andere schützenswerte Daten gesprochen oder werden solche Daten in der Konferenz präsentiert, so darf eine solche Konferenz nicht aufgezeichnet werden.

Software für Videokonferenzen oder Remote-Unterstützung erlaubt häufig auch die Freigabe von Bildschirminhalten zur Präsentation oder sogar zur Fernsteuerung.

[2] Zusätzlich betreibt die GWDG im eigenen Rechenzentrum einen Dienst mit Zoom-Software. Wird dieser Dienst entsprechend den Vorgaben der GWDG eingesetzt, so kann zumindest verhindert werden, dass Kommunikationsinhalte über Server des Anbieters Zoom laufen. Trotzdem werden sogenannte Metadaten (u.a. Informationen über Meetings und deren Dauer, Teilnehmer und deren Rechnerkonfiguration) auch in diesem Fall an den Anbieter Zoom übertragen. Auch dieser Betrieb ist damit nicht datenschutzkonform möglich, außer alle Teilnehmer willigen freiwillig in die Übertragung der Daten zu Zoom ein.

[3] Ausnahme für diese Regel: Die bei der GWDG gehostete Version von Zoom darf mit speziell für diesen Zweck dafür bereitgestellte Konten und darüber sichergestellte spezielle Konfiguration für solche Konferenzen verwendet werden.

Anlage 2

- Eine dauerhafte Freigabe ist für Arbeitsplatzrechner auch im Home-Office nicht zulässig.
- Temporäre Freigaben im Rahmen von Videokonferenzen werden akzeptiert, soweit diese für die Aufgabenerfüllung notwendig sind.
- Dabei sollten bevorzugt einzelne Anwendungsfenster statt des gesamten Desktops freigegeben werden.

Telefonie stellt im mobilen Arbeiten technische und organisatorische Herausforderungen. Die primäre technische Herausforderung ist die Erreichbarkeit unter der dienstlichen Telefonnummer. Organisatorisch ist darauf zu achten, dass nicht andere Personen dienstliche Telefongespräche mithören können.

- Verwenden Sie soweit möglich die Software-Telefonie auf einem für das mobile Arbeiten verwendeten Gerät. Die Stiftungsuniversität stellt dafür eine Software innerhalb der Telefonanlage der Stiftungsuniversität bereit (den „Jabber-Client“). Damit sind Sie über ihr mobiles Gerät unter ihrer dienstlichen Telefonnummer erreichbar und auch von Ihnen ausgehende Telefonate erfolgen mit der dienstlichen Telefonnummer.
- Ist der Einsatz des Jabber-Clients nicht möglich, kann ihre dienstliche Telefonnummer an ein Diensthandy oder an eine private Telefonnummer weitergeleitet werden. Sie sind so über ihre dienstliche Telefonnummer erreichbar. Rückrufe würden aber über die Handynummer oder die private Telefonnummer erfolgen, sodass diese – möglicherweise unerwünscht - für die Kommunikationspartner sichtbar wäre. Zudem können bei der Weiterleitung für die Stiftungsuniversität und bei der Nutzung privater Telefone für die Mobilarbeitenden zusätzliche Kosten entstehen.
- Stellen Sie sicher, dass keine weiteren Personen Telefongespräche beim mobilen Arbeiten mithören können. Ist ein Telefonieren in einer Umgebung, in der ein Mithören nicht vermieden werden kann (z.B. während Dienstreisen), unbedingt nötig, so muss bei den Gesprächen darauf geachtet werden, dass das Gespräch so geführt wird, dass potentielle Mithörer keine sensiblen Informationen erhalten können.

3.6 Datenspeicherung und Datenverarbeitung

Alle dienstlichen Daten sollten auf Systemen der Stiftungsuniversität gespeichert werden. Für mobiles Arbeiten sollten die vorhandenen technischen Möglichkeiten genutzt werden, die eine Datenhaltung auf den Systemen der Stiftungsuniversität sicherstellen.

Die Stiftungsuniversität bzw. die GWDG bietet Zugang zu Anwendungen und Daten über Terminalserver (verschiedene Dienste der Hersteller Microsoft und Citrix). Bei Nutzung dieser Dienste wird das im mobilen Arbeiten genutzte Gerät nur zur Bildschirmdarstellung und als Eingabegerät mittels Maus und Tastatur verwendet. Alle Daten und Informationen verbleiben dabei von der Bildschirmanzeige abgesehen in der Stiftungsuniversität. Alle Verarbeitungen finden durch Programme auf Rechnern in der Stiftungsuniversität statt. Bei Einsatz von Terminalservern entstehen deshalb die geringsten Risiken für Datenschutz und Informationssicherheit beim mobilen Arbeiten.

Anlage 2

- Nutzen Sie im mobilen Arbeiten nach Möglichkeit die zentral bereitgestellten Terminalserver.
- Sollen im mobilen Arbeiten schützenswerte Daten verarbeitet werden, so ist das nur über die zentralen Terminalserver zulässig.

Ein ähnlicher Zugriff wie auf Terminalserver ist technisch auch auf Büroarbeitsplätze möglich, wenn zuvor eine geeignete VPN-Verbindung zum Universitätsnetz aufgebaut wurde. Dieses Vorgehen birgt aber Nachteile und Risiken. Einerseits muss der Büroarbeitsplatz permanent eingeschaltet sein und verbraucht Strom und stellt eine (vermeidbare) Brandgefahr dar. Zudem wird der Büroarbeitsplatz durch den aktvierten Terminalserverdienst auch für Unberechtigte angreifbar.

- Ein Zugriff auf den Büroarbeitsplatz aus dem mobilen Arbeiten heraus sollte nur in begründeten Ausnahmefällen genehmigt, freigeschaltet und genutzt werden.

Alternativ kann im mobilen Arbeiten eine Datenverarbeitung lokal auf dem mobilen Arbeitsplatz (statt über Terminalserver) erfolgen, wenn nur auf Daten zugegriffen werden muss, die über gesicherte Verbindungen auch für externe Zugriffe bereitgestellt werden und dort gespeichert sind und bleiben (z.B. im SharePoint der Stiftungsuniversität oder der OwnCloud der GWDG oder auf Netzlaufwerken, wenn zuvor eine VPN-Verbindung aufgebaut wurde).

Soll mobiles Arbeiten auch ohne Netzverbindung erfolgen (z.B. auf Reisen), so ist dies nicht ohne eine Speicherung der zu bearbeitenden Daten auf dem im mobilen Arbeiten eingesetzten Gerät möglich. Trotzdem soll sichergestellt werden, dass dienstliche Daten nach Abschluss der Arbeiten auf den Systemen der Stiftungsuniversität gespeichert werden. Daher sollten die jeweiligen Daten zwischen zentralem Speicher und lokalem Rechner synchronisiert werden (z.B. mit OwnCloud oder SharePoint) statt Versionen auf dem lokalen Rechner anzulegen und zu bearbeiten, die dann nach Abschluss der Arbeiten manuell zu den Systemen der Stiftungsuniversität kopiert werden müssten. Diese Arbeitsvariante ist beim Einsatz privater Geräte für schützenswerte Daten nicht erlaubt, da deren Speicherung auf privaten Geräten nicht zulässig ist.

Die Nutzung externer Clouddienste zur Speicherung dienstlicher Daten ist grundsätzlich nicht zulässig und speziell für mobiles Arbeiten auch nicht nötig. Hierauf ist auch besonders bei der Nutzung von Office 365 von Microsoft zu achten (insbesondere, wenn Office 365 zur Nutzung der Kommunikationssoftware Teams aktiviert wird).

Beim Einsatz privater Rechner ist bei schützenswerten Daten besondere Aufmerksamkeit geboten, falls auf dem privaten Rechner zur Sicherung der eigenen Daten Cloud-Backups genutzt werden. In diesem Fall muss sichergestellt werden, dass dienstliche Daten nicht ebenfalls im externen Cloud-Backup eingeschlossen sind.

Anlage 2

3.7 Verwendung schriftlicher Unterlagen und Drucken

Schriftliche Unterlagen mit schützenswerten Daten dürfen die Stiftungsuniversität nicht verlassen und dürfen daher nicht beim mobilen Arbeiten genutzt werden, d.h. weder zu häuslichen Arbeitsplätzen oder auf Reisen mitgenommen werden.

Schriftliche Unterlagen mit schützenswerten Daten dürfen auch beim mobilen Arbeiten nicht durch Ausdrucken erzeugt werden und so außerhalb der Stiftungsuniversität gelangen. Bei entsprechenden Arbeitstätigkeiten muss daher das Drucken aus entsprechenden Anwendungen soweit möglich technisch verhindert werden. Ist ein technischer Schutz nicht möglich so ist das Verbot organisatorisch zu lösen.

3.8 E-Mail auf privaten Geräten

Die Informationssicherheitsrichtlinie der Stiftungsuniversität legt fest, dass dienstliche Daten grundsätzlich auf dienstlichen Geräten zu speichern sind. Von diesem Grundsatz kann abgewichen werden, wenn ein spezifisches Informationssicherheitskonzept dies erlaubt.

Ein häufiger Fall, in dem der Wunsch besteht, von dieser Regel abzuweichen, ist der Zugriff auf dienstliche E-Mails über private Geräte (insbesondere auch Smartphones). Soweit dies nicht lediglich über einen Webbrowser erfolgt, werden dabei E-Mail-Inhalte zum privaten Gerät synchronisiert und dort gespeichert. Für den E-Mail-Zugriff über private Geräte wird folgende Ausnahme allgemein geregelt:

Die Synchronisation von E-Mails auf privaten Geräten und die damit verbundene Datenspeicherung wird erlaubt, solange nicht zu erwarten ist, dass E-Mails besonders schutzwürdige Inhalte im Sinne von Datenschutz- oder anderen Geheimhaltungsanforderungen enthalten. Für E-Mail-Konten, bei denen aufgrund der Funktion der Kontoinhaber zu erwarten ist, dass E-Mails besonders schutzwürdige Inhalte im Sinne von Datenschutz- oder anderen Geheimhaltungsanforderungen enthalten, ist eine Synchronisation auf private Geräte nicht zulässig.

4 Risikoanalyse und Entscheidung über mögliche Formen mobilen Arbeitens

Bei einer Genehmigung mobilen Arbeitens muss im Votum der zuständigen Führungskraft auch entschieden werden, unter welchen Bedingungen mobiles Arbeiten zugelassen werden kann. Die Entscheidung muss davon abhängig gemacht werden, welche Informationen eine Person mobil bearbeiten soll und welche Rechte mit Konten der Person verbunden wären. Die Entscheidung sollte auf den folgenden Regeln basieren.

Bezüglich des Einsatzes von privaten Rechnern:

- Grundsätzlich hat der Einsatz dienstlicher Rechner Vorrang. Steht ein geeigneter dienstlicher Rechner zur Verfügung, so sollte der Einsatz eines privaten

Rechners nicht genehmigt werden. Hiervon kann nur in begründeten Fällen abgewichen werden.
- Die lokale Verarbeitung von schützenswerten Daten ist auf einem privaten Rechner nicht zu erlauben.
- Der Einsatz eines privaten Rechners zum Zugriff auf Terminalserver (oder auf Büroarbeitsplätze als Terminalserver) sollte nicht erlaubt werden, wenn darüber schützenswerte Daten verarbeitet werden. Hiervon kann nur in begründeten Fällen abgewichen werden.

Bezüglich Speicherung von Daten auf Rechnern im mobilen Arbeiten

- Die Speicherung von schützenswerten Daten ist auf privaten Rechnern nicht erlaubt.
- Dienstliche Daten sollten beim mobilen Arbeiten auf zentralen Speichersystemen verbleiben und nicht auf den mobilen Rechnern gespeichert werden (von temporären Dateien, die von Programmen automatisch erzeugt werden abgesehen).
- Ist im mobilen Arbeiten ein Arbeiten ohne Netzverbindung nötig, so sollten zu bearbeitende Daten über Synchronisation mit zentralen Speichern bereitgestellt werden, um eine Verfügbarkeit der Daten im zentralen Speicher sicherzustellen.

Bezüglich der im mobilen Arbeiten verwendeten Konten:

- Für Arbeiten mit Konten, die über erhöhte Rechte (z.B. Administrationskonten, Konten mit Zugriffsrechten auf sensible Daten oder Systeme) verfügen, müssen Dienstrechner genutzt werden. Die Nutzung von privaten Geräten ist nicht zulässig.

Bei Verstößen gegen die Genehmigungsauflagen sollte eine Kündigung der Vereinbarung zum mobilen Arbeiten geprüft werden.

5 Hinweise zum Einsatz privater Hard- und Software

5.1 Sichere Konfiguration und sichere Nutzung

Für den Einsatz privater Rechner im dienstlichen Kontext müssen die nachstehenden Anforderungen, die sonst an dienstliche Rechner gestellt werden, auch erfüllt werden. Dabei handelt es sich um ganz allgemeine Sicherheitsanforderungen, die schon im eigenen Interesse auch im privaten Umfeld umgesetzt werden sollten. Personen, die private Geräte einsetzen wollen, müssen die Einhaltung dieser Anforderungen bestätigen.

- **Halten Sie Betriebssystem und Anwendungssoftware aktuell**. Nutzen Sie die Update-Prozeduren des Betriebssystems (z.B. Windows-Update) und der Anwendungssoftware (z.B. Aktivieren der automatischen Updates in Firefox und anderen Anwendungen). Wenn eine Anwendungssoftware keine automatischen Updates anbietet, sollten Sie selbst regelmäßig nach neuen Versionen

suchen. Solche Software ist erfreulicherweise heute selten. Betriebssysteme (z.B. Windows XP oder Windows 7) oder Anwendungen dürfen nicht mehr zum Einsatz kommen, wenn dafür keine Updates mehr vom Hersteller zur Verfügung gestellt werden, denn dann werden auch sicherheitsrelevante Fehler der Software nicht mehr beseitigt. Das betrifft z.B. Windows XP oder Windows 7. Diese Betriebssysteme dürfen nicht für Homeoffice genutzt werden.

- **Installieren Sie Virenschutzprogramme und halten Sie diese aktuell.** Bei aktuellen Windows-Betriebssystemen reicht hierfür auch der im Betriebssystem enthaltene Virenschutz „Windows Defender“. Angehörige der Universität (nicht der UMG) können alternativ auch die durch die Universität lizenzierte Antiviren-Software Sophos installieren. Die Lizenzverträge erlauben ausdrücklich den Einsatz auf privaten Rechnern von Universitätsangehörigen, solange diese Rechner nicht zusätzlich auch für kommerzielle Zwecke (z.B. in Nebentätigkeiten) eingesetzt werden.
- **Arbeiten Sie nicht mit privilegierten Konten (Admin-Konten).** Admin-Rechte sollten nur zum Einsatz kommen, wenn Sie den Rechner administrieren wollen, z.B. zur Installation von Software. Nutzen Sie für normale Arbeiten ein einfaches Benutzerkonto. Leider verleiten die üblichen Prozesse beim Setup eines neuen Windows-Rechners dazu, nur ein Konto anzulegen, das dann naturgemäß ein Admin-Konto sein muss (eines wird ja mindestens benötigt). Sie müssen also selber aktiv werden, um neben dem Admin-Konto ein einfaches Benutzerkonto als Konto für die tägliche Arbeit anzulegen.
- **Sorgen Sie für Sicherheit der Daten beim Einsatz mobiler Rechner.** Notebooks und Tablets sind dafür da, an verschiedenen Orten eingesetzt also auch transportiert zu werden. Dadurch besteht ein erhöhtes Risiko, dass Rechner und damit die darauf gespeicherten Daten beschädigt werden oder verloren gehen. Schützen Sie die Daten auf ihrem Rechner durch Backups gegen einen Verlust. Schützen Sie die Daten auch gegen Einsicht durch Fremde im Fall eines versehentlichen Verlusts oder Diebstahls, indem Sie die Daten auf dem Rechner verschlüsseln. Windows-Versionen für den professionellen Einsatz (Windows Pro, Enterprise, Education) enthalten mit Bitlocker eine entsprechende Verschlüsselungssoftware. Bei den Home-Versionen fehlt diese leider. Hier kann freie Software wie VeraCrypt zum Einsatz kommen. Aber Vorsicht bei jeglichem Einsatz von Verschlüsselungsverfahren. Sichern Sie den Wiederherstellungsschlüssel! Bei einem Schlüsselverlust bleiben die Daten verschlüsselt. Ohne den Schlüssel kann niemand die Daten lesen – auch Sie nicht!
- **Befolgen Sie Sicherheitsregeln beim Surfen im Netz und bei der Nutzung von E-Mail und anderen Kommunikationsdiensten**. Klicken Sie nicht auf Links mit unklaren Zielen, insbesondere nicht auf Links zum Download und zur Installation von Software. Anhänge von E-Mails oder anderen Kommunikationsdiensten sollten Sie nur öffnen, wenn ihre Ungefährlichkeit z.B. durch Herkunft und Kontext anzunehmen ist. Wenn Sie einen Anhang nicht wirklich erwarten, fragen Sie lieber beim (angeblichen) Absender nach und vergewissern Sie sich, dass sie mit der richtigen Person kommunizieren. Beim Einsatz privater Rechner ist zu erwarten, dass dort auch private E-Mail-Konten genutzt werden. Auch über private E-Mails erhaltene Schadsoftware kann zu Problemen mit dienstlichen Daten führen. Möglicherweise sind Sie bei Verwendung eines privaten E-

Mail-Kontos auch schlechter gegen Schadsoftware geschützt als bei dem dienstlichen Konto. Ein Grund mehr, hier besonders vorsichtig zu sein.

- **Deaktivieren Sie die automatische Ausführung von Makros.** Cyberkriminelle nutzen bevorzugt Makros in Office-Dokumenten, um Schadsoftware auf Rechnern zu platzieren. Stellen Sie sicher, dass die automatische Ausführung von Makros deaktiviert ist.

5.2 Aufbewahrung und Zugriffe

Für reguläre Telearbeit gelten strenge Anforderungen an Arbeitsräume und Arbeitsmittel. Auch im mobilen Arbeiten sollten private Rechner mit schützenswerten Daten möglichst sicher aufbewahrt werden. Der Zugriff aus Sicht der Stiftungsuniversität fremder Personen auf dienstliche Daten muss verhindert werden. Fremde in diesem Sinn sind auch Haushaltsangehörige. Der private Rechner sollte ausschließlich vom Universitätsangehörigen selbst und nicht von anderen Haushaltsangehörigen genutzt werden.[4] Bei einer lokalen Verarbeitung personenbezogener Daten oder aus anderen Gründen besonders vertraulicher Daten muss der Einsatz des privaten Rechners unterbleiben.

6 Verarbeitung personenbezogener Daten

Soweit nicht einzelne Einrichtungen spezielle Regelungen erlassen haben (wie z.B. die Personalabteilung) finden die folgenden allgemeinen Regeln Anwendung.

6.1 Elektronisch gespeicherte Daten

Da die Verarbeitung personenbezogener Daten rechtmäßig und erforderlich sein muss, gelten weiterhin die Betroffenenrechte auf Transparenz (Information und Auskunft), Berichtigung, Löschung, Einschränkung der Verarbeitung und Widerspruch sowie Widerruf der Einwilligung. Die Informationspflichten gemäß Art. 13 und 14 DSGVO müssen weiterhin eingehalten werden. Muster dazu finden Sie auf der Homepage des Datenschutzbeauftragten.

[4] Sollte für mobiles Arbeiten in einer Sondersituation wie der Corona-Pandemie kein dienstlicher Rechner bereitgestellt werden können, so kann in zu begründenden Ausnahmefällen genehmigt werden, dass ein privater Rechner mit Mehrpersonennutzung zur Nutzung im mobilen Arbeiten zugelassen wird. In einem solchen Fall der Mehrpersonennutzung muss das Risiko abgewogen werden, das von einem Zugriff durch Haushaltsangehörige ausgehen könnte.
Wird entschieden, dass der Einsatz eines privaten Rechners erfolgen soll, obwohl auch andere Haushaltsangehörige diesen benutzen, so muss zumindest für die dienstliche Nutzung ein separates Benutzerkonto genutzt werden. Falls schützenswerte Daten überhaupt auf dem Rechner gespeichert werden, müssen Zugriffsrechte auf diese Daten so eingestellt werden, dass die Haushaltsangehörigen keinen Zugriff auf diese Daten haben. Ebenso müssen die Haushaltsangehörigen zum sicheren Umgang mit dem Rechner z.B. beim Surfen oder mit E-Mail und Kommunikationsdiensten angewiesen werden.

Anlage 2

Auskunft und Löschung personenbezogener Daten darf auch von Privatrechnern aus nur über den Dienstweg, d.h. über die Datenschutzmanagerin oder den Datenschutzmanager der Universität bzw. der UMG gewährt werden. Die Anweisung der Datenschutzmanagerin oder des Datenschutzmanagers ist abzuwarten.

6.2 Papierakten

Papierakten mit personenbezogenen Daten dürfen nicht mit nach Hause genommen werden, da sie dort nicht sicher verwahrt werden können. Es ist schon der Anschein zu vermeiden, dass Akten Unbefugten zur Kenntnis gelangt sein könnten!

Falls üblicherweise in Papierform vorliegende Dokumente im mobilen Arbeiten (in Form des Home-Office) benötigt werden, so sind Prozesse durch die Dienststelle zu organisieren, die solche Dokumente in digitaler Form bereitstellen. Scanprozesse zur Digitalisierung müssen dabei auf dem Campus stattfinden. Die Bereitstellung und Speicherung erfolgt auf Datenspeichern der Stiftungsuniversität.

7 Quellenangaben

[1] Georg-August-Universität Göttingen, „Richtlinie zur Informationssicherheit der Georg-August-Universität Göttingen / Georg-August-Universität Göttingen Stiftung Öffentlichen Rechts," *Amtliche Mitteilungen I der Georg-August-Universität Göttingen,* pp. 46-89, 24 Januar 2020.

[2] GWDG, „Mobiles Arbeiten," [Online]. Available: https://gwdg.de/mobile-working. [Zugriff am 20 März 2020].

[3] Georg-August-Universität Göttingen, „Informationen für Universitätsmitarbeiter*innen zum neuartigen Coronavirus (2019-nCoV)," März 2020. [Online]. Available: https://www.uni-goettingen.de/de/621808.html. [Zugriff am 18 März 2020].