GEORG-AUGUST-UNIVERSITÄT
GÖTTINGEN

Datenschutz- und Informationssicherheitsaspekte beim mobilen Arbeiten

– insbesondere bei Ausweitung in der Corona-Krise –

Inhaltsverzeichnis

1 Einleitung

Dieses Dokument macht verbindliche Vorgaben und gibt Hinweise für Teilnehmer*innen am Home-Office im Rahmen der Corona-Krise. Dieses Dokument ist vollständig zu lesen und zu befolgen.

1.1 Auswirkungen der Corona-Krise auf Datenschutz und Informationssicherheit

Die Ausbreitung des neuartigen Coronavirus zwingt dazu, neue Wege zu suchen, um die Arbeitsfähigkeit der Universität soweit wie möglich aufrechtzuerhalten. Dadurch verändern sich in der Abwägung von Chancen und Risiken mit Blick auf Datenschutz und Informationssicherheit Bewertungen für die Balance zwischen den Zielen Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationssystemen für die Dauer der Krise. In der Krise werden sonst unübliche Methoden eingesetzt.

Um überhaupt kurzfristig eine – wenn auch eingeschränkte – Arbeitsfähigkeit aufrechtzuerhalten, erfolgt in der Krise eine massive Ausweitung von mobilem Arbeiten oder Home-Office. Home-Office in Coronazeiten wird unbürokratischer umgesetzt als es die normalen Prozesse für Telearbeit vorsehen.

Aber auch in technischer Hinsicht werden Wege beschritten, die sonst nicht oder nur nach langer Prüfung gewählt werden würden. Beispielsweise wird auf die Nutzung privater Rechner im provisorischen Home-Office zurückgegriffen, weil eine ausreichende Anzahl dienstlicher Rechner dafür kurzfristig gar nicht bereitgestellt werden kann oder es wird auf externe Dienste in Public-Clouds zurückgegriffen, die sonst vermieden werden sollen, weil die eigenen Dienste durch den massiven Anstieg der Nutzung dem Ansturm nicht mehr gewachsen sind.

Nachstehend sollen Regeln und Hinweise gegeben werden, wie die Kernanforderungen des Datenschutzes und der Informationssicherheit unter diesen Bedingungen so gut wie möglich erfüllt werden können. Die Hinweise können aber auch zukünftig bei Entscheidungen innerhalb der regulären „spezifischen Informationssicherheitskonzepte“ entsprechend der Informationssicherheitsrichtlinie der Universität [1] helfen.

1.2 Datenschutz- und Informationssicherheitsziele, Datenkategorien

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 die*den Betroffene*n durch Information über die Verarbeitung sowie Berichtigungs-, Sperr- und Löschrechte umgesetzt werden. Hier ergeben sich Probleme bei der Datenverarbeitung auf privaten Rechner oder in der Public Cloud.

Die Informationssicherheit will Vertraulichkeit, Integrität und Verfügbarkeit von Informationen (Daten) und informationsverarbeitenden Systemen gewährleisten. Auch hier ergeben sich Probleme für die Gewährleistung der Erreichung dieser Ziele, sobald Informationen auf Systemen verarbeitet werden, auf die die Universität keinen Einfluss mehr hat.

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 Universität 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).

1.3 Weitere Informationen

Die Universität informiert auf ihrer Webseite mit ständigen Aktualisierungen über Maßnahmen zum Schutz vor dem Corona-Virus und über Regelungen und Empfehlungen zur aktuellen Situation [2].

Informationen zu technischen Lösungen und konkreten IT-Systemen stellt die GWDG auf ihren Webseiten bereit, insbesondere auch zum mobilen Arbeiten unter [3].

2 Datenspeicherung

Dienstliche Daten sollten, um die oben genannten Ziele (s. Abschnitt 1.2) zu erreichen, nach Möglichkeit auf zentralen Speichersystemen der Universität gespeichert werden. Schützenswerte Daten müssen besonders gesichert und auf zentralen Systemen der Universität gespeichert werden.

Daten können auch im Home-Office im SharePoint der Universität, in GWDG-Cloud-Share oder der von der GWDG betriebenen Academic-Cloud ohne zusätzliche Maßnahmen gespeichert werden. Auch persönliche Netzlaufwerke und Gruppenlaufwerke (mit Ausnahme der Zentralverwaltung) stehen wie auf dem Campus zur Verfügung, wenn zuvor eine sichere Verbindung über die VPN-Gateways der GWDG aufgebaut wurde. Wegen des zusätzlichen Aufwands der Einrichtung einer VPN-Verbindung und möglichen Engpässen bei VPN-Verbindungen in der aktuellen Situation sollte geprüft werden, ob die Speicherung in SharePoint oder GWDG-Cloud-Share/Academic-Cloud bevorzugt werden kann.

Für nicht-personenbezogene, schützenswerte Daten ist ein anderer Weg, die Speicherung von Daten auf den Rechnern im Home-Office zu vermeiden, die Nutzung von Remote-Desktop-Verbindungen zu Terminal-Servern der Universität (im Zentralverwaltungsnetz für Verwaltungsmitarbeiter oder im „Erweiterten Verwaltungsnetz“ für andere Beschäftigte mit Zugriff auf Verwaltungsanwendungen) bzw. GWDG (allgemeiner Terminalserver mit Zugriff auf Netzlaufwerke). Soweit die benötigten Anwendungen auf solchen Servern bereitgestellt werden, sollten diese Dienste bevorzugt genutzt werden, da hier automatisch eine Speicherung von Daten auf den Speichersystemen der Universität bzw. GWDG erfolgt.

Die Nutzung externer Clouddienste zur Speicherung schützenswerter Daten ist grundsätzlich nicht zulässig und speziell für Home-Office 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 schützenswerte Daten nicht ebenfalls im externen Cloud-Backup eingeschlossen sind.

3 Einsatz von Cloud-Lösungen zur Kommunikation

Die Corona-Krise führt zu einer massenhaften Einführung von Home-Office. Die quantitativ für den Einsatz in normalen Zeiten ausgelegten eigenen Dienste für Telefon- und Videokonferenzen oder Online-Schulungen sind durch den massiven Nutzungsanstieg teilweise überlastet. Daher werden aktuell kurzfristig zusätzliche Dienste aufgebaut, aber auch freie und kommerzielle, externe Dienste zusätzlich angeboten (s. auch Anleitung der GWDG zum mobilen Arbeiten [2]).

Kommunikationsdienste bieten auch Möglichkeiten zum Datenaustausch in Chats oder über Dokumentenablagen oder zur Aufzeichnung von Konferenzen. Chats, Datenspeicherungen und Aufzeichnungen bei externen Dienstleistern sollten für schützenswerte Daten vermieden werden. Beteiligte an der Kommunikation müssen informiert sein und ihre Zustimmung bekunden, wenn eine Aufzeichnung oder Speicherung von Daten vorgenommen wird.

Der Austausch personenbezogener oder anderer schützenswerter Daten oder die Aufzeichnung von Konferenz über entsprechende Inhalte ist grundsätzlich nicht zulässig.

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

4 Hinweise zum Einsatz privater Hard- und Software

4.1 Allgemein

Die Informationssicherheitsrichtlinie der Universität [1] erlaubt in Maßnahme A.17 die Nutzung privater Hard- und Software nur, „wenn die spezifischen Informationssicherheitskonzepte für die auf den genutzten Rechner verarbeiteten Daten und die genutzten Teilbereiche der Infrastruktur den Einsatz erlauben“.

In der besonderen Situation durch die Corona-Epidemie wurde eine Erlaubnis zum Einsatz privater Hardware durch Anweisung des Präsidiums gegeben: „Wo dies möglich und sicher ist, bittet die Universitätsleitung um Einsatz auch privater Geräte, da es nicht möglich ist, alle Personen mit dienstlichen Geräten zu versorgen“ [3].

Die Erlaubnis zum Einsatz privater Hardware gilt nicht, wenn für Home-Office-Tätigkeiten dienstliche Hardware bereitgestellt wird, insbesondere auch bei der Verarbeitung schützenswerter Daten im Bereich der Verwaltung.

Auch wenn die formalen Anforderungen an ein „spezifisches Informationssicherheitskonzept“ mit dieser Anweisung nur sehr eingeschränkt erfüllt sind, muss diese Anweisung in der besonderen Situation als ausreichende Grundlage für den Einsatz privater

Rechner akzeptiert werden. Das „Wo dies … sicher ist“ wird in diesem Kapitel „4 Hinweise zum Einsatz privater Hard- und Software“ konkretisiert.

4.2 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:

- **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“. Sie können alternativ auch die durch die Universität lizensierte 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 Tabletts 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-Version 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.

4.3 Aufbewahrung und Zugriffe

Für reguläre Telearbeit gelten strenge Anforderungen an Arbeitsräume und Arbeitsmittel. Für die besondere Situation des temporären Home-Office in Rahmen der Bekämpfung der Corona-Epidemie können diese Auflagen nicht überall und/oder nicht vollständig umgesetzt oder eingefordert werden.

Dennoch sollten private Rechner mit schützenswerten Daten möglichst sicher aufbewahrt werden. Der Zugriff aus Sicht der Universität fremder Personen auf dienstliche Daten sollte so gut wie möglich verhindert werden. Fremde sind in diesem Sinn auch Familienmitglieder.

Im Idealfall nutzt der Universitätsangehörige ausschließlich selbst und nicht andere Familienmitglieder den privaten Rechner. Das wird nicht immer möglich sein. In einem solchen Fall der Mehrpersonennutzung muss das Risiko abgewogen werden, das von einem Zugriff durch Familienmitglieder ausgehen könnte. Bei einer lokalen Verarbeitung personenbezogener Daten oder aus anderen Gründen besonders vertraulicher Daten sollte der Einsatz des privaten Rechners unterbleiben.

Wird entschieden, dass der Einsatz eines privaten Rechners erfolgen soll, obwohl auch andere Familienmitglieder 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 Familienmitglieder keinen Zugriff auf diese Daten haben. Ebenso sollten die Familienmitglieder zum sicheren Umgang z.B. beim Surfen oder mit E-Mail und Kommunikationsdiensten mit dem Rechner angewiesen werden.

5 Verarbeitung personenbezogener Daten

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

5.1 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.

Auskunft und Löschung personenbezogener Daten darf auch von Privatrechnern aus nur über den Dienstweg (Datenschutzmanager - Hr. Marcus Remmers, Leiter IT -) gewährt werden. Die Anweisung des Datenschutzmanagers ist abzuwarten.

5.2 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 Home-Office benötigt werden, so sind Prozesse organisiert oder sollten organisiert werden, die solche Dokumente in digitaler Form bereitstellen. Scanprozesse zur Digitalisierung müssen dabei auf dem Campus stattfinden. Die Bereitstellung und Speicherung erfolgt auf Datenspeichern der Universität.

6 Ausnutzung der Corona-Krise durch Internet-Kriminalität und in Sozialen Medien

Wie alle Ereignisse, die in den Medien große Aufmerksamkeit erregen, wird auch die Corona-Krise von Internet-Kriminellen genutzt, um Sie über E-Mails zum Download von Schadsoftware oder zu kurzfristigen Zahlungen oder einfach zur Anmeldung an einer gefälschten Webseite zu verleiten, um dort ihr Passwort abzugreifen. Die ungewöhnliche Arbeitssituation in der Krise kann es den Kriminellen erleichtern, Sie zu falschen Handlungen zu veranlassen. Seien Sie besonders aufmerksam, prüfen Sie Absender und Kontext von E-Mails besonders gründlich und vergewissern Sie sich im Zweifelsfall lieber einmal mehr (z.B. durch telefonische Rückfragen), ob die eingegangenen E-Mails wirklich vom angegebenen Absender stammen und alle Anlagen und Links ungefährlich sind.

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].