Merkblatt zu Informations- und Datenschutz[1]

Sicherheitshinweise

Bei der mobilen Arbeit sollten Sie die gleichen Sicherheitsanforderungen wie an Ihrem Arbeitsplatz im Büro berücksichtigen. Dabei dienen folgende Maßnahmen zur Orientierung:

1) Mobile Arbeit ist aus Sicherheitsgründen ausschließlich auf geeigneter privater oder durch die Universität bereitgestellter Hardware auszuführen. Nutzen Sie zur Verbindung mit den Datenquellen der Universität eine VPN-Verbindung des URZ.

2) Falls Sie mit privaten Geräten arbeiten, verwenden Sie ausschließlich die VDI-Umgebung des URZ. Damit ist sichergestellt, dass Dokumente, an denen Sie arbeiten, auf Datenträgern im Netz der Universität verbleiben und somit auch die übliche Datensicherung (Backup) gewährleistet werden kann.

3) Wenn Sie Ihren privaten Internet-Anschluss verwenden: Richten Sie Ihren Computer so ein, dass er mit dem privaten Netzwerk durch ein Kabel oder ein verschlüsseltes WLAN verbunden ist. Ihr WLAN sollte so eingerichtet sein, dass man sich nur mit einem ausreichend langen und komplexen Passwort einwählen kann.

4) Finden Sie einen geeigneten Platz, um Papier-Dokumente zu lagern. Dokumente mit personenbezogenen Daten müssen verschlossen aufbewahrt werden, am besten in einem verschlossenen Raum oder Behälter. Achten Sie auch darauf, dass Ihre Geräte und Speichermedien nicht zugänglich sind, wenn Sie den Raum verlassen, z. B. abends nach getaner Arbeit.

5) Organisieren Sie Ihren Arbeitsplatz so, dass sich private und dienstliche Daten nicht mischen.

6) Wenn Sie Ihren Arbeitsplatz kurzfristig verlassen, sperren Sie den Rechner (z.B. bei Windows mittels der Tastenkombination „Windows + L“).

7) Wenn Sie an einem dienstlichen Computer arbeiten, nutzen Sie diesen ausschließlich für dienstliche Zwecke. Schließen Sie an diesem Gerät keine private Hardware (z. B. externe Festplatten oder USB-Sticks) an. So verringern Sie das Risiko, dass Schadsoftware Ihren Computer befallen und Ihre Daten kompromittiert werden. Falls der Computer doch infiziert wurde, melden Sie dies schnellstens dem IT-Service-Desk.

8) Richten Sie nach Möglichkeit einen Arbeitsplatz in einem eigenen Raum oder in einer eigenen Ecke ein. Wählen Sie den Platz so, dass andere nicht den Bildschirm sehen können – auch nicht durch ein Fenster. Eine Sichtschutzfolie für den Monitor kann dies unterstützen. Achten Sie beim Verlassen des Arbeitsplatzes darauf, dass Türen und – vor allem im Erdgeschoss – Fenster verschlossen bzw. geschlossen sind, um eine unbefugte Kenntnisnahme, einen Verlust oder eine Veränderung von Daten zu verhindern. Sollte dies in Ihrer häuslichen Umgebung nicht vollständig möglich sein,

[1] Die Aushändigung eines Merkblattes mit Hinweisen und Regelungen zu Datenschutz und Informationssicherheit ist eine ausdrückliche Anforderung aus dem IT-Grundschutz (Baustein: INF.9.M2 Regelungen für mobile Arbeitsplätze).

gehören zumindest Ihre Papierdokumente in einen verschlossenen Schreibtisch oder Schrank.

9) Wenn Sie Dokumente an Ihrem häuslichen Arbeitsplatz ausdrucken müssen, dann achten Sie darauf, dass Sie diese Dokumente unverzüglich aus dem Drucker entnehmen, damit andere Personen im Haushalt keine Kenntnis dieser Daten nehmen können. Achten Sie darauf, dass Sie keine Druckaufträge auf Drucker in Ihren Dienstgebäuden abschicken, da in diesem Fall unberechtigte Personen Einblick in diese Dokumente nehmen könnten.

10) Werfen Sie dienstliche Papierdokumente nicht in Ihren privaten Papiermüll. Sammeln Sie Ihren Papiermüll, lagern Sie ihn verschlossen und nehmen Sie ihn mit, wenn Sie wieder ins Dienstgebäude gehen. Entsorgen Sie den Papiermüll dann dort nach den geltenden Regeln.

11) Für den Fall eines Datenverlusts (z. B. Verlust von Papierunterlagen oder Datenträgern) oder eines Datenschutzverstoßes (z. B. Zugang von Unbefugten an den Computer) besteht eine Meldepflicht. Diese sind unverzüglich bei der/dem unmittelbaren Vorgesetzten und beim Datenschutzmanagement (Kontakte s.u.) anzuzeigen.

12) Wenn Sie am häuslichen Arbeitsplatz dienstlich telefonieren müssen, dann achten Sie darauf, dass Sie dafür einen ungestörten Bereich aufsuchen, damit andere Personen im Haushalt keine Kenntnis von Ihrem Telefonat nehmen können.

13) Zudem wird empfohlen, dass Ihre private Nummer bei Ihren Anrufen nicht übertragen wird, weil sonst Kundinnen und Kunden Ihre Privatnummer des Handys oder Ihres Haushalts auch in späteren Kontakten nutzen könnten. Achtung: Einige Telefonkonferenzsysteme funktionieren nur mit übertragener Rufnummer.

14) Wenn Sie für die Kommunikation untereinander einen Messenger nutzen, achten Sie darauf, keine sensiblen Informationen auszutauschen.

15) Nutzen Sie für dienstliche Aufgaben ausschließlich Ihre dienstliche E-Mailadresse, nicht private Mailadressen.

16) Für Beschäftigte der Zentralverwaltung gilt die Dienstanweisung zur Informationssicherheit.

Datenschutz

1) Es gelten die Datenschutzvorgaben gemäß der Anlage 6 zur Dienstvereinbarung Mobile Arbeit. Bei der Zuordnung von Schutzbedarfskategorien können Sie sich an einem Leitfaden orientieren, der von der Stabsstelle für Datenschutz und Informationssicherheit zur Verfügung gestellt wird:

   https://intranet.uni-leipzig.de/zentralverwaltung/referat-fuer-datenschutz-und-informationssicherheit/regelungen/

2) Zum Umgang mit Datenpannen orientieren Sie sich bitte am entsprechenden Leitfaden:

   https://intranet.uni-leipzig.de/zentralverwaltung/referat-fuer-datenschutz-und-informationssicherheit/sicherheits-und-datenschutzvorfaelle/

Verarbeitung personenbezogener Daten

1) Auch bei der Verarbeitung personenbezogener Daten während der mobilen Arbeit sind die datenschutzrechtlichen Vorschriften zu beachten, insbesondere die EU-Datenschutz-Grundverordnung (DSGVO), das Sächsische Datenschutzdurchführungsgesetz (SächsDSDG), das Sächsische Hochschulfreiheitsgesetz (SächsHSFG) und die Sächsische Hochschulpersonendatenverordnung (SächsHSPersDatVO).

2) Personenbezogene Daten sind gemäß Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

3) Verarbeitung ist gemäß Art. 4 Nr. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

4) Personenbezogene Daten dürfen gem. Art. 29 DSGVO ausschließlich auf Weisung des Verantwortlichen verarbeitet werden, es sei denn, eine gesetzliche Regelung schreibt eine Verarbeitung dieser Daten vor. Als Weisung gelten neben Einzelanweisungen der Vorgesetzten u. a. Verordnungen, Dienstvereinbarungen, allgemeine Dienstanweisungen, Prozessbeschreibungen, Ablaufpläne, betriebliche Dokumentationen und Handbücher.

5) Sofern bei der mobilen Arbeit personenbezogene Daten verarbeitet werden, sind die Grundsätze der DSGVO für die Verarbeitung personenbezogener Daten zu wahren; sie sind u. a. in Art. 5 Abs. 1 DSGVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten müssen

a) auf rechtmäßige und faire Weise, und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz")

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung")

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung")

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick

auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“)

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung“)

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten richtet sich auch während der Mobilen Arbeit nach Art. 9 DSGVO.

Wichtige Kontakte (direkt, Vorwahl 0341 97 - ...)

Datenschutzmanagement	30 117
Datenschutzbeauftragter	30 081
IT-Servicezentrum	33 333
Gebäudeleittechnik (GA-Zentrale) der Universität	34 333