IT-Sicherheitsvorgaben bei der Ausübung von Mobiler Arbeit

Zum Datenschutz und zur Informationssicherheit gelten die gleichen rechtlichen Regelungen wie an der Dienststelle. Da bei Mobiler Arbeit eine erhöhte Gefahr der Einflussnahme oder Missbrauchsmöglichkeiten durch Dritte besteht, müssen zur Minimierung dieses Risikos von den Beschäftigten je nach Schutzniveau der zu verarbeitenden Daten zusätzliche Vorgaben eingehalten werden.

In Abhängigkeit von der Arbeitstätigkeit und dem Schutzbedarf der zu verarbeitenden Daten ergeben sich die nachfolgenden IT-Sicherheitsvorgaben, die in drei Schutzkategorien unterteilt sind:

1. Verarbeitung von Daten ohne gesteigertes Schutzniveau
2. Verarbeitung von (nicht sensiblen) personenbezogenen Daten und/oder vertraulichen Daten
3. Verarbeitung von personenbezogenen sensiblen Daten und/oder Personaldaten

Die IT-Sicherheitsvorgaben eines höheren Schutzniveaus schließen alle IT-Sicherheitsvorgaben aus den niedrigeren Niveaus mit ein. Bei Unklarheiten bezüglich der Schutzkategorie der Daten ist der Datenschutzbeauftragte der Universität Leipzig zu befragen, dessen Einschätzung maßgebend ist. Bei der Zuordnung von Schutzbedarfskategorien können Sie sich auch 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/

Bei der Umsetzung der nachfolgend benannten IT-Sicherheitsvorgaben werden die Beschäftigten von der für die jeweilige Einrichtung verantwortlichen technischen IT-Betreuungsstelle unterstützt.

1. Verarbeitung von Daten ohne gesteigertes Schutzniveau

a) Begriffsbestimmung

Unter Daten ohne gesteigertes Schutzniveau (im Vergleich zu den Daten, die unten unter den Nummern 2 und 3 aufgeführt sind) werden Daten verstanden, die nicht personenbezogen und nicht vertraulich sind.

b) Beispiele

- Erstellen von Lehrmaterialien für Lehrveranstaltungen und Praktika
- Konzeptionelle Arbeiten (z. B. Entwurf von Präsentationen, Erarbeitung von Vorträgen)
- Recherchearbeiten

c) Vorgaben

Private IT-Geräte sollen nur zum Einsatz kommen, sofern aktuell keine dienstlichen IT-Geräte für Mobile Arbeit zur Verfügung stehen. Je nachdem, ob private oder dienstliche

IT-Geräte für Mobile Arbeit genutzt werden, sind nachfolgende Anforderungen zu erfüllen. Für alle Geräte gilt:

- Es muss ein aktuelles Betriebssystem installiert sein (mitsamt aller aktuellen Sicherheitsupdates).
- Erforderlich ist ein installiertes Virenprogramm.
- Notwendig ist eine installierte und aktivierte Firewall.
- Der Zugriff auf das Gerät muss durch Passwort, PIN oder einen anderen Zugriffschutz gesichert sein.
- Der genutzte Benutzeraccount darf keine Administratorenrechte besitzen.
- Datenzugriffe auf die Universität Leipzig sind grundsätzlich zu verschlüsseln (HTTPS, SSH, VPN).
- Sperrung des Bildschirms beim (kurzzeitigen) Verlassen des Gerätes, damit ein unbefugter Zugriff durch Dritte nicht einfach möglich ist.
- Für dienstliche Aufgaben ist ausschließlich die dienstliche E-Mailadresse zu verwenden.
- Im Falle einer Virus-Infektion des IT-Gerätes oder bei einem ähnlichen Sicherheitsvorfall ist unverzüglich die für die jeweilige Einrichtung verantwortliche technische IT-Betreuungsstelle zu informieren und das Gerät vom Internet zu trennen.
- Sofern private Internet-Anschlüsse genutzt werden (WLAN, LAN, LTE, 5G), muss das Gerät sicher mit dem Netzwerk verbunden werden. WLAN Netze müssen verschlüsselt und mit einem ausreichend langen und komplexen Passwort versehen sein. Der Anschluss des Gerätes durch ein Netzwerkkabel soll bevorzugt werden.
- Netzwerkverbindungen mit öffentlichen WLAN Netzen sollen vermieden werden. VPN muss in diesen Netzen immer aktiviert sein, um den Datenverkehr innerhalb des öffentlichen WLAN abzusichern. Geräte in öffentlichen Netzen müssen durch eine Firewall abgesichert sein.
- Der Bildschirm soll durch andere Personen nicht direkt einsehbar sein - auch nicht durch ein Fenster. Eine Blickschutzfolie für den Monitor kann dies unterstützen.

Für private Geräte gilt weiterhin:

- Es sollen keine dienstlichen Dateien auf dem Gerät gespeichert werden. Über eine Fernzugriffs [1] -Verbindung ist das Arbeiten auf Rechnern in der Universität Leipzig von der Ferne möglich und die Daten verbleiben somit innerhalb der Universität. Die jeweils zuständige verantwortliche technische Betreuungsstelle stellt eine VDI-Umgebung (Virtual Desktop Infrastructure) für das sichere Arbeiten aus der Ferne bereit.
- Falls ein Fernzugriff nicht möglich ist, dürfen private und dienstliche Dateien sich nicht mischen. Alle dienstlichen Dateien müssen in einem separaten Ordner (mit

[1] Fernzugriff: Zugriff über ein verschlüsseltes Protokoll (SSH, RDP oder andere) auf einen in der Universität Leipzig betriebenen Fernzugriffsserver bzw. -infrastruktur (SSH-, Terminalserver, VDI-Umgebung etc.).

Unterordnern) gespeichert werden. Dieser Ordner soll verschlüsselt sein. In diesen Ordnern dürfen keine privaten Dateien abgelegt werden.

- Zugriffe auf dienstliche Laufwerke ohne eine Fernzugriffs-Verbindung sind nicht gestattet.

Für dienstliche Geräte gilt weiterhin:

- Das Gerät muss sicher aufbewahrt und vor einem unbefugten Zugriff Dritter geschützt sein
- Es muss ein Client-Management-Agent installiert sein.
- Datenträger müssen verschlüsselt sein.
- Es darf keine private Hardware (z. B. externe Festplatten oder USB-Sticks) angeschlossen werden, ausgenommen Drucker und Scanner.
- Dateien auf dem Gerät, die Arbeitsergebnisse sind, müssen spätestens zum Ende des Arbeitstages auf ein Laufwerk oder System der Universität Leipzig übertragen werden, um Datenverlust zu vermeiden.
- Zugriffe auf dienstliche Laufwerke sind über VPN- oder Fernzugriffs-Verbindung zu realisieren.

2. Verarbeitung von (nicht sensiblen) personenbezogenen Daten und/ oder vertraulichen Daten

a) Begriffsbestimmung

Personenbezogene Daten sind gem. Art. 4 Nr. 1 EU-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.

Vertrauliche Daten sind alle Daten, die nicht für die Öffentlichkeit bestimmt sind, beispielsweise noch nicht zur Veröffentlichung vorgesehene Forschungsergebnisse, Daten von Mitarbeiter:innen, Studierenden oder Interna.

b) Beispiele

Für personenbezogene Daten:

- Bewerber:innen-/Studierenden-/Prüfungsdaten
- Daten, die im Zusammenhang mit einem Beschäftigungsverhältnis stehen

Für vertrauliche Daten:

- nicht veröffentlichtes Forschungsmaterial
- strategische Dokumente
- Daten aus dem Rechnungswesen

c) Vorgaben

Die Nutzung privater Hard- und Software ist für die Verarbeitung personenbezogener oder vertraulicher Daten nicht gestattet. Hiervon ausgenommen sind Drucker und Scanner. Die Nutzung eines Smartphones oder Tablets soll vermieden werden.

Es gelten besondere Anforderungen:

- Die Datenträger müssen verschlüsselt sein.
- Die Datenverarbeitung muss grundsätzlich über eine Fernzugriffs-Umgebung erfolgen, damit die verarbeiteten Daten immer auf Rechner der Universität Leipzig verbleiben. Hierfür ist die von der verantwortlichen technischen IT-Betreuungsstelle bereitgestellte VDI-Umgebung zu verwenden. Falls ein Fernzugriff nicht möglich ist, muss eine VPN-Verbindung auf die notwendigen Laufwerke genutzt werden.
- Cloud-Speicher, die nicht direkt durch die Universität Leipzig betrieben werden, dürfen nicht genutzt werden.
- Personenbezogene oder vertrauliche Daten dürfen nicht über Messenger-Plattformen ausgetauscht werden.

3. Verarbeitung von personenbezogenen sensiblen Daten und/oder Personaldaten

a) Begriffsbestimmung

Sensible Daten sind die in Art. 9 Abs. 1 EU-DSGVO genannten Daten. Es handelt sich hierbei um personenbezogene Daten betreffend

- ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- genetische Daten
- biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung

Personaldaten sind alle personalaktenrelevanten Daten i. S. v. Buchstabe A Ziffer 1 Nr. 2 VwV Personalakten Beamte (i. V. m. Punkt 2.1 VwV Personalakten) für Beschäftigte und Beamte und damit alle in einem inneren Zusammenhang mit dem Arbeits- bzw. Dienstverhältnis stehenden wesentlichen Daten, insbesondere

- Bewerbungsunterlagen und Bewerbungsschreiben
- Lebenslauf
- Lichtbild
- Referenzen und Zeugnisse
- frühere Arbeitsverträge im öffentlichen Dienst
- aktueller Arbeitsvertrag mit sämtlichen Änderungen und Ergänzungen
- Dokumente über familiäre Veränderungen
- dienstliche Beurteilungen
- Zwischenzeugnisse

- Bestätigungen über Fortbildungsmaßnahmen
- Abmahnungen
- Beurlaubungen (Dauer/Gründe)
- Teilzeitbeschäftigung (Dauer/Anteil)
- Krankheitsbescheinigungen
- Urlaubsanträge und Urlaubsbewilligungen
- Schwerbehinderung oder Gleichstellung
- Krankheitsbedingte und sonstige Fehlzeiten
- Kündigungsschreiben bzw. Aufhebungsvertrag
- Schulzeugnisse
- Unterlagen über die betriebliche Altersversorgung

b) Beispiele

- Vorbereitung von Arbeitsverträgen und Zeugnissen
- Bearbeitung von Urlaubsanträgen und Krankenscheinen

c) Vorgaben

Der Nutzerzugriff auf personenbezogene sensible Daten und/oder Personaldaten darf ausschließlich mit über vom Universitätsrechenzentrum geprüften und verwalteten dienstlichen IT-Geräten (Notebook oder PC) erfolgen.

Es gelten folgende zusätzliche Anforderungen:

- Die Datenverarbeitung darf ausschließlich über eine vom Universitätsrechenzentrum bereitgestellte VDI-Umgebung erfolgen. Der Zugriff muss über eine Zweifaktor- Authentifizierung gesichert sein.
- Ein Datenaustausch darf nur in dem Maß stattfinden, welches auch innerhalb der
- Dienststelle gestattet ist.