Anlage 5

Anforderungen: Vertraulichkeit, Datenschutz und Informationssicherheit

Bei Mobiler Arbeit gelten die gleichen Anforderungen an den Umgang mit vertraulichen Informationen und personenbezogenen Daten wie bei der Tätigkeit in der Dienststelle. Da insbesondere das Risiko für einen unberechtigten Zugriff auf zu schützende Informationen und Daten durch Dritte außerhalb der Dienststelle als höher einzuschätzen ist, müssen spezielle Sicherheitsvorkehrungen getroffen werden. In Abhängigkeit von der Tätigkeit, dem Schutzbedarf von Informationen und Daten und dem verwendeten Endgerät ergeben sich deshalb unterschiedliche Erfordernisse, die von Ihnen während der Mobilen Arbeit strikt einzuhalten sind. Dieses Dokument gliedert sich in folgende Abschnitte:

Inhalt

I. Allgemeine Bestimmungen

1. Datenschutzrecht

Für den Umgang mit personenbezogenen Daten sind die Grundsätze der Datenschutz-Grundverordnung (DS-GVO) zu wahren; sie sind in Art. 5 Abs. 1 DS-GVO 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“).**

Insbesondere für sensible personenbezogene Daten und Beschäftigten- bzw. Personaldaten sind zusätzliche Anforderungen zu beachten. Diese sind beispielsweise festgelegt in Art. 9 DS-GVO, § 18 des Landesdatenschutzgesetzes Nordrhein-Westfalen (DSG NRW) sowie weiteren Regelungen, insbesondere in den §§ 83 ff. des Landesbeamtengesetzes Nordrhein-Westfalen (LBG NRW). Die Gesamttexte der DS-GVO, des DSG NRW sowie des LBG und weiterer relevanter Gesetze finden Sie auf den Seiten der Stabsstelle Datenschutz.

2. Geheimhaltungs- und Vertraulichkeitsvereinbarungen

An der Universität Paderborn werden in unterschiedlichen Kontexten häufige sogenannte Geheimhaltungs- oder Vertraulichkeitsvereinbarungen geschlossen (z. B. mit Drittmittelgebern oder Industriepartnern). Geheimhaltungsbedürftige oder vertrauliche Informationen sind im Regelfall Informationen, die als vertraulich gekennzeichnet oder aus den Umständen heraus als vertraulich anzusehen sind, insbesondere Informationen über betriebliche Abläufe, Geschäftsbeziehungen, Know-how und solche Informationen, die von ähnlicher Natur sind. Vertrauliche Informationen können auch solche sein, die im Einzelfall nicht den Anforderungen eines Geschäftsgeheimnisses im Sinne des Gesetzes zum Schutz von Geschäftsgeheimnissen (GeschGehG) entsprechen; ferner können sie personenbezogenen sein, müssen es aber nicht.

Ob und wie weit sich im Rahmen der dienstlichen Tätigkeit Einschränkungen an den Umgang mit Informationen und Daten beim Mobilen Arbeiten aus Geheimhaltungs- oder Vertraulichkeits-vereinbarungen ergeben, muss stets individuell berücksichtigt werden.

3. Informationssicherheit

Zweck und Ziel der Informationssicherheit ist die Erfüllung von gesetzlichen Verpflichtungen und Auflagen, der Schutz der an der Universität Paderborn verarbeiteten Informationen, die Aufrechterhaltung von informationstechnischen Systemen sowie die Vermeidung von materiellen und immateriellen Schäden für die Universität Paderborn sowie von der Datenverarbeitung betroffenen Personen und Organisationen. Die Informationssicherheit ist eine Grundvoraussetzung zur Sicherstellung von Vertraulichkeit und Datenschutz.

Maßgeblich für die Mobile Arbeit an der Universität Paderborn sind der BSI-Grundschutzstandard 200-2 sowie das IT-Grundschutz-Kompendium des BSI (Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de) in den jeweils aktuellen Fassungen. Die entsprechenden Module sind im Anhang aufgeführt.

II. Konkrete Umsetzungshinweise

Die folgenden Seiten fassen die wesentlichen Anforderungen an den Umgang mit vertraulichen Informationen und personenbezogenen Daten bei Mobiler Arbeit zusammen. Die Anforderungen unterscheiden sich nach dem Schutzbedarf von Informationen und Daten und nach Endgeräte-Klassen.

1. Schutzbedarf von Informationen und Daten

In Abhängigkeit von der Arbeitstätigkeit und dem Schutzbedarf von Informationen und Daten ergeben sich die nachfolgenden IT-Sicherheitsvorgaben, die in drei Schutzkategorien unterteilt sind (siehe Definition von Schutzbedarfsklassen der Universität Paderborn):

1. Schutzbedarf „normal“: Eine unberechtigte Weitergabe und/oder Offenlegung hätte begrenzt negative Auswirkungen für die Universität Paderborn sowie für das informationelle Selbstbestimmungsrecht betroffener Personen
2. Schutzbedarf „hoch“: Eine unberechtigte Weitergabe und/oder Offenlegung hätte erhebliche Auswirkungen für die Universität Paderborn sowie für das informationelle Selbstbestimmungsrecht betroffener Personen
3. Schutzbedarf „sehr hoch“: Eine unberechtigte Weitergabe und/oder Offenlegung hätte existenzbedrohende Auswirkungen für die Universität sowie für das informationelle Selbstbestimmungsrecht betroffener Personen.

Die Vorgaben eines höheren Schutzniveaus schließen alle Vorgaben aus den niedrigeren Niveaus mit ein. Bei Unklarheiten bezüglich der Schutzkategorie der Daten ist das Informationssicherheitsteam und – im Fall personenbezogener Daten – der*die Datenschutzbeauftragte der Universität Paderborn zu befragen, dessen*deren Einschätzungen maßgebend sind.

2. Anforderungen an das mobile Arbeiten für alle Bearbeitungsformate

Vertrauliche Informationen und personenbezogene Daten, die Gegenstand der dienstlichen Tätigkeit sind, sind bei Mobiler Arbeit so zu schützen, dass ein unbefugter Zugang zu und ein unberechtigter Zugriff auf die Informationen und Daten durch Dritte (auch Familienangehörige) wirksam verhindert wird. Öffentliche Orte wie z. B. Zugabteile, Cafés und Grünanlagen sind daher für die Mobile Arbeit nur bedingt geeignet und erfordern wirksame Schutzmaßnahmen.

Dienstliche Originalunterlagen verbleiben in den Räumen der Universität Paderborn. Bei dienstlicher Notwendigkeit können nach Absprache mit dem*der Vorgesetzten Originale oder Kopien in die Mobile Arbeit mitgenommen werden. Originale sind gemäß der Absprache auf einem sicheren Transportweg in die Räume der Universität Paderborn zurückzubringen. Kopien mit vertraulichen Informationen und/oder

personenbezogenen Daten sind nach Abschluss der Arbeiten in der Dienststelle datenschutzkonform zu vernichten. Eine datenschutzkonforme Vernichtung dienstlicher Unterlagen wird regelmäßig durch die Zentralverwaltung der Universität Paderborn (Dezernat 5) organisiert.

Dienstliche Unterlagen (einschließlich Datenträger) müssen geschützt aufbewahrt werden. Der Transport von dienstlichen Unterlagen sollte nur in geschlossenen Behältern vorgenommen werden.

3. Anforderungen an das mobile Arbeiten in Abhängigkeit von Endgeräte-Klassen

a. Klassen von IKM-Endgeräten

Folgende Klassen von Endgeräten werden unterschieden

1. Stationärer (dienstlicher) Büroarbeitsplatz in den Ausprägungen
    a. Komplett von einer IT-Abteilung betrieben und gepflegt
    b. Teilweise (sicherheitsrelevante Dinge) von einer IT-Abteilung betrieben und gepflegt, dokumentierte zusätzliche Rechte sind an den*die Nutzer*in vergeben
    c. Selbst administrierte Geräte
2. Mobile (dienstliche) Endgeräte in den Ausprägungen
    a. Komplett von einer IT-Abteilung betrieben und gepflegt
    b. Teilweise (sicherheitsrelevante Dinge) von einer IT-Abteilung betrieben und gepflegt, dokumentierte zusätzliche Rechte sind an den*die Nutzer*in vergeben
    c. Selbst administrierte Geräte
3. Private Geräte (immer in der Ausprägung des selbstadministrierten Gerätes)

b. Überblick über die erlaubten Bearbeitungsformate

		Schutzbedarf normal	**Schutzbedarf hoch**	**Schutzbedarf sehr hoch**
2	**a**	Erlaubt	Erlaubt	Erlaubt mit Auflagen
	b	Erlaubt	Erlaubt mit Auflagen	Nicht erlaubt
	c	Erlaubt mit Auflagen	Erlaubt mit Auflagen	Nicht erlaubt
3		Erlaubt mit Auflagen	Nicht erlaubt	Nicht erlaubt

c. Anforderungen für alle Endgeräte-Klassen

Für alle Geräte gelten folgende Anforderungen:

- Es muss ein aktuelles Betriebssystem jeweils mitsamt aller aktuellen Sicherheitsupdates installiert sein. Updates sind automatisiert zu installieren. Genutzte Software ist ebenfalls aktuell zu halten.
- Erforderlich ist ein installiertes Virenprogramm (sofern möglich, bei Windows 10 integriert), das das Gerät regelmäßig überprüft.
- Notwendig ist zusätzlich eine installierte und aktivierte Firewall (sofern möglich, bei Windows 10 integriert).
- 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 Paderborn erfolgen grundsätzlich verschlüsselt (HTTPS, SSH, VPN).
- Sperrung des Bildschirms beim (kurzzeitigen) Verlassen des Gerätes, damit ein unbefugter Zugriff durch Dritte nicht einfach möglich ist.
- Im Falle einer Virus-Infektion des IT-Gerätes oder bei einem anderen Sicherheitsvorfall ist unverzüglich die für die jeweilige Einrichtung verantwortliche technische IT-Betreuungsstelle zu informieren (siehe Abschnitt 5.) 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.
- Der Bildschirm soll durch andere Personen nicht direkt einsehbar sein - auch nicht durch Familienangehörige oder ein Fenster. Eine Blickschutzfolie für den Monitor kann dies unterstützen.
- Die Nutzung von E-Mail, Cloudspeichern, Videokonferenzanbietern, Messengern und ähnlichen Diensten erfolgt über die von der Universität Paderborn betriebenen und/oder verantworteten Systeme. Die Nutzung externer Dienste ist nur zulässig, wenn alle damit verbundenen datenschutzrechtlichen Anforderungen erfüllt werden.
- Bei der Durchführung von Videokonferenzen ist darauf zu achten, dass Einblicke in die Privatsphäre vermieden werden. Die Auswahl der Umgebung oder des Raumes, die bzw. Positionierung der Kamera, die De-Personalisierung der Umgebung oder die Verwendung virtueller Hintergründe oder Hintergrundschärfe können dies unterstützen.

d. Auflagen bei (mindestens) Schutzbedarf normal

Private IT-Geräte sollen nur zum Einsatz kommen, sofern aktuell keine dienstlichen IT-Geräte für Mobile Arbeit zur Verfügung stehen. Unabhängig davon, ob private oder dienstliche IT-Geräte für Mobile Arbeit genutzt werden, sind nachfolgende Anforderungen zu erfüllen.

Für dienstliche Geräte gelten neben den allgemeinen Anforderungen folgende Auflagen:

- Das Gerät muss sicher aufbewahrt und vor einem unbefugten Zugriff Dritter geschützt sein.
- Datenträger müssen verschlüsselt sein. Aktuelle Smartphones und Tablets erfüllen diese Anforderung ab Werk.
- 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 Paderborn übertragen werden, um Datenverlust zu vermeiden.

Für private Geräte gilt weiterhin:

- Es sollen keine dienstlichen Dateien auf dem Gerät gespeichert werden. Über eine Fernzugriffs-Verbindung ist das Arbeiten auf Rechnern in der Universität Paderborn von der Ferne möglich und die in den Dateien gespeicherten Informationen und Daten verbleiben somit innerhalb der Universität Paderborn. Die jeweils zuständige verantwortliche technische Betreuungsstelle stellt

eine remote-Umgebung (Virtual Desktop Infrastructure o.ä.) 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 Unterordnern) gespeichert werden. Dieser Ordner soll verschlüsselt sein. In diesen Ordnern dürfen keine privaten Dateien abgelegt werden. Werden dienstliche Dateien gespeichert muss das Gerät sicher aufbewahrt und vor einem unbefugten Zugriff Dritter geschützt sein.

e. Zusätzliche Auflagen bei mindestens Schutzbedarf hoch

Die Nutzung privater Hard- und Software ist für die Bearbeitung dienstlicher Unterlagen nicht gestattet. Hiervon ausgenommen sind Drucker und Scanner. Die Nutzung eines Smartphones oder Tablets soll vermieden werden.

Es gelten folgende zusätzliche Auflagen:

- Die Datenträger (auch USB-Sticks, externe Festplatten) müssen verschlüsselt sein. Aktuelle Smartphones und Tablets erfüllen diese Anforderung ab Werk.
- Die Datenverarbeitung muss grundsätzlich über eine Fernzugriffs-Umgebung erfolgen, damit die verarbeiteten Daten immer auf Rechner der Universität Paderborn verbleiben. Hierfür ist die von der verantwortlichen technischen IT-Betreuungsstelle bereitgestellte VDI-Umgebung (o.ä.) zu verwenden.
- Falls ein Fernzugriff nicht möglich ist, muss eine VPN-Verbindung auf die notwendigen Laufwerke genutzt werden.
- Die Nutzung von externen Cloud-Diensten (wie bspw. E-Mail, Cloudspeichern, Videokonferenzanbietern, Messengern) ist nur in Ausnahmefällen erlaubt, sofern die Dateien verschlüsselt oder pseudonymisiert werden und alle weiteren damit verbundenen datenschutzrechtlichen Anforderungen erfüllt werden.

f. Zusätzliche Auflagen bei Schutzbedarf sehr hoch

Der Nutzerzugriff auf dienstliche Unterlagen darf ausschließlich mit über von der zuständigen IT-Abteilung geprüften und verwalteten dienstlichen IT-Geräten (Notebook oder PC) erfolgen.

Es gelten folgende zusätzliche Auflagen:

- Die Datenverarbeitung darf ausschließlich über eine vom Universitätsrechenzentrum bereitgestellte VDI-Umgebung oder andere Remote-Lösung erfolgen. Der Zugriff soll wenn möglich über eine Zweifaktor-Authentifizierung gesichert sein.
- Ein Datenaustausch darf nur in dem Maß stattfinden, welches auch innerhalb der Dienststelle gestattet ist.
- Die Nutzung von E-Mail, Cloudspeichern, Videokonferenzanbietern, Messengern und ähnlichen Diensten erfolgt ausschließlich über die von der Universität Paderborn betriebenen und/oder verantworteten Systeme. Die Nutzung externer, nicht von der Universität Paderborn verantworteten, Dienste ist nicht zulässig.

4. Telefonie

Für die telefonische Weiterleitung und/oder Offenlegungen von vertraulichen Informationen und personenbezogenen Daten gelten die o.a. Anforderungen und Auflagen sinngemäß. Zur Unterstützung Mobiler Arbeit wird über die Telefonanlage der Universität Paderborn folgende Funktionalität bereitgestellt:

- Die Weiterleitung der dienstlichen Rufnummer sollte eingerichtet werden
- Rufnummern der eingehenden Anrufe sind regelmäßig zu löschen
- Private Rufnummern sollten bei ausgehenden Anrufen unterdrückt werden
- Soft-Clients sollten nur auf dienstlichen Geräten installiert werden

5. Informationssicherheitsvorfälle und Meldung der Verletzung des Schutzes personenbezogener Daten

Erkannte Informationssicherheitsvorfälle/Datenschutzverletzungen oder belastbare Hinweise darauf sind unverzüglich der Dienststelle und dem*der Datenschutzbeauftragten der Universität Paderborn zu melden. Eine Kontaktaufnahme sollte insbesondere bereits dann erfolgen, wenn die Annahme besteht, dass die Vertraulichkeit von Informationen und Daten, gefährdet sein kann und/oder dass Dritte unbefugt Zugriff oder Zugang zu vertraulichen Informationen und/oder personenbezogenen Daten haben oder hatten (bspw. ein gestohlenes/verlorenes Notebook, eine gestohlene/verlorene Tasche mit Datenträgern und/oder dienstlichen Papierdokumenten etc.). Festgestellte Sicherheitslücken sind der Dienststelle ebenfalls sofort anzuzeigen.

Die Meldung erfolgt über das Ticketsystem der Universität Paderborn unter https://www.uni-paderborn.de/universitaet/informationssicherheit/informationssicherheitsvorfall/.

III. Ansprechpartner*innen

Angelegenheit	**Zuständige Stelle**	**Kontaktdaten**
Fragen zum Datenschutz	Stabsstelle Datenschutz	datenschutz@upb.de
Fragen zur Informationssicherheit	Stabsstelle Informationssicherheit	informationssicherheit@upb.de
Informationssicherheitsvorfall/ Verletzung des Schutzes personenbezogener Daten	Vorfallteam	vorfall@upb.de
Technischer Support	IMT Dezernat 6	imt@upb.de it-service@zv.uni-paderborn.de
Datenschutzkonforme Aktenvernichtung * *keine Anlaufstelle für allgemeine Informationen zum Thema Altakten	Dezernat 5	altakten-datenschutz@zv.upb.de
Datenträgerentsorgung	Dezernat 5	Datentraegerentsorgung@zv.uni-paderborn.de

IV. Weitere Informationen und Anleitungen

Information	Link
Daten sicher aufbewahren	https://hilfe.uni-paderborn.de/Daten_sicher_aufbewahren
Daten sicher teilen	https://hilfe.uni-paderborn.de/Daten_sicher_teilen
Dateiverschlüsse-lung einsetzen	https://hilfe.uni-paderborn.de/Dateiverschlüsselung_einsetzen
Netzwerkspeicher	https://hilfe.uni-paderborn.de/Netzwerkspeicher
Sciebo	https://hilfe.uni-paderborn.de/Sciebo
Signierte E-Mails	https://hilfe.uni-paderborn.de/Signierte_E-Mails
Schutzbedarf Informationsklassen	https://www.uni-paderborn.de/fileadmin/informationssicherheit/20200702_Schutzbedarf_Informationsklassen_v1.pdf
Richtlinie Sciebo-Nutzung	https://www.uni-paderborn.de/fileadmin/informationssicherheit/20200702_Richtlinie_Sciebo_v1.pdf

V. Anhang

Aus dem BSI-Standard werden die folgenden Module zzgl. aller dort verwiesenen Module zugrunde gelegt:

- CON 2 Datenschutz
- CON 3 Datensicherungskonzept
- CON 7 Informationssicherheit auf Auslandsreisen,
- CON 6 Löschen und Vernichten
- CON 9 Informationsaustausch
- INF 1 Gebäude,
- INF 8 Häuslicher Arbeitsplatz,
- INF 9 Mobiler Arbeitsplatz,
- NET 3.3 VPN,
- OPS 1.2.4 Telearbeit,
- OPS 2.2 Cloud Nutzung
- SYS 2.1 Allgemeiner Client,
- SYS3.1 Laptops,
- SYS 3.2.1 Allgemeine Smartphones und Tablets,
- SYS 3.3 Mobiltelefon
- SYS 4.1 Drucker, Kopierer und Multifunktionsgeräte
- SYS 3.4 Mobile Datenträger,
- DER 2.1 Behandlung von Sicherheitsvorfällen