UNIVERSITÄT BIELEFELD

Fakultät für Linguistik und Literaturwissenschaft

IT-Richtlinie

§1 Grundsätze, Rechte und Pflichten 1
§2 Geltungsbereich 2
§3 Verantwortlichkeiten für IT-Geräte/-Dienste (Geräteklassen) 2
§4 Verarbeitung dienstlicher Daten, Zugriff auf IT-Dienste und Daten-/Netzwerkinfrastruktur 3
§5 Rechte und Pflichten des BITS und der dez. Admins 3
§6 Sicherheitsmaßnahmen 4
§7 Nutzung von Cloud-Diensten und KI-Systemen 4
§8 Bereitstellung und Finanzierung von IT-Ausstattung 6
§9 Ansprechperson für IT-Angelegenheiten 6
§10 IT-Notfall / Incident Management 7
§11 Inkrafttreten 7
Anlage 1 Glossar 9
Anlage 2 Matrix Schutzbedarfsfeststellung IT-Systeme/Daten 11
Anlage 3 Auszug Hausrundschreiben Anwendungspflicht (DSGVO) 12

Präambel

Erfolgreiche Forschung, Lehre und Verwaltung ist auf zuverlässige Prozesse und sichere Informationstechnik (IT) angewiesen. Die Bedrohungen für die Universität und die Fakultät für Linguistik und Literaturwissenschaft wachsen und die IT wird verletzlicher für Angriffe auf ihre digitale Infrastruktur. Die Richtlinie soll daher dazu beitragen, die Sicherheit der IT-Landschaft der Fakultät für Linguistik und Literaturwissenschaft zu erhöhen und zu gewährleisten.

§1 Grundsätze, Rechte und Pflichten

(1) Im Rahmen der dienstlichen Tätigkeiten gelten grundsätzlich die Richtlinien und Leitlinien der Universität in der jeweils geltenden Fassung. Diese maßgeblichen Vorgaben finden sich unter www.uni-bielefeld.de/datenschutz sowie www.uni-bielefeld.de/informationssicherheit.

(2) Die grundsätzliche Verantwortlichkeit für die IT-Sicherheit bei Bereitstellung und Betrieb der IT-Geräte und -Dienste der Fakultät obliegt der Fakultätsleitung.

(3) Darüber hinaus tragen alle Nutzer*innen/Anwender*innen die Verantwortung für ihre dienstlichen Tätigkeiten, insbesondere für die Einhaltung der Datenschutzbestimmungen und die Informationssicherheit. Die AG- und Bereichsleitungen tragen die Verantwortung, die Mitglieder und Angehörigen ihres nachgeordneten Bereichs im Rahmen der jährlichen IT-Sicherheitsunterweisung auf die geltenden Regelungen hinzuweisen und für diese zu sensibilisieren.

(4) Zudem sind von allen Mitgliedern und Angehörigen der Fakultät für Linguistik und Literaturwissenschaft die im Folgenden festgelegten Regelungen zu beachten und zu befolgen.

(5) Im Konfliktfall gelten zentrale Regelungen vorrangig. Wie die unter (1) genannten Regelungen zum Datenschutz und Informationssicherheit sowie die IT-Benutzungsordnung des BITS. **BITS - Benutzungsordnung - Universität Bielefeld**

§2 Geltungsbereich

(1) Der Geltungsbereich der Richtlinie umfasst die IT-Geräte und -Dienste, die seitens der Fakultät für Linguistik und Literaturwissenschaft betrieben und angeboten werden. Im Folgenden gilt für „IT-Geräte und -Dienste“ stets, dass hiermit ausschließlich IT-Geräte und -Dienste der Fakultät gemeint sind.

(2) Für IT-Geräte und -Dienste, die zentral seitens der Universität Bielefeld (bspw. durch das BITS) betrieben und angeboten werden, gelten die jeweils aktuellen zentralen Regelungen und Richtlinien.

§3 Verantwortlichkeiten für IT-Geräte/-Dienste (Geräteklassen)

(1) Zur Umsetzung der Datenschutzbestimmungen und der Informationssicherheit werden folgende Geräteklassen für IT-Geräte/-Dienste sowie Zuständigkeiten und Verantwortung der Fakultätsleitung und der Arbeitsgruppenleitungen festgelegt. Jegliche dienstlich beschafften Geräte sind grundsätzlich als Geräteklasse Nr. 1 oder Nr. 2 oder, in begründete Ausnahmefälle als Geräteklasse Nr.3 oder Nr. 4 zu betreiben.

Geräteklassen:

Nr. 1) Dienstliche IT-Geräte und -Dienste der Fakultät im vollwertigen IT-Service

Für dienstliche IT-Geräte/-Dienste die zentral installiert und gemanagt werden, wird seitens des Teams IT-Services das vollumfängliche Management übernommen.

Nr. 2) Dienstliche IT-Geräte und Dienste der Fakultät im teilweisen IT-Service

Für IT-Geräte/-Dienste, die aus technischen oder organisatorischen Gründen nur teilweise durch das Team IT-Services gemanagt werden, obliegt für die seitens der Teams IT-Services übernommenen Services die Verantwortlichkeit für die Geräte/Dienste bei der Fakultätsleitung.

Für alle weiteren Teile der IT-Geräte/-Dienste, Installationen und Konfigurationen, die nicht im Management des Teams IT-Services liegen, obliegt die Verantwortlichkeit für Bereitstellung und Betrieb der zuständigen Arbeitsgruppenleitung.

Nr. 3) Dienstliche IT-Geräte und Dienste der Fakultät außerhalb des IT-Services

Für IT-Geräte sowie Dienste, die in **begründeten Ausnahmefällen** außerhalb der IT-Services betrieben werden, obliegt jegliche Verantwortlichkeit der zuständigen Arbeitsgruppenleitung.

Geräte ohne aktuelles und „sicheres“ Betriebssystem **oder** ohne geprüfte BSI-Konfiguration (mind. Basisschutz) dürfen grundsätzlich nicht auf IT-Dienste/-Anwendungen zugreifen, insbesondere auf Dienste/Daten mit min. hohem Schutzbedarf. Diese als unsicher zu betrachtenden Geräte dürfen nicht mit dem Campus-Netzwerk verbunden werden.

Nr. 4) Private IT-Geräte

Der Zugriff auf IT-Dienste und Daten- und Netzwerkinfrastruktur der Fakultät mit privaten IT-Geräten

ist nicht zulässig. In besonderen Ausnahmefällen und nach Prüfung durch das Team IT-Service kann private Hardware verwendet werden. Voraussetzung dafür ist ein aktueller Virenscanner und die Installation aktueller Sicherheitspatches. Für Externe, Gäste etc. können **je nach Verfügbarkeit** Geräte und Ausstattung leihweise über den IT-Service der Fakultät zur Verfügung gestellt werden, siehe § 7 Abs. 5. Für den Zugriff auf zentrale IT-Dienste der Universität gilt § 2 Abs. 2. in diesem Dokument.

(2) Die Verantwortlichkeit umfasst im Wesentlichen:

Nr. 1) Umsetzung der BSI-Vorgaben, v.a. für die Geräteklassen Nr. 1 und Nr. 2

Nr. 2) Installation von aktueller Systemsoftware, Einrichtung eines aktiven, aktuellen Virenschutzes und ggf. aktiver Absicherung mit „Personal Firewall“

Nr. 3) Prüffähige Dokumentation und Inventarisierung der betriebenen IT-Geräte und -Dienste

§4 Verarbeitung dienstlicher Daten, Zugriff auf IT-Dienste und Daten- und Netzwerkinfrastruktur

(1) Der Zugriff auf Daten und IT-Dienste ist nur jenen Nutzer*innen gestattet, die eine Zulassung und Nutzungserlaubnis des BITS haben. Vgl. § 3 der BITS-Benutzungsordnung.

(2) Dienstliche Daten sind jegliche Daten, die im Rahmen einer dienstlichen Tätigkeit erstellt oder verarbeitet werden. Insbesondere sind auch Forschungsdaten dienstliche Daten.

(3) Für die Verarbeitung von dienstlichen Daten sind dienstliche IT-Geräte und IT-Dienste (Hard- und Software) der Universität Bielefeld zu nutzen.

§5 Rechte und Pflichten des BITS und der dezentralen Admins

(1) Die Mitarbeitenden des BITS haben nach der allg. Benutzungsordnung §6 die Möglichkeit, bei Störungen Nutzungserlaubnisse und Rechte temporär einzuschränken, die Sicherheit von Passwörtern zu überprüfen und die Möglichkeit zur technischen Fehlersuche in diverse Logfiles zu schauen. Dies geschieht nach Maßgabe der gesetzlichen Bestimmungen, das BITS ist zur Wahrung des Telekommunikations- und Datengeheimnisses und zur Einhaltung der einschlägigen datenschutzrechtlichen Vorschriften, insbesondere der DSGVO und des Datenschutzgesetzes NRW verpflichtet.

(2) Vergleichbares gilt für die dezentralen Administratoren (Team IT-Service) der Fakultät für Linguistik und Literaturwissenschaft. Auch ihnen ist es im begrenzten Umfang möglich, Nutzer*innen Konten zu sperren, Passwortänderungen anzustoßen/durchzuführen und auch in verschiedene Logfiles Einsicht zu nehmen.

(3) Vgl. hierzu § 6 der **BITS - Benutzungsordnung - Universität Bielefeld**

§6 Sicherheitsmaßnahmen

(1) IT-Geräte (Laptop, Tablet, Smartphone, USB-Sticks etc.) und IT-Dienste sind gegen unbefugte Kenntnisnahme zu schützen. Hierfür sind mindestens folgende Sicherheitsmaßnahmen umzusetzen:

Nr. 1) Schützen Sie Ihre IT-Geräte vor unbefugtem Zugriff durch sichere Passwörter, Biometrie (Fingerabdruck, Gesichtserkennung etc.) oder ähnliche Funktionen.

Nr. 2) Sperren Sie die Geräte regelmäßig, wenn sie den Arbeitsplatz (auch nur kurz) verlassen.

Nr. 3) Um Diebstählen vorzubeugen, lagern Sie insbesondere mobile IT-Geräte sicher (z.B. in einem abgeschlossenen Schrank) oder nutzen Sie bspw. Laptopschlösser.

Nr. 4) Die Weitergabe von persönlichen Passwörtern sowie das Arbeiten mit den Zugangsdaten anderer Personen ist verboten. Auch Gruppenaccounts sind zu vermeiden.

Nr. 5) Zur Vermeidung des unbefugten Datenzugriffs im Falle eines Diebstahls müssen Verschlüsselungsmöglichkeiten für Datenträger genutzt werden, dies gilt im Besonderen für mobile Endgeräte, externe Festplatten und USB-Sticks etc.

(2) Eine Nutzung von dienstlichen IT-Geräten und IT-Diensten durch unbefugte dritte Personen (bspw. im Haushalt lebende Personen wie Partner*innen/Kinder) ist ausdrücklich verboten.

§7 Nutzung von Cloud-Diensten und KI-Systemen

(1) Zweck und Geltungsbereich

Diese Regelungen konkretisieren die Nutzung von Cloud-Diensten und KI-Systemen im Rahmen der IT-Richtlinie der Fakultät für Linguistik und Literaturwissenschaft.

Sie gelten für alle Mitarbeitenden der Fakultät ohne Unterscheidung von wissenschaftlich und nicht-wissenschaftlich Mitarbeitenden.

Ziel ist es, die Nutzung moderner digitaler Werkzeuge zu ermöglichen und zugleich die Einhaltung datenschutz-, sicherheits- und hochschulrechtlicher Vorgaben sicherzustellen.

(2) Rechtsgrundlagen

Die Nutzung von Cloud-Diensten und KI-Systemen erfolgt insbesondere auf Grundlage:

- der Datenschutz-Grundverordnung (DSGVO),
- des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW),
- des Hochschulgesetzes Nordrhein-Westfalen (HG NRW),
- der jeweils geltenden IT-Sicherheits- und Datenschutzrichtlinien der Universität Bielefeld

(3) Grundsätze der Nutzung

Die Nutzung von Cloud-Diensten und KI-Systemen ist nur zulässig, sofern:

- sie dienstlichen Zwecken dient und
- die Datenverarbeitung ausschließlich innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums erfolgt oder wenn für das jeweilige Drittland ein Angemessenheitsbeschluss der EU-Kommission gemäß Art. 45 DSGVO besteht.
- Die Nutzung von Cloud-Diensten oder KI-Systemen in Drittstaaten ohne Angemessenheitsbeschluss ist unzulässig, auch wenn andere geeignete Garantien gemäß Art. 46 DSGVO vorgesehen sind, sofern keine ausdrückliche Freigabe durch die Universität Bielefeld erfolgt,

- keine schutzbedürftigen oder vertraulichen Daten entgegen dieser Ordnung verarbeitet werden.

Die Verantwortung für die rechtmäßige Nutzung verbleibt stets bei der nutzenden Person.
Eine pauschale Übertragung dienstlicher Daten in externe Systeme ist unzulässig.

(4) Nutzung von Cloud-Diensten

Cloud-Dienste dürfen für dienstliche Zwecke nur genutzt werden, wenn:

- sie von der Universität freigegeben sind oder
- ausschließlich öffentlich zugängliche bzw. nicht schutzbedürftige Informationen verarbeitet werden.

Die Nutzung privater Cloud-Speicher für dienstliche Daten ist unzulässig.

Personenbezogene Daten dürfen nur dann in Cloud-Diensten verarbeitet werden, wenn:

- ein Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO besteht,
- der Dienst datenschutzrechtlich geprüft und freigegeben wurde.

(5) Nutzung von KI-Systemen

KI-Systeme dürfen als unterstützende Werkzeuge in Lehre, Forschung und Verwaltung eingesetzt werden.
KI-Systeme ersetzen nicht die fachliche, wissenschaftliche oder rechtliche Verantwortung der nutzenden Person.
Ergebnisse von KI-Systemen sind kritisch zu prüfen und dürfen nicht ungeprüft übernommen werden.

(6) Verbotene Datenverarbeitung in KI-Systemen

Die Eingabe oder Verarbeitung folgender Daten in nicht ausdrücklich freigegebenen KI-Systemen ist untersagt:

- personenbezogene Daten von Studierenden, Mitarbeitenden oder Dritten
- Prüfungsleistungen und Prüfungsunterlagen
- Forschungsdaten mit Personenbezug
- unveröffentlichte wissenschaftliche Ergebnisse
- vertrauliche Verwaltungs- und Personalinformationen
- Zugangsdaten, Passwörter, Zertifikatschlüssel oder interne Systeminformationen

(7) IT-Sicherheit

Cloud- und KI-Dienste dürfen nur über dienstliche Benutzerkonten genutzt werden.
Private Benutzerkonten sind für dienstliche Zwecke unzulässig.
Sicherheitsmaßnahmen wie Multi-Faktor-Authentifizierung sind zu nutzen, sofern verfügbar.
Der Einsatz nicht freigegebener Browser-Erweiterungen oder externer Plugins ist untersagt.

Weitergehende zentrale Regelungen der Universität Bielefeld bleiben unberührt.

§8 Bereitstellung und Finanzierung von IT-Ausstattung

(1) Die zur Erbringung der dienstlichen Aufgaben notwendigen IT-Geräte, IT-Dienste und weitere EDV-Ausstattung sind allen Mitarbeiter*innen (inkl. Hilfskräften) **seitens des Bereiches und der Bereichsleitung zur Verfügung zu stellen**.

(2) Die **Finanzierung** der notwendigen Ausstattung erfolgt grundsätzlich **aus dem Budget der jeweiligen Professur oder Arbeitsgruppe**.

(3) Grundsätzlich sind bei der Beschaffung von IT-Geräten und Diensten (PCs, Laptops, Tablets, Telefone/Smartphones, Monitore, Drucker, Konferenzsysteme) die bestehenden Rahmenverträge der Universität Bielefeld zu nutzen, sofern keine gewichtigen Gründe dagegensprechen.

(4) Beschaffungen von IT-Geräten und Diensten außerhalb bestehender Rahmenverträge oder anderer Geräte, die im Betrieb einen Netzanschluss benötigen, sind **im Vorlauf des Beschaffungsprozesses** mit dem Team IT-Service abzustimmen.

(5) Sofern weitere Personen (**Studierende, Stipendiaten, Gäste**) dienstliche Daten verarbeiten, sind diesen ebenfalls dienstliche Geräte, Ausstattung und Dienste zur Verfügung zu stellen. Hierfür können **je nach Verfügbarkeit** Geräte und Ausstattung über den IT-Service der Fakultät ausgeliehen werden. Das Team IT-Services kann in begründeten Fällen Gäste-Zugänge einrichten.

(6) Vor der Beschaffung und Nutzung neuer IT-Dienste / IT-Verfahren und Projekten ist in Abstimmung mit dem DISK ein VVT/TOM, eine Schutzbedarfsfeststellung zu erstellen und ggf. eine Risikoanalyse durchzuführen. Die Ergebnisse sind wie auch die getroffenen Sicherheitsmaßnahmen von den zuständigen Verfahrensverantwortlichen zu dokumentieren und einer regelmäßigen Revision zu unterziehen. Die DISKs der Fakultät stehen hier beratend zur Seite, dass Ausfüllen der Dokumente obliegt den Verantwortlichen.

§9 Ansprechperson für IT-Angelegenheiten

(1) Für jedes Studienfach wird von der zuständigen Bereichsleitung eine Person als Ansprechpartner für IT-Angelegenheiten benannt.

(2) Die IT-Ansprechpersonen sind Ansprechpartner für alle IT-Belange des Bereiches insbesondere bei Beschaffung und Einführung neuer IT-Geräte und IT-Dienste.

(3) Die Ansprechpersonen unterstützen die Arbeitsgruppenleitung, v.a. in der Umsetzung sowie der lfd. Aktualisierung einer angemessenen und prüffähigen Dokumentation und Inventarisierung der in der AG betriebenen IT-Geräte und -Dienste nach §3 (2) Nr. 2.

§10 IT-Notfall / Incident Management

(1) Die Regelungen für IT-Notfälle sind im Geschäftsfortführungsplans der Fakultät in der jeweiligen aktuellen Fassung geregelt und sind verbindlich von allen Mitarbeitenden im Rahmen eines IT-Notfalls einzuhalten.

(2) Bei einer Datenpanne durch einen Informationssicherheitsvorfall muss der Vorfall selbstständig über folgendes Formular gemeldet werden:

https://www.uni-bielefeld.de/verwaltung/datenschutz/formulare-gesetze/datenpanne.xml

Diese Meldung sollte so schnell wie möglich nach Bekanntwerden des Vorfalls geschehen, das Zeitfenster beträgt maximal 72h.
Das Onlineformular sollte so detailliert wie möglich ausgefüllt werden.
Aus diesen Informationen wird ein Ticket beim ServiceDesk erstellt, dass auch die zentralen Stellen in der Universität über den Vorfall informiert.

(3) Ein IT-Sicherheitsvorfall ist jedes Ereignis, das die Sicherheit von Daten, Netzwerken oder Systemen gefährdet. Solche Vorfälle können verschiedene Ursachen haben, zum Beispiel technische Fehler, Angriffe oder menschliches Versagen. Es ist wichtig, schnell zu reagieren, um die Auswirkungen so klein wie möglich zu halten. Informieren Sie unverzüglich das Team IT-Service der LiLi über den Vorfall und befolgen Sie deren Anweisungen.

§11 Inkrafttreten

Diese Richtlinie tritt am Tag nach Veröffentlichung im Intranet der Fakultät für Linguistik und Literaturwissenschaft in Kraft.

gez. Friederike Kern
Dekanin der Fakultät für Linguistik und Literaturwissenschaft

Ansprechpersonen

Bereich	**Kontakt**
Stabsstelle Informationssicherheit	informationssicherheit@uni-bielefeld.de oder -3032
Behördliche Datenschutzbeauftragte	datenschutzbeauftragte@uni-bielefeld.de oder -5225
Team IT-Services	IT Support LiLi oder -3643, -5268 PEVZ
Datenschutz- und Informationssicherheits-koordinator*in der Fakultät (DISK)	PEVZ
IKM-Verantwortliche	PEVZ

Anlage 1 Glossar

Begriff	Definition / Erläuterung
Basisschutz	Mindestanforderungen an IT-Sicherheit, die durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert werden; z. B. sichere Konfiguration, aktuelle Software, Virenschutz.
BITS	Bielefelder IT-Servicezentrum (zentrale IT-Einrichtung der Universität Bielefeld).
BSI-Konfiguration	IT-Sicherheitskonfiguration, die den Vorgaben des BSI-Grundschutzes entspricht.
Datenschutzbestimmungen / Datenschutzrecht	Gesamtheit der rechtlichen Regelungen zum Schutz personenbezogener Daten, insbesondere DSGVO, Landesdatenschutzgesetz NRW und interne Datenschutzrichtlinien der Universität.
Dienstliche Daten	Alle Daten, die im Rahmen dienstlicher oder wissenschaftlicher Tätigkeiten entstehen oder verarbeitet werden, insbesondere Forschungs-, Verwaltungs- und Lehrdaten.
Dienstliche IT-Geräte/-Dienste	Von der Universität oder Fakultät bereitgestellte Hardware, Software und Netzressourcen, die für dienstliche Zwecke bestimmt sind.
DISK (Datenschutz- und Informationssicherheitskoordinator*in)	Fakultätsinterne Koordinationsstelle für Datenschutz und Informationssicherheit; Schnittstelle zur zentralen Stabsstelle Informationssicherheit.
Firewall-Hardware	Physische oder virtuelle Netzkomponente zur Kontrolle und Filterung von Datenverkehr zwischen Netzwerken.
Geräteklasse	Zuordnung von IT-Geräten und -Diensten zu definierten Service- und Verantwortlichkeitsstufen (Klassen 1–4) gemäß § 3 der Richtlinie.
Informationssicherheit	Schutz von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und IT-Systemen.
IT-Dienste	Anwendungen, Serverdienste, Netzwerke, Cloud- oder Kommunikationsdienste, die zur dienstlichen Aufgabenerfüllung bereitgestellt werden.
IT-Geräte	Rechner, Laptops, Tablets, Smartphones, Server, Speichersysteme und vergleichbare elektronische Geräte inkl. Betriebssystem
IT-Notfall	Ereignis, das wesentliche IT-Systeme oder Daten gefährdet oder außer Betrieb setzt und besondere Maßnahmen gemäß IT-Geschäftsfortführungsplan erfordert.
IT-Verfahren	Organisatorisch oder technisch definierte Abläufe, bei denen IT-Systeme Daten verarbeiten (z. B. Datenbanken, Forschungsplattformen).
Netzwerkinfrastruktur	Gesamtheit der physischen und logischen Komponenten (z. B. Switches, Router, WLAN), die den Datenaustausch innerhalb der Fakultät und zur Universität ermöglichen.
PEVZ	Personen- und Einrichtungsverzeichnis der Universität Bielefeld; dient der Veröffentlichung von Zuständigkeiten und Kontaktdaten.

Persönliche Unversehrtheit	Schutz von Leben, Gesundheit und körperlicher Sicherheit von Personen. Relevant bei IT-Ausfällen mit sicherheitskritischen Folgen.
Prüffähige Dokumentation	Vollständige und nachvollziehbare Aufzeichnung aller IT-Systeme, Konfigurationen, Verantwortlichkeiten und Sicherheitsmaßnahmen.
Schutzbedarf / Schutzbedarfsfeststellung	Bewertung des erforderlichen Schutzniveaus von Daten oder IT-Systemen (normal, hoch, sehr hoch) in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit.
Verfahrensverantwortliche*r	Person, die für den Betrieb und die Sicherheit eines IT-Verfahrens oder einer Anwendung verantwortlich ist.
Vertraulichkeit	Eigenschaft von Informationen, nur autorisierten Personen zugänglich zu sein.
Verfügbarkeit	Fähigkeit eines IT-Systems oder Dienstes, bei Bedarf zuverlässig nutzbar zu sein.
Integrität	Unversehrtheit und Korrektheit von Daten und Systemen; Schutz vor unbefugter Veränderung.
Zugriff	Möglichkeit, auf Daten oder IT-Dienste zuzugreifen, sie zu lesen, zu verändern oder zu löschen; umfasst auch die Netzverbindung.

Anlage 2 Matrix Schutzbedarfsfeststellung IT-Systeme/Daten“

Beeinträchtigung (Kategorie)	Bedrohung	Folgen des Schadens		
1. Beeinträchtigung der Aufgabenerfüllung	Unbefugte Einsicht in Daten (Verlust von Vertraulichkeit) Manipulation der Daten (Verlust von Integrität) Verlust der Daten (Verlust von Verfügbarkeit)	Für alle Benutzer des Systems tolerierbar ...führt maximal zum Ausfall einzelner Arbeitsabläufe (tolerierbare Ausfallzeit mehr als einen Arbeitstag).	Für einzelne Benutzer des Systems nicht tolerierbar ...schränkt die Aufgabenerfüllung in einem Teilbereich ein (tolerierbare Ausfallzeit zwischen einer und 24 Stunden).	Für alle Benutzer des Systems nicht tolerierbar ...gefährdet den Gesamtauftrag der Universität (tolerierbare Ausfallzeit weniger als eine Stunde).
2. Negative Innen-und/oder Außenwirkung	Unbefugte Einsicht in Daten Manipulation der Daten Verlust der Daten	**Geringer** Ansehens- und Vertrauensverlust eines Teilbereichs der Universität	Ansehens- und Vertrauensverlust der Universität bei einer **eingeschränkten** Öffentlichkeit oder Hoher Ansehensverlust eines Teilbereichs der Universität	**Landesweiter** Ansehens und Vertrauensverlust der Universität in der **breiten** Öffentlichkeit
3. Finanzielle Auswirkungen	Unbefugte Einsicht in Daten Manipulation der Daten Verlust der Daten	Finanzieller Schaden weniger als ca. 150.000€	Finanzieller Schaden weniger als ca. 3 Millionen €	Finanzieller Schaden mehr als ca. 3 Millionen €
4. Beeinträchtigung der persönlichen Unversehrtheit	Unbefugte Einsicht in Daten Manipulation der Daten Verlust der Daten	...erscheint nicht möglich	...kann nicht absolut ausgeschlossen werden	Gravierende Auswirkungen sind möglich (Gefahr für Leib und Leben).
5. Verstoß gegen Gesetze, Vorschriften und/oder Verträge	Unbefugte Einsicht in Daten Manipulation der Daten Verlust der Daten	...verstößt gegen Gesetze oder Vorschriften mit **geringen** Konsequenzen ...hat geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen zur Folge.	...verstößt gegen Gesetze oder Vorschriften mit **erheblichen** Konsequenzen. ...hat Vertragsverletzungen mit hohen Konventionalstrafen und/oder erheblichen Haftungsschäden zur Folge.	...verstößt **fundamental** gegen Gesetze oder Vorschriften ...hat Vertragsverletzungen zur Folge, deren Haftungsschäden für die UniBi ruinös sind.
Notwendiger Schutzbedarf:		**normal**	**hoch**	**sehr hoch**

Anlage 3 Auszug Hausrundschreiben Anwendungspflicht (DSGVO)

Gesamtverantwortung und Verantwortung von Prozesseigentümern sowie Linienverantwortlichen

Die datenschutzrechtlich Verantwortliche für administrative Verarbeitungstätigkeiten ist die Universitätsleitung. Das Rektorat trägt die Gesamtverantwortung für die Einhaltung des Datenschutzes.

Ungeachtet der Gesamtverantwortung der Hochschulleitung ist der Datenschutz ein integraler Bestandteil der jeweiligen Fachaufgabe. Somit trägt jede **Führungskraft**, ausgehend von der fachlichen Verantwortung, die datenschutzrechtliche Verantwortung für ihren Geschäftsbereich.

Das bedeutet, dass **Prozesseigentümer*innen und Linienverantwortliche** die datenschutzrechtlichen Anforderungen in ihrem Geschäftsbereich beachten, und umsetzen.

In den **Fakultäten** und allen weiteren Einrichtungen **liegt die Verantwortung bei den Dekaninnen und Dekanen**, die durch die Fakultätsverwaltungsleitung unterstützt werden, bzw. bei den entsprechenden dezentralen Einrichtungsleitungen.

Die Umsetzung der datenschutzrechtlichen Vorgaben kann von den Führungskräften auch auf Mitarbeiter*innen übertragen werden, sofern diese das entsprechende Fachwissen haben. Die Führungskraft behält in diesem Fall weiterhin die Organisations- und Kontrollverantwortung, das heißt, sie stellt sicher, dass die verantwortliche Person das erforderliche Wissen besitzt und die datenschutzrechtlichen Aufgaben verantwortungsvoll und in der erforderlichen Art und Weise wahrnimmt.

II. Verantwortung der Beschäftigten

Beschäftigte ohne Führungs- oder Fachverantwortlichkeit beachten in ihrem jeweiligen Aufgabengebiet die Regelungen des Datenschutzes. Sie nehmen die künftig angebotenen Informations- und Schulungsangebote wahr und verarbeiten die ihnen zugänglichen personenbezogenen Daten nur im Rahmen der ihnen übertragenen Aufgaben. Insbesondere achten sie darauf, dass nur Berechtigte auf die von ihnen verwalteten personenbezogenen Daten Zugriff haben. Sie haben Verstöße gegen die Datenschutzleitlinie oder anderer Vorschriften zum Schutz personenbezogener Daten unverzüglich der oder dem Vorgesetzten mitzuteilen.

III. Verantwortung im Bereich der Lehre

Die Wahrung des Datenschutzes für Verarbeitungstätigkeiten im Rahmen von Studien- und Prüfungsleistungen obliegt abseits der Aufgabenerfüllung der Universität den Studierenden selbst und der oder dem verantwortlichen Lehrenden (Betreuerin oder Betreuer). Wenn im Rahmen von Studien- und Prüfungsleistungen von Studierenden Leistungen erbracht werden, bei denen personenbezogene Daten verarbeitet werden, so sind die Studierenden grundsätzlich selbst für die Wahrung des Datenschutzes verantwortlich. Betroffen sind beispielsweise solche Fallgestaltungen, bei denen Studierenden für eine Bachelor- oder Masterarbeit Befragungen durchführen und in diesem Kontext personenbezogene Daten erheben und verarbeiten. Lehrende müssen bei der Betreuung der bzw. des Studierenden gewährleisten, dass die Erbringung der Studien- und Prüfungsleistung möglich ist, ohne datenschutzrechtliche Vorschriften zu verletzen und die Studierenden diesbezüglich informieren und begleiten.

IV. Verantwortung im Bereich der wissenschaftlichen Forschung

Die Wahrung des Datenschutzrechts für Verarbeitungstätigkeiten im Rahmen von Forschungsvorhaben obliegt der Person, die – in Ausübung der wissenschaftlichen Freiheit – in dem Forschungsvorhaben die Projektleitung bekleidet.

V. Verantwortung der Studierendenschaft

Abseits der rechtlichen Aufgabenerfüllung der Universität trägt die Universität für die Studierenden und deren Umgang mit personenbezogenen Daten keine datenschutzrechtliche Verantwortlichkeit. Hier hat die Universitätsleitung die Rechtsaufsicht und muss die Studierendenschaft auffordern, die Prozessverantwortung zu klären und auszuüben