Dienstanweisung zum Datenschutz und zur Informationssicherheit in der mobilen Arbeit und Telearbeit

vom 31.01.2023

Die Carl von Ossietzky Universität Oldenburg, vertreten durch das Präsidium, - im Folgenden „Dienststelle“ genannt – hat gemäß § 37 NHG am 31.01.2023 die folgende Dienstanweisung beschlossen:

1. Anwendungsbereich

Mit dieser Dienstanweisung werden der Datenschutz und die Informationssicherheit in der mobilen Arbeit und der Telearbeit geregelt. Die Kenntnisnahme und Beachtung dieser Dienstanweisung sind gem. Ziff. 12 der Dienstvereinbarung über die mobile Arbeit und Telearbeit vom 11.01.2023 Voraussetzung für die Teilnahme an der mobilen Arbeit und Telearbeit.

2. Grundsätzliche Vorgaben

(1) Werden in mobiler Arbeit oder Telearbeit personenbezogene Daten verarbeitet, ist die Arbeitsorganisation am mobilen Arbeitsplatz oder Telearbeitsplatz so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die geeignet sind,

a) Unbefugten den Zutritt zu dienstlichen Geräten, an dem personenbezogene Daten verarbeitet werden, zu verwehren (Zutrittskontrolle),
b) zu verhindern, dass der häusliche oder mobile Arbeitsplatz von Unbefugten genutzt wird (Zugangskontrolle),
c) zu gewährleisten, dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden (Zugriffskontrolle), sowie
d) zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten erfolgt (Weitergabekontrolle).

(2) Bei Datenschutzverstößen oder Sicherheitsvorfällen ist unverzüglich die Stabsstelle Datenschutz- und Informationssicherheitsmanagement zu informieren. Die an der Universität Oldenburg etablierten Prozesse gelten auch im Rahmen des Arbeitens in mobiler Arbeit und Telearbeit.

(3) Die Stabsstelle Datenschutz- und Informationssicherheitsmanagement (DISM) und der Datenschutzbeauftragte stehen für Beratungen zur Verfügung.

3. Schutzbedarfsfeststellung

(1) Vor Aufnahme der Tätigkeit ist mit der*dem Vorgesetzten der Schutzbedarf der zu bearbeitenden personenbezogenen Daten nach dem Schutzstufenkonzept der Landesbeauftragten für den Datenschutz Niedersachsen zu bestimmen. Etwaige Geheimhaltungsvereinbarungen sind in die Schutzbedarfsfeststellung einzubeziehen.

(2) Je höher der Schutzbedarf der zu bearbeitenden Daten eingestuft wird, desto höher sind die zu ergreifenden Datensicherheitsmaßnahmen.

(3) Daten der Schutzstufe E des Schutzstufenkonzepts der Landesbeauftragten für den Datenschutz Niedersachsen dürfen weder in mobiler Arbeit noch in der Telearbeit verarbeitet werden.

(4) Beispiele von Datenkategorien und deren Schutzbedarf sind in Anlage 1 aufgeführt, und für die Bewertung des konkreten Schutzbedarfs heranzuziehen.

4. Arbeitsplatzumgebung

(1) Die Arbeitsplatzumgebung ist gemessen an den auszuführenden Tätigkeiten so auszugestalten, dass vom Grundsatz her die Vertraulichkeit und Verfügbarkeit der Daten wie am Arbeitsplatz am Dienstort sichergestellt ist.

(2) Dies bedeutet insbesondere, dass

a) unbefugte Dritte durch Auswahl des Arbeitsortes und ggf. Einrichtung des Arbeitsplatzes keinen Blick auf den Bildschirm und in die Papierunterlagen werfen können,
b) Sichtschutzfolien angeboten werden, wenn dies erforderlich ist,
c) eine Clean-Desk-Policy gilt, die festlegt, dass beim Verlassen des Arbeitsplatzes grundsätzlich alle Unterlagen sicher verschlossen werden und vor unberechtigtem Zugriff geschützt werden müssen,
d) Papierunterlagen in Dokumentenmappen oder Schränken verschlossen werden können,
e) Fenster bei Verlassen des Arbeitsplatzes grundsätzlich geschlossen werden,
f) beim Verlassen des Arbeitsplatzes die Endgeräte zu sperren sind (Bildschirmsperre),
g) darauf zu achten ist, dass vertrauliche Gespräche (z. B. Telefongespräche, Videokonferenzen) nicht von unbefugten Personen oder Sprachassistenten (z. B. Alexa, Siri) mitgehört werden.

5. Genutzte Hardware

(1) Die genutzte Hard- und Software ist (soweit sie nicht ohnehin durch die universitären Zugangsdaten geschützt ist) durch angemessene Zugangsdaten zu schützen. Passwörter und Zugangsdaten dürfen unter keinen Umständen an Dritte (hierzu gehören auch Haushaltsangehörige und Gäste) weitergegeben werden.

(2) Beim Transport der Hardware oder Nutzung dieser im öffentlichen Raum ist diese angemessen gegen Diebstahl und unbefugte Einsichtnahme zu schützen.

(3) Bei der Verwendung privater Telefone sind deren Anruflisten regelmäßig zu löschen.

Grundsätzlich ist nur die Verwendung universitätseigener Systeme gestattet. Bei ausnahmsweiser Verwendung fremder IT-Systeme muss sichergestellt werden, dass alle Informationen, inklusive temporärer Daten, nach Beendigung der jeweiligen Tätigkeit von den Geräten gelöscht werden.

6. Umgang mit Papierdokumenten

(1) Beim Umgang und insbesondere während des Transportes von Papierdokumenten besteht ein erhöhtes Verlustrisiko und damit verbunden das Risiko eines meldepflichtigen Datenschutzvorfalls. Es dürfen daher nur die zwingend für die dienstliche Aufgabenerfüllung erforderlichen Dokumente außerhalb der Dienststelle transportiert werden. Diese sind in geeigneten Behältnissen (mit Namen der Organisationseinheit im Falle eines Verlustes) zu transportieren.

(2) Akten sind vor Mitnahme auszutragen.

(3) Beim Transport dürfen Papierdokumente nicht unbeaufsichtigt im öffentlichen Raum bleiben und sind so zu schützen, dass Dritte keine Einsicht nehmen können.

(4) Daten der Schutzstufe D sollen grundsätzlich nicht in Papierform im Homeoffice und während der mobilen Arbeit verarbeitet werden. Dies gilt insbesondere auch für Personalaktendaten oder Dokumente mit einer Vielzahl von Daten der Schutzstufe D.

(5) Soweit möglich, soll nicht mit den Originaldokumenten, sondern mit Kopien gearbeitet werden.

(6) Eine Entsorgung erfolgt nur über die Entsorgungsstrukturen der Universität Oldenburg (Datenentsorgungsbehälter), im Ausnahmefall über geeignete Aktenvernichter, die mindestens der Sicherheitsstufe 4 (vgl. DIN 66399) entsprechen.

7. Datenverarbeitung

(1) Die Speicherung von Daten hat grundsätzlich auf den üblichen Netzlaufwerken oder den von der Universität Oldenburg zentral zugelassenen Cloud-Speicherdiensten (Cloud-Storage) zu erfolgen. Nur so ist gewährleistet, dass die Daten regelmäßig gesichert werden und Datenverlust vermieden wird.

(2) Ausnahmen hiervon dürfen nur gemacht werden, wenn eine Verbindung zu den Netzlaufwerken oder Cloud-Speicherdiensten der Universität Oldenburg nicht möglich ist oder dienstliche Belange dies nicht zulassen. Die Speicherung auf den Netzlaufwerken oder Cloud-Speicherdiensten der Universität Oldenburg ist unverzüglich nach Wiederherstellung einer Verbindung nachzuholen. Lokale Kopien von personenbezogenen und geheimen Daten sind anschließend zu löschen.

(3) Aufbewahrungs- und Löschfristen gelten auch für die im Homeoffice gelagerten Daten und Dokumente.

8. Inkrafttreten

Die Dienstanweisung tritt zum 01.04.2023 in Kraft.

Anlage 1

Orientierungshilfen zur Einordnung der Schutzstufen nach Schutzstufenkonzept der Landesbeauftragten für den Datenschutz Niedersachsen (LfD)

Tabelle 1 – Schutzstufe A

Schutz-stufe	**Erläuterung der jeweiligen Schutzstufe und welche personenbezogenen Informationen dieser Stufe im Regelfall zugeordnet werden können.**	**Typische Tätigkeiten an der Universität Oldenburg, bei denen im Regelfall Daten der jeweiligen Schutzstufe verarbeitet werden**

A	Schutzstufe A betrifft Daten, die von den Betroffenen frei zugänglich gemacht wurden („Öffentlich zugängliche Daten“). Ebenfalls können dieser Gruppe auch Daten zugeordnet werden, die gar keine personenbezogenen Daten mehr enthalten („Anonyme Daten):
	
	- Angaben zu Personen, die zur Veröffentlichung freigegeben sind:
	  - Kontaktangaben,
	  - Tätigkeitsbereiche,
	  - Publikationen.
	
	- Weitere Personeninformationen, die aufgrund einer Einwilligung veröffentlicht werden dürfen:
	  - Fotos, Video- und Audioaufnahmen,
	  - Lebensläufe, Profilinformationen,
	  - Persönliche Angaben,
	
	- Lehrveranstaltungsbezogene Inhalte, die maximal Angaben zu den Urhebern enthalten:
	  - Vorlesungsverzeichnis,
	  - Vorlesungsmaterialien/Skripte (ggfs. Urheberrechte beachten),
	  - Übungsmaterialen (ggfs. Urheberrechte beachten).
		- Gestaltung und Pflege von Webseiten
		
		- Erstellung universitätsbezogener Dokumente, die keine personenbezogenen Daten (bis auf evtl. Ansprechpersonen) enthalten:
		  - Ordnungen, Satzungen, Dienstvereinbarungen, Vertragsmuster
		  - Rundschreiben, Formulare, Merkblätter
		  - Informationsmaterial
		  - Konzepte
		
		- Entwicklung von Lehr- und Lernkonzepten und Lehrveranstaltungsmaterialen
		
		- Erstellung von Informationsmaterial für die Öffentlichkeitsarbeit (Flyer, Broschüren, Berichte)

Tabelle 2 – Schutzstufe B

Schutz-stufe	Erläuterung der jeweiligen Schutzstufe und welche personenbezogenen Informationen dieser Stufe im Regelfall zugeordnet werden können.	Typische Tätigkeiten an der Universität Oldenburg, bei denen im Regelfall Daten der jeweiligen Schutzstufe verarbeitet werden

B	Schutzstufe B betrifft Daten, deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lässt, die aber von den Betroffenen nicht frei zugänglich gemacht wurden („Intern verfügbare Daten“). Hierbei handelt es sich zumeist um Daten, die nur einem bestimmten Personenkreis verfügbar gemacht werden sollen:
	
	- Dienstliche Daten der Beschäftigten, die die interne Organisation betreffen:
	  - Geschäftsverteilungspläne,
	  - Organigramme, Arbeitsanweisungen,
	  - Post- und E-Mailverteiler,
	  - Zuständigkeiten.
	
	- Interne Kommunikationsdaten:
	  - Adressen,
	  - Durchwahl,
	  - Universitäts-Account.
	
	- Tätigkeitsbezogene Angaben in Protokollen von hochschulöffentlichen Gremiensitzungen
	
	- Kontaktinformationen Dritter (Vertragspartner, Drittmittelgeber, Behörden und ähnlich verbundenen Einrichtungen)
		- Organisation und Abstimmung von Terminen mit internen und externen Einrichtungen
		
		- Fachberatung und Ticketsupport von Nutzenden der internen Systeme und Softwarelösungen, wenn dabei auf keine weiteren Daten der Schutzstufen C, D und E zugegriffen wird
		
		- Entwicklung und Pflege von internen Systemen und Software, wenn dabei auch Daten der Kategorie B verarbeitet werden
		
		- Verwaltung von Gebäuden und Koordinierung von Neu, Umbau- und Sanierungsarbeiten
		
		- Bekanntmachung von Wahlergebnissen
		
		- Einholung von Angeboten
		
		- Bestellvorgänge und Beschaffungen
		
		- Administration des Modulkatalogs

Tabelle 3 – Schutzstufe C

Schutz-stufe	Erläuterung der jeweiligen Schutzstufe und welche personenbezogenen Informationen dieser Stufe im Regelfall zugeordnet werden können.	Typische Tätigkeiten an der Universität Oldenburg, bei denen im Regelfall Daten der jeweiligen Schutzstufe verarbeitet werden

C	Schutzstufe C betrifft Daten, deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen könnte („Ansehen") („Eingeschränkte Daten)":
	
	- Persönliche Daten von Mitarbeitenden/ Studierenden, soweit die Informationen nicht dem Schutzbedarf D oder E zuzuordnen sind:
	  - Private Kontaktinformationen
	  - Kontoinformationen
	  - Stellenbewertung
	  - Tätigkeitsbezogene Informationen (Teilnahme an Sitzungen, Gremien)
	
	- Veranstaltungsbezogene Teilnehmenden-Informationen, wie etwa Anwesenheitslisten oder Kontaktlisten
	
	- Vertragsunterlagen (zu Dritten):
	  - Rechnungen,
	  - Reise- und Lohnabrechnungen,
	  - Drittmittelverträge.
	
	- Benutzernamen und Passwörter
	
	- Forschungsdaten, die noch persönliche Informationen der Teilnehmenden enthalten, die nicht den Schutzstufen D und E zuzuordnen sind.
	
	- Studien- und Prüfungsleistungen einzelner Veranstaltungen
	
	- Prüfungsergebnisse/Ergebnislisten einzelner Prüfungsleistungen
	
	- Individuelle Schließberechtigungen
	
	- Persönliche Angaben in Protokollen von nicht hochschulöffentlichen Gremiensitzungen
	
	- E-Mail und telefonische Kommunikationsinhalte, sofern keine Daten der Schutzstufe D und E ausgetauscht werden
		- Zulassungsverfahren
		
		- Beratung von Studieninteressierten
		
		- Einschreibungsangelegenheiten
		
		- (Nachweise, Zahlungseingänge) Korrektur von Studien- und Prüfungsleistungen
		
		- Betreuung von Veranstaltungen in Stud.IP
		
		- Verwaltung und Kontrolle von Drittmittelprojekten
		
		- Personalkostenverwaltung
		
		- Veranstaltungsorganisation
		
		- Allgemeine Sekretariatsaufgaben, sofern keine sensiblen Daten (beispielsweise besondere Datenkategorien nach Art. 9 DSGVO) betroffen sind
		
		- Nutzung von lesendem SAP-Zugriff, sofern dabei kein Zugriff auf Daten der Schutzstufe D erfolgt
		
		- Betreuung rechtlicher Verfahren (Arbeitnehmererfindungen, BAföG-Angelegenheiten, Zulassungsverfahren), soweit keine Angelegenheiten der Schutzstufe D oder E betroffen sind
		
		- Organisation innerhalb der Einrichtung (Abstimmungen, Zugang zu Dokumenten, Terminkoordination, Fristenüberwachung)
		
		- Beratung und Betreuung von Studierenden zu lehrveranstaltungsbezogenen Themen
		
		- Informationsmanagement und Datenlieferung für Personalkostenbudgetierung, -bewirtschaftung und -planung
		
		- Organisation und Durchführung von Vergabeverfahren
		
		- Organisation und Verwaltung der Schließberechtigungen
		
		- Organisation und Abwicklung von Dienstreisen
		
		- Rechnungswesen

		- Systemadministration von Systemen soweit auf den Systemen keine Daten der Schutzstufe D verarbeitet werden - Ticketbearbeitung im Service-Desk

Tabelle 4 – Schutzstufe D

Schutz-stufe	**Erläuterung der jeweiligen Schutzstufe und welche personenbezogenen Informationen dieser Stufe im Regelfall zugeordnet werden können.**	**Typische Tätigkeiten an der Universität Oldenburg, bei denen im Regelfall Daten der jeweiligen Schutzstufe verarbeitet werden**

D	Schutzstufe D betrifft Daten, deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte („Existenz") („Sensible Daten"):
	
	- Personalunterlagen und Personalakteninhalte (zu Beschäftigten):
	  - Arbeitszeugnisse,
	  - Gesundheitsdaten,
	  - Krankmeldungen,
	  - Sozialdaten,
	  - Abwesenheitszeiten (Urlaub, Krankheit),
	  - Leistungsbewertung,
	  - Bewerbungsunterlagen,
	  - Gutachten im Berufungsverfahren.
	
	- E-Mail und telefonische Kommunikationsinhalte, sofern auch Daten der Schutzstufe D ausgetauscht werden
	
	- Leistungsinformationen über Studierende (z. B. Prüfungsakte, Leistungsübersicht, Abschluss)
	
	- Daten besonderer Kategorien nach Art. 9 DSGVO
	
	- Forschungsergebnisse, sofern sensible Daten betroffen sind
	
	- Daten die der Geheimhaltung unterliegen
		- Personalangelegenheiten
		
		- Nutzung von SAP, soweit dabei auch auf Personalaktendaten zugegriffen wird
		
		- Betreuung rechtlicher Verfahren im Personalwesen oder in Härtefall-Angelegenheiten
		
		- Untersuchungen der Innenrevision
		
		- Berufungs- und Bewerbungsverfahren
		
		- Beratung und Betreuung von Studierenden und Beschäftigten zu physischen und psychischen Belastungen, Härtefällen, usw.
		
		- Strafrechtliche Ermittlungsmaßnahmen
		
		- Systemadministration von Systemen soweit auf den Systemen Daten der Schutzstufe D verarbeitet werden.

Tabelle 5 – Schutzstufe E

Schutz-stufe	**Erläuterung der jeweiligen Schutzstufe und welche personenbezogenen Informationen dieser Stufe im Regelfall zugeordnet werden können.**	**Typische Tätigkeiten an der Universität Oldenburg, bei denen im Regelfall Daten der jeweiligen Schutzstufe verarbeitet werden**
E	Schutzstufe E betrifft Daten, deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen könnte („Hochsensible Daten“): - Forschungsdaten, sofern hochsensible Daten betroffen sind: - z. B. Strafakten, Zeugenschutzprogramme	- Forschungsarbeiten mit Daten aus hochsensiblen Bereichen