Instructions concerning data protection and information security for mobile working and teleworking

from 31.01.2023

The University of Oldenburg, represented by the Presidential Board,- hereinafter referred to as the "University" - and the Staff Council of the University of Oldenburg, represented by the Chairperson, - hereinafter referred to as the "Staff Council" - have concluded the following agreement on 31 January 2023 in accordance with Section 78 of the Lower Saxony Staff Representation Act (NPersVG):

1. Scope

These instructions govern data protection and information security for mobile working and teleworking. Acknowledgement and compliance with these instructions are a requirement for participation in mobile working and teleworking in accordance with No. 12 of the Agreement concerning mobile working and teleworking of 11 January 2023.

2. Basic guidelines

(1) If personal data are processed when mobile working or teleworking, the work organisation of the mobile workstation or teleworking workstation must be arranged in such a way that it meets the special requirements for data protection. In particular measures should be taken that

a) Bar unauthorised persons from accessing university equipment on which personal data are processed (physical access control),
b) Prevent the home office or mobile workstation from being used by unauthorised persons (physical access control),
c) Guarantee that personal data are not read, copied, changed or removed without authorisation while being processed (data access control), and
d) Guarantee that personal data cannot be read, copied, changed or removed without authorisation while being transmitted electronically or during transportation or storage on data carriers, and that it is possible to check and establish the places to which personal data are transmitted (transfer control).

(2) In the event of data privacy breaches or security incidents, the Data Protection and Information Security Unit must be informed immediately. The processes established at the University of Oldenburg also apply in the context of mobile working and teleworking..

(3) The Data Protection and Information Security Unit (DISM) and data protection officer are available to provide advice.

3. Security requirements analysis

(1) Before commencing work, the staff member must consult their superior to determine the security requirements in accordance with the security levels concept of the Data Protection Officer for Lower Saxony for the personal data that they will be processing. Any confidentiality agreements must be incorporated in the security requirements analysis.

(2) The greater the security requirements for the data in question, the stronger the data security measures needed..

(3) Protection level E data from the security levels concept of the Data Protection Officer for Lower Saxony must not be processed either while mobile working or teleworking.

(4) Examples of data categories and their security requirements are given in Annex 1, and should be referred to when assessing the specific security requirements

4. Workingstation environment

(1) The workstation environment must be organised appropriately for the work that has to be done, so that confidentiality and availability of data is always ensured at the place of employment as much as at the workstation

(2) Specifically, this means that

a) the choice of work location and where relevant the organisation of the workstation prevents unauthorised third parties from viewing the screen and paper documents,
b) privacy film is offered where necessary,
c) there is a clean-desk policy stipulating that all documents must be securely locked away and protected from unauthorised access when absent from the workstation,
d) paper documents can be secured in document folders or cupboards,
e) windows are always closed on leaving the workstation,
f) the devices must be locked on leaving the workstation),
g) care is taken that confidential conversations (e.g. telephone calls, video conferences) cannot be overheard by unauthorised persons or virtual assistants (e.g. Alexa, Siri).

5. Hardware use

(1) The hardware and software used must (unless already protected by the university access code) be protected with suitable access codes. Passwords and access codes must not in any circumstances be passed to third parties (this also includes members of the household and guests).

(2) When transporting the hardware or using it in public spaces, it must be suitably protected against theft and unauthorised viewing.

(3) When using private telephones, call lists must be regularly deleted..

Generally, it is only permitted to use the university's own systems. If outside IT systems are used in exceptional circumstances, staff must make sure that all information, including temporary files, is deleted from the devices at the end of the work.

6. Handling paper documents

(1) When using paper documents and in particular during their transportation there is an increased risk of loss and with it the risk of a notifiable data privacy incident. Therefore, documents may only be transported outside the university if they are essential for the fulfilment of official duties. They must be transported in suitable receptacles (with the name of the organisational unit in the event of loss).

(2) Files must be signed out before removal.

(3) During transport, paper documents must not be left unattended in public spaces and must be protected in such a way that third parties cannot inspect them..

(4) Protection level D data basically must not be processed in paper form in the home office and during mobile working. This also applies in particular to personnel file data or documents with a variety of Protection level D data.

(5) Where possible work should take place using copies, not the original documents

(6) Disposal takes place only via the disposal structures of the University of Oldenburg (data disposal container), or in exceptional cases using suitable file shredders which must be at least Security level 4 (see DIN 66399).

7. Data processing

(1) Storage of data must basically take place on the normal network drives or the officially-approved cloud storage of the University of Oldenburg. This is the only way to guarantee that the data are regularly secured and data loss is avoided.

(2) Exceptions from this are only permitted if it is not possible to connect to the network drives or cloud storage of the University of Oldenburg or there are official interests preventing it. Staff must make sure that all data is stored on the network drives or cloud storage systems of the University of Oldenburg immediately after the connection is restored. Local copies of personal data and confidential data must then be deleted.

(3) Retention periods and deletion deadlines also apply to data and documents employees store at home..

8. Entry into force

The instructions enter into force on 01 April 2023..

Appendix 1

Aids to orientation for classification of security levels in accordance with the security levels concept of the Data Protection Officer for Lower Saxony

Table 1 – Protection level A

Protection level	**Notes on the protection level and which personal information can generally be categorised in this level**	**Typical activities at the University of Oldenburg which generally involve processing data of that protection level**

A	Protection level A involves data that have been made freely accessible by the data subjects (publicly available data). This group can also include data that no longer contain personal data (anonymised data):
	
	- Data concerning individuals that have been released for publication:
	  - contact details,
	  - fields of work,
	  - publications.
	
	- Other personal information which may be published on the basis of consent:
	  - photographs, video and audio recordings,
	  - CVs, profile information,
	  - personal data,
	
	- Course-related content including maximum details of copyright holders:
	  - course catalogue,
	  - lecture materials/scripts (NB check for copyright),
	  - practice materials (NB check for copyright).
		- Design and maintenance of websites
		
		- Production of university-related documents that do not contain any personal data (except possibly for contact details):
		  - regulations, articles of association, agreements, model contracts
		  - circulars, forms, leaflets
		  - information material
		  - Concepts
		
		- Development of teaching and learning concepts and course-related materials
		
		- Production of information material for public relations (flyers, brochures, reports)

Table 2 – Protection level B

Protectio level	Notes on the protection level and which personal information can generally be categorised in this level	Typical activities at the University of Oldenburg which generally involve processing data of that protection level

B	Protection level B covers data that are not expected to cause particular harm if improperly used, but which have not been made freely accessible by the data subject (internally available data). This is generally data which have only been made available to a specific group of people:
	
	- Official data of staff members, used for internal organisation:
	  - plans for the distribution of duties,
	  - organigrams, work instructions,
	  - postal and email distribution lists,
	  - responsibilities.
	
	- Internal communication data:
	  - addresses,
	  - direct telephone,
	  - university account.
	
	- Work-related details in minutes of university committee meetings
	
	- Third-party contact information (contractors, third-party funders, government agencies, and similarly related entities)
		- Organisation and agreement of appointments with internal and external institutions
		
		- Expert advice and ticket support for users of internal systems and software solutions, if no other data of protection levels C, D and E is accessed in the process
		
		- Development and maintenance of internal systems and software, if this also involves processing category B data
		
		- Management of buildings and coordination of construction, conversion and renovation work
		
		- Announcement of election results
		
		- Calling for tenders
		
		- Ordering processes and procurement
		
		- Administration of the modules catalogue

Table 3 – Protection level C

Protection level	Notes on the protection level and which personal information can generally be categorised in this level	Typical activities at the University of Oldenburg which generally involve processing data of that protection level

C	Protection level C covers data that might cause particular harm to the data subject in their social position or economic circumstances if improperly used (reputation) (restricted data):
	
	- Personal data of employees/students, insofar as the information is not assigned to protection requirement D or E:
	  - private contact information
	  - account information
	  - job evaluation
	  - Activity-related information (participation in meetings, committees)
	
	- Event-related participant information, such as attendance lists or contact lists
	
	- Contractual documents (with third parties):
	  - invoices,
	  - travel expenses and pay slips,
	  - third party contracts.
	
	- User names and passwords
	
	- Research data that still contain personal information of participants, but are not categorised Protection level D and E.
	
	- Study and examination work for individual courses
	
	- Examination results / lists of results of individual examination tasks
	
	- Individual master key authorisations
	
	- Personal data in minutes of non-university committee meetings
	
	- Email and telephone communication content, provided that no data of protection level D and E are exchanged
		- Admissions procedures
		
		- Providing advice to potential students
		
		- Registration matters
		
		- (documentation, payments) Correction of academic and examination results
		
		- Support for courses in Stud.IP
		
		- Administration and monitoring of externally funded projects
		
		- Personnel cost management
		
		- Course organisation
		
		- General Secretariat duties, provided no sensitive data (e.g. special data categories in accordance with Art. 9 GDPR) are concerned
		
		- Use of read-only SAP access, provided this does not involve access to Protection level D data
		
		- Support for legal proceedings (employee inventions, BAföG-related matters, admissions procedures), provided no Protection level D or E matters are concerned
		
		- Organisation within the institution (consultations, access to documents, appointment coordination, monitoring deadlines)
		
		- Advice and support for students on course-related issues
		
		- Information management and data delivery for budgeting, managing and planning personnel costs
		
		- Organisation and realisation of allocation of places
		
		- Organisation and administration of master key authorisations

		- Organisation and execution of business trips - Accounting - Systems administration provided no Protection level D data are processed on the systems - Ticket processing by service desk Systemadministration von Systemen soweit auf den Systemen keine Daten der Schutzstufe D verarbeitet werden

Table 4 – Protection level D

Protection level	**Notes on the protection level and which personal information can generally be categorised in this level**	**Typical activities at the University of Oldenburg which generally involve processing data of that protection level**

D	Protection level D covers data that could cause serious harm to the data subject in their social position or economic circumstances if improperly used (existence) (sensitive data):
	
	- Personnel documents and personnel file contents (on employees):
	  - references,
	  - health data,
	  - sick notes,
	  - social data,
	  - absences (holiday, sick leave),
	  - performance assessments,
	  - application documents,
	  - reports for appointment procedures.
	
	- Contents of email and telephone communications, if Protection level D data are exchanged
	
	- Information about student performance (e.g. examination records, performance overview, degree)
	
	- Data from special categories in accordance with Art. 9 GDPR
	
	- Results of research, where sensitive data are concerned
	
	- Data that is subject to confidentiality
		- Personnel matters
		
		- Use of SAP, if this also involves accessing personnel file data
		
		- Support for legal proceedings in HR or in cases of hardship
		
		- Internal audit investigations
		
		- Appointment and application procedures
		
		- Advice and support for students and employees concerning physical and mental problems, hardship, etc.
		
		- Criminal investigations
		
		- Systems administration if Protection level D data are processed on the systems.

Table 5 – Protection level E

Protection level	Notes on the protection level and which personal information can generally be categorised in this level	Typical activities at the University of Oldenburg which generally involve processing data of that protection level
E	Protection level E covers data that could cause harm to the health, life or freedom of the data subject if improperly used (highly sensitive data): - Research records, if highly sensitive data are concerned: - e.g. criminal files, witness protection programmes	- - Research work involving data from highly sensitive fields