Die Landesbeauftragte für den
Datenschutz Niedersachsen

Eckpunkte für die datenschutzkonforme Durchführung von Online-Prüfungen in den niedersächsischen Hochschulen (Stand: November 2021)

Im Sommersemester 2021 hat die Landesbeauftragte für den Datenschutz (LfD) Niedersachsen eine Abfrage bei den niedersächsischen Hochschulen dazu durchgeführt, welche Verfahren bei Online-Prüfungen eingesetzt werden. Das Ergebnis der Auswertung hat unter Berücksichtigung der einschlägigen Literatur zu diesem Thema[1] zu den folgenden Eckpunkten für die datenschutzkonforme Durchführung von Online-Prüfungen in den niedersächsischen Hochschulen geführt.

Vorwort:

An einer Vielzahl niedersächsischer Hochschulen wurden Hochschulprüfungen während der Corona-Pandemie auf elektronischem Wege angeboten. Auch wenn die meisten Hochschulen mittlerweile wieder in den Präsenzbetrieb zurückgekehrt sind, ist davon auszugehen, dass dieses Prüfungsformat zumindest in einigen Studiengängen dauerhaft erhalten bleibt.

Online-Prüfungen müssen so ausgestaltet sein, dass sowohl die prüfungsrechtlichen Grund-sätze als auch die datenschutzrechtlichen Anforderungen eingehalten werden. Der prüfungsrechtliche Grundsatz der Chancengleichheit gebietet, spezielle Instrumente zur Täuschungsprävention vorzusehen. Zugleich bergen Online-Prüfungen im Vergleich zu herkömmlichen analogen Prüfungen höhere Risiken für die Privatsphäre der Prüflinge. Dies gilt insbesondere, wenn zum Ausschluss von Täuschungshandlungen Video- und Audiotechniken in den privaten Räumlichkeiten der Studierenden zum Einsatz kommen. Hier gilt es, einen sachgerechten Ausgleich der betroffenen Rechtsgüter zu erzielen und durch die Vorgabe datenschutzrechtlicher Standards sicherzustellen, dass es nicht zu rechtswidrigen Eingriffen in die Grundrechte auf informationelle Selbstbestimmung der Prüflinge kommt (Art. 2 Abs.1 i.V.m. Art. 1 Abs.1 GG).

[1] Gutachten Prof. Hoeren „Zur datenschutzrechtlichen Zulässigkeit von Überwachungsfunktionen bei Online-Klausuren (06/2020); Gutachten Prof. Forgo u.W. „Rechtliche Aspekte von E-Assessments an Hochschulen (2016), Prof. Alexander Roßnagel „Datenschutz im E-Learning“, ZD 6/2020 S. 296 ff., Albrecht in ZD 2/2021 „Aufsichtsklausuren aus dem Homeoffice“

Inhaltsverzeichnis

1. Schaffung einer Rechtsgrundlage in der Prüfungsordnung:

Bei der Durchführung von Online-Prüfungen sind die Vorgaben der EU-Datenschutzgrund-verordnung (DS-GVO) einschlägig. Fachspezifische Rechtsgrundlage iSd Art. 6 Abs. 1 Buch-stabe e) DS-GVO für die Verarbeitung der Daten der Prüflinge sind die §§ 7 und 17 Nieder-sächsisches Hochschulgesetz (NHG) i.V.m den hochschuleigenen Prüfungsordnungen. Die Einwilligung der Studierenden ist grundsätzlich im Hinblick auf das dem Prüfungswesen immanente Über- und Unterordnungsverhältnis problematisch (vgl. Erwägungsgrund 43 DS-GVO) und birgt wegen der jederzeitigen Widerrufbarkeit trotz der ex-nunc-Wirkung des Widerrufs (vgl. Art. 7 Abs. 3 Satz 2 DS-GVO) gewisse Risiken für die weitere Verfahrensdurch-führung. Somit muss das gesamte Verfahren, dem Bestimmtheits- und dem Verhältnismäßigkeitsgrundsatz Rechnung tragend, vollumfänglich in der jeweiligen Prüfungsordnung der Hochschule geregelt werden.

2. Wahrung des Verhältnismäßigkeitsgrundsatzes:

Von den Hochschulen sind solche Verfahren zu wählen, die im Hinblick auf die Zielerreichung den geringsten Eingriff in die Grundrechte auf informationelle Selbstbestimmung der Prüflinge darstellen. Dies betrifft sowohl die Entscheidung über die Art der Prüfung als auch die Entscheidung über die sich daran anknüpfende Verfahrensausgestaltung.
Generell gilt, dass eine Umwidmung analoger Aufsichtsarbeiten in sog. Open-Book-Prüfungen, bei denen keine Abfrage von Faktenwissen erfolgt, Hilfsmittel grundsätzlich zulässig sind und keine Überwachungsmaßnahmen vorgesehen sind, die datenschutzrechtlich unbedenklichste Variante darstellt. Sofern sich diese Prüfungsart nicht realisieren lässt, ist Folgendes zu beachten: Das Täuschungsrisiko bei Online-Prüfungen mit streng geregelten Hilfsmitteln (sog. Closed-Book-Klausuren) ist naturgemäß höher als bei Präsenzprüfungen. Gleichwohl sind solche Verfahrensschritte zu vermeiden, die nicht einmal bei analogen Prüfungen gerechtfertigt wären. Anknüpfungspunkt für die gebotene Verhältnismäßigkeitsprüfung ist somit stets die Aufsichtsfunktion einer klassisch-analogen Präsenzprüfung.

Im Einzelnen gelten somit die nachfolgenden Punkte:

3. Identitätsfeststellung der Prüflinge

Die Identitätsfeststellung der Prüflinge erfolgt grundsätzlich durch Vorlage des Studierenden- oder des amtlichen Lichtbildausweises per Webcam. Temporäre Speicherungen dürfen nur zur Identitätsfeststellung erfolgen. Die Anfertigung dauerhafter Kopien ist unzulässig.

4. Videoaufsicht

Eine Videoaufsicht durch aufsichtsführende Personen ist zur Vermeidung von Täuschungshandlungen grundsätzlich nicht zu beanstanden. Die Aufsicht hat sich dabei auf das hierfür unerlässliche Maß zu beschränken. Dies bedeutet, dass sie – wie auch bei analogen Prüfungen - grundsätzlich als Überblickskontrolle zu erfolgen hat. Individuelle Einzelkontrollen sind nur bei konkretem Täuschungsverdacht zulässig, wobei die betroffenen Prüflinge hierüber unverzüglich zu informieren sind, beispielsweise durch das Nutzen optischer Anzeigefelder.
Unbedenklich erscheint im Rahmen der Videoaufsicht die Aufforderung zur Bildschirmfrei-gabe durch die aufsichtsführende Person bei konkretem Täuschungsverdacht, sofern gewährleistet ist, dass die übrigen Prüflinge keinen Einblick in diesen Bereich erlangen (sog. Breakout-Raum).

5. Einsatz von Kameras

Sofern **Kameras** eingesetzt werden, sind die Verfahren im Hinblick auf die Ausrichtung der Kamera so auszugestalten, dass die Privatsphäre der Prüflinge gewahrt bleibt. Die pauschale Aufforderung zum sog. **Raumschwenk der Kamera in die Privaträume** zur Feststellung alleiniger Anwesenheit des Prüflings stellt als Raumüberwachung einen unverhältnismäßigen Eingriff in die private Lebenssphäre des Prüflings dar. Die Aufforderung kann allenfalls in Fällen konkreten Täuschungsverdachts auf Einwilligungsbasis gerechtfertigt sein. Voraussetzung hierfür ist, dass das Verfahren so ausgestaltet ist, dass den Prüflingen als Alternative die Ab-leistung der Prüfung in den Räumen der Hochschule ermöglicht wird und sie somit vorab die freie Entscheidung darüber haben, ob und ggf. wie viel ihrer Privatsphäre sie im Rahmen der Hochschulprüfung preisgeben wollen.
Verhältnismäßig und damit datenschutzrechtlich unbedenklich erscheint dagegen die Aufforderung, zu Beginn der Prüfung die Kamera kurz auf den Arbeitsbereich zu richten, um dadurch unzulässige Hilfsmittel auszuschließen.

6. Videoaufzeichnungen

Videoaufzeichnungen sind grundsätzlich unzulässig. Sie dürfen insbesondere nicht „auf Vorrat“ angefertigt werden, sondern nur in besonderen Ausnahmefällen bei konkreten Anhaltspunkten eines Täuschungsverdachts zu Beweiszwecken und sind auf die konkret betroffene Person zu begrenzen. Wegen der stärkeren Eingriffsintensität, die Aufzeichnungen im Vergleich zu reinen Aufsichtsmaßnahmen aufweisen, ist zudem zu fordern, dass sie nur gegenüber den Prüflingen zum Einsatz kommen, die vorab in diese Verfahren eingewilligt haben. Dies setzt voraus, dass den Prüflingen als Alternative die Ableistung einer Prüfung in den Räumen der Hochschule ermöglicht wird. Zudem ist

sicherzustellen, dass die Aufzeichnungen unverzüglich nach Bestandskraft der prüfungsrechtlichen Entscheidung gelöscht werden.

7. Weitere Überwachungsmaßnahmen

Weitere Überwachungsmaßnahmen, die über die reine Videoaufsicht hinausgehen und unverhältnismäßig in die Vertraulichkeit und Integrität des IT-Systems des Prüflings (sog. IT-Grundrecht[2]) eingreifen, sind unzulässig. Dabei ist zunächst festzuhalten, dass die Prüflinge durch eine Regelung in der Hochschulordnung nicht verpflichtet werden können, zur Durch-führung von Online-Prüfungen solche Programme auf ihr privates Endgerät herunterzuladen und dort zu installieren, die eine über die Verarbeitung der IP-Adresse hinausgehende Daten-verarbeitung erfordert. Die Vorgabe entsprechender Programme kann nur auf freiwilliger Basis erfolgen und setzt alternativ die Möglichkeit zur Ablegung der Prüfung in den Räumen der Hochschule voraus.
Selbst wenn diese Voraussetzungen vorliegen, bleibt der Einsatz solcher Programme unverhältnismäßig und damit unzulässig, bei denen nicht gewährleistet werden kann, dass nach Abschluss der Online-Prüfung kein weiterer Zugriff auf die privaten IT-Systeme der Prüflinge erfolgt. Kann dieses Risiko aber verneint werden, bestehen keine Bedenken gegen den Ein-satz von Prüfungssoftware, die lediglich sicherstellt, dass während der Prüfung keine weiteren Programme verwendet bzw. keine Internetseiten aufgerufen werden können.

8. Einsatz besonderer Überwachungsprogramme/ Verarbeitung biometrischer Daten

Der Einsatz besonderer Überwachungsprogramme, die biometrische Daten verarbeiten, ist mangels einer spezialgesetzlichen Rechtsgrundlage unzulässig und wäre auch stets als unverhältnismäßig anzusehen. Dies betrifft insbesondere solche Verfahren, die auf einer Aufzeichnung und Auswertung der Tastatur- oder Mausbewegungen mit dem Ziel der eindeutigen Zuordnung des jeweiligen Bewegungsmusters zu einem Prüfling beruhen. Hierbei ist zu berücksichtigen, dass biometrische Daten (vgl. Art. 4 Nr. 14 DS-GVO) nach Art. 9 Abs. 1 DS-GVO besonders schutzwürdige Daten darstellen, die nur unter engen Voraussetzungen verarbeitet werden dürfen.

[2] vgl. BVerfGE 120, 274 ff. (Online-Durchsuchungen)

9. Einsatz externer Dienstleister

Sofern externe Dienstleister eingesetzt werden, ist ein **Auftragsverarbeitungsvertrag** gem. Art. 28 DS-GVO abzuschließen. Werden personenbezogene Daten außerhalb der EU bzw. außerhalb des Europäischen Wirtschaftsraums verarbeitet, sind die Regelungen des internationalen Datentransfers (Art. 44 ff. DS-GVO) zu beachten.

Bezüglich Datentransfers in die USA hat der Europäische Gerichtshof (EuGH) mit Urteil vom 16.07.2020 (Rs. C-311/18 - Schrems II) festgestellt, dass das US-Recht kein Schutzniveau gewährleistet, das dem in der EU gleichwertig ist. Daher ist es bei Datenübermittlungen in die USA erforderlich, dass geeignete Garantien nach Art. 46 DS-GVO durch wirksame zusätzliche Maßnahmen ergänzt werden. Der Europäische Datenschutzausschuss hat am 18.06.2021 die *„Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data - Version 2.0“* verabschiedet. In diesem Papier werden die Anforderungen an zusätzliche Maßnahmen, z.B. eine dem Stand der Technik entsprechende Ende-zu-Ende Verschlüsselung, beschrieben und es werden konkrete Beispiele genannt. Die Ausführungen im Schrems II-Urteil gelten entsprechend für Übermittlungen auf der Grundlage von Binding Corporate Rules oder anderer Übermittlungsinstrumente.

In der Praxis wird es für die Hochschulen darauf ankommen, ob diese Anforderungen erfüllt werden können. Beim Einsatz von Videokonferenzsystemen von US-Anbietern, die dem Anwendungsbereich problematischer US-Gesetze unterfallen, namentlich der FISA 702[3], dürfte dies im Regelfall wegen der aus technischen Gründen erforderlichen unverschlüsselten Übertragung von Verkehrs- und Metadaten nicht möglich sein. Nur wenn nachgewiesen wird, dass die FISA 702 in der Praxis nicht auf den konkreten Transfer angewendet wird und daher die Wirksamkeit der Übermittlungsinstrumente (z. B. Standardvertragsklauseln) nicht beeinträchtigt, kann die Übermittlung auf dieser Grundlage ohne zusätzliche Maßnahmen erfolgen (siehe Recommendations 01/2020 Rn. 49). Alternativ kann auf „On-Premise“-Lösungen zurückgegriffen werden, bei denen die Videokonferenz-Software auf eigenen Servern installiert wird und auch der Verbindungsaufbau keine Datenübermittlung in die USA erfordert. Die Hochschulen sind hier gehalten, die vorhandenen datenschutzkonformen Lösungen zu nutzen.

[3] Section 702 des Foreign Intelligence Surveillance Act (FISA), 50 U.S. Code §§ 1881, 1881a; eingeführt durch FISA Amendments Act of 2008 vom 10. Juli 2008, abrufbar unter: https://www.law.cornell.edu/uscode/text/50.

10. Weitere Anforderungen, die aus der unmittelbaren Geltung der DS-GVO folgen

1. Die Hochschule hat die **Betroffenenrechte gem. Art. 12 ff DS-GVO** in transparenter und nachvollziehbarer Weise zu erfüllen.
2. Die im Rahmen der Online-Prüfungen gewählten Verfahren sind in das **Verzeichnis der Verarbeitungstätigkeiten** aufzunehmen **(vgl. Art. 30 DS-GVO).**
3. **Prüfung einer Datenschutz-Folgenabschätzung (DSFA):**
   Unter Geltung der DS-GVO gehört es zu den Pflichten des Verantwortlichen, bei Formen der Verarbeitung, die ein voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, eine DSFA nach Art. 35 DSGVO durchzuführen. Die Durchführung der DSFA dient dazu, in einem systematischen Vorgehen geplante Verarbeitungsvorgänge zu beschreiben, ihre Notwendigkeit und Verhältnismäßigkeit zu beurteilen, die Risiken für die Rechte und Freiheiten der betroffenen Personen zu bewerten und zur Bewältigung dieser Risiken vorab Abhilfemaßnahmen festzulegen.
   Um Anwendern die Beantwortung dieser Frage zu erleichtern, hat die Landesbeauftragte für den Datenschutz Niedersachsen ein Prüfschema entwickelt. Damit können Verantwortliche für ihren Verantwortungsbereich prüfen, ob die Durchführung einer DSFA erforderlich ist. Neben einer Checkliste und einem umfangreichen Glossar der wichtigsten Begriffe enthält das Schema auch Hinweise auf weitere Hilfestellungen zum Thema DSFA. Das Prüfschema steht unter https://lfd.niedersachsen.de/ download/165235 bereit.
   Das Kurzpapier der Datenschutzkonferenz (DSK) zur DSFA finden Sie unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf.
4. **Umsetzung geeigneter technisch-organisatorischer Maßnahmen (toM):**
   Die Artikel 24, 25 und 32 der DS-GVO geben die technisch-organisatorischen Rahmenbedingungen vor, innerhalb derer „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen“ vom Verantwortlichen geeignete, angemessene, zu dokumentierende und regelmäßig zu überprüfende Sicherungsmaßnahmen zu treffen sind.
   Hierzu muss der Verantwortliche in einer Risikobetrachtung geeignete technisch-organisatorischen Maßnahmen (toM) benennen und umsetzen, die dem ermittelten Risiko angemessen sind. Der Verantwortliche ist hierbei frei bei der Auswahl der von ihm gewählten toM, solange das von ihm ermittelte Risiko damit angemessen berücksichtigt wird. Aufgrund dieses

risikobasierenden Ansatzes der DS-GVO ist es nicht vorgesehen, allgemeine Mindeststandards vorzugeben oder darauf fußende Praxisbeispiele zu benennen. Für Online-Prüfungen spezifische Beispiele für technisch und organisatorisch zu bewertende Gefährdungen und risikoerhöhende Sachverhalte sind bereits in den Ziffern 1. bis 9. enthalten.
Weitergehende generische Gefährdungen und Maßnahmen zur Herstellung eines angemessenen Schutzniveaus befinden sich im Kapitel 4 der „OH Videokonferenzsysteme“ der DSK und den Ziffern 13 bis 16 der „Fragen und Antworten zu Videokonferenzsystemen“ der LfD Niedersachsen. Diese weisen bereits eine große Schnittmenge mit Maßnahmen für Online--Prüfungen auf.
Diese allgemeinen Maßnahmen sind für sich allein genommen jedoch nicht ausreichend und müssen noch individuell angepasst und ergänzt werden.
Darüberhinausgehende toM lassen sich beispielsweise aus den folgenden Quellen ableiten:

- Standard-Datenschutzmodell (SDM) - generische Maßnahmen im SDM Kapitel 7[4] sowie SDM –Maßnahmenkatalog (erste Bausteine von einzelnen Aufsichtsbehörden in Erprobung)
- BSI - IT-Grundschutz-Kompendium (https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html) und ggf. BSI-Grundschutzmaßnahmen (alt)
- ISO 27001 generische Maßnahmen[5]
- IT-Grundschutz-Profile[6]

Im Ergebnis der Prüfung, welche toM wirksam, geeignet und angemessen sind, wird deutlich, dass es zwar typische toM gibt, diese jedoch in den allermeisten Fällen durch individuelle toM ergänzt werden müssen. Der Verantwortliche muss daher einen Katalog der toM für die individuelle Verarbeitung erstellen. Dieser enthält detaillierte Beschreibungen aller zu treffenden technischen Maßnahmen. Zudem beschreibt er, welche organisatorischen Regelungen für die

[4] Das Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 2.0b, von der 99. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 17. April 2020 beschlossen, abrufbar unter: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/
[5] Standard ISO 27001 “Information technology — Security techniques — Information security management systems — Requirements” von der International Organization for Standardization, abrufbar: https://www.iso.org/standard/54534.html
[6] IT-Grundschutz-Profile gemäß den BSI-Spezifikationen, vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Strukturbeschreibung.pdf?__blob=publicationFile&v=6 und https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzProfile/Profile/itgrundschutzProfile_Profile.html

sichere Einführung bzw. den weiteren Betrieb der betrachteten Verarbeitungstätigkeit erforderlich sind.

Die Landesbeauftragte für den Datenschutz Niedersachsen hat als weitere Hilfestellung eine Handlungsempfehlung für Praktiker zum technisch-organisatorischen Datenschutz bereitgestellt. Diese Handlungsempfehlung beantwortet die Frage, wie Verantwortliche die geeigneten toM ermitteln können, um die Anforderungen der DS-GVO ordnungsgemäß zu berücksichtigen. Der hierzu entwickelte „Prozess zur Auswahl angemessener Sicherungsmaßnahmen (ZAWAS)“ ist geeignet, sowohl bei der Durchführung einer DSFA als auch bei einer normalen Verarbeitungstätigkeit die technisch-organisatorischen Maßnahmen systematisch herzuleiten.

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5
30159 Hannover
Telefon 0511 120-4500
Fax 0511 120-4599
E-Mail an poststelle@lfd.niedersachsen.de schreiben