

## **Handreichung zu Online-Prüfungen an Hochschulen**

Stand: 28. Juli 2022

### **Einleitung**

Wegen der Corona-Pandemie mussten Hochschulen auf online-basierte Lehrangebote umstellen und haben auch Online-Prüfungen durchgeführt. Dies hat einen Digitalisierungsschub in der Hochschullehre erzeugt. Es ist absehbar, dass die aufgebauten Online-Möglichkeiten über die Corona-Pandemie hinaus genutzt und Online-Prüfungen an Hochschulen in NRW weiterhin stattfinden werden. Dies kann auch dem Interesse von Prüflinge entsprechen. Zugleich werden Prüflinge während der Online-Prüfung in ihrem privaten häuslichen Umfeld beobachtet und so in ihrer Privatsphäre tangiert. Damit derartige Prüfungen im Einklang mit den Grundrechten der Prüflinge auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz und dem Recht auf Privatsphäre gemäß Art. 7 und dem Recht auf den Schutz personenbezogener Daten gemäß Art. 8 der Grundrechtecharta der Europäischen Union (EU) durchgeführt werden, haben wir die nachfolgende Handreichung erstellt.

Die Hochschulen haben bei Online-Prüfungen die Datenschutzbelange der Prüflinge mit dem prüfungsrechtlichen Grundsatz der Chancengleichheit in Einklang zu bringen. Diese Handreichung soll dazu eine Hilfestellung geben. Sie zeigt die Grenzen videobasierter Aufsicht im Verhältnis zum Schutz der Privatsphäre der Prüflinge auf und geht unter anderem auf folgende Fragen ein: Wie läuft die Authentifizierung der Prüflinge online ab? Darf die Prüfung aufgezeichnet werden? Darf die Kamera im privaten Wohnraum der Prüflinge geschwenkt werden? Die behördlichen Datenschutzbeauftragten der Hochschulen des Landes NRW hatten im Vorfeld Gelegenheit zur Stellungnahme zu dieser Handreichung. Viele Hinweise aus diesem Kreis wurden vorliegend berücksichtigt.

In dieser Handreichung wird ausschließlich die Online-Prüfung in Form der Online-Klausur (sog. klassische Aufsichtsklausur in elektronischer Form) betrachtet, die wie eine klassische Aufsichtsklausur innerhalb weniger Stunden und entweder ohne oder mit genau vorgegebenen zugelassenen Hilfsmitteln unter Aufsicht angefertigt wird.

## Rechtsgrundlage für die Verarbeitung personenbezogener Daten

Unabhängig davon, wie die Abnahme von Online-Prüfungen konkret ausgestaltet ist, werden personenbezogene Daten der Betroffenen verarbeitet, insbesondere zur Identifizierung der Prüflinge.

Nach Art. 6 Abs. 1 Satz 1 Datenschutz-Grundverordnung (DS-GVO) ist eine Verarbeitung personenbezogener Daten durch öffentliche Stellen dann rechtmäßig, wenn entweder eine Einwilligung vorliegt oder eine Rechtsgrundlage im materiellen Recht nach Art. 6 Abs. 1 Satz 1 Buchstabe c oder e DS-GVO in Verbindung mit Art. 6 Abs. 3 DS-GVO die Verarbeitung erlaubt. Die Rechtsgrundlage für die Durchführung von Online-Prüfungen ergibt sich aus Art. 6 Abs. 1 Buchstabe e, Abs. 3 DSGVO in Verbindung mit §§ 64 Abs. 2 Satz 2, 82a Hochschulgesetz NRW (HG NRW) in Verbindung mit den jeweiligen Prüfungsordnungen der Hochschulen.

Nach § 64 Abs. 2 Satz 2 HG NRW kann in der Prüfungsordnung geregelt werden, dass Hochschulprüfungen in elektronischer Form oder in elektronischer Kommunikation (Online-Prüfungen) abgelegt werden. Hierbei sind nach § 64 Abs. 2 Satz 3 HG NRW insbesondere Bestimmungen zum Datenschutz zu treffen. Nach der Gesetzesbegründung (Vgl. LT-Drs. 17/14963, S. 57) soll mit der Änderung des § 64 Abs. 2 HG NRW mit dessen neuem Satz 3 die Bedeutung der Beachtung datenschutzrechtlicher Grundsätze bei Online-Prüfungen klargestellt werden.

Die Regelung des § 64 Abs. 2 Satz 2 HG NRW in Verbindung mit den jeweiligen Prüfungsordnungen der Hochschulen können eine geeignete Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Rahmen der Durchführung von Online-Prüfungen im Sinne von Art. 6 Abs. 3 DS-GVO darstellen, vorausgesetzt, die jeweiligen Hochschulrektorate haben darin entsprechende, datenschutzgerechte Regelungen hinsichtlich der Art und Weise der Durchführung von Online-Prüfungen erlassen. Die nationale Rechtsgrundlage muss – über die Voraussetzungen des Art. 6 Abs. 3 Sätze 2 und 3 DS-GVO hinaus – gemäß dessen Satz 4 ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen (Grundsatz der Verhältnismäßigkeit).

Erlässt eine Hochschule zur Durchführung von Online-Prüfungen Regelungen nach Maßgabe des § 64 Abs. 2 Satz 2 und Satz 3 HG NRW, hat sie die danach vorgesehenen Datenverarbeitungen auf das zu beschränken, was für die Abnahme der Online-Prüfungen angemessen und erforderlich ist. Dazu kommt es auf die Umstände des Einzelfalls an. Bei Prüfungen ist die Chancengleichheit aller Prüflinge zu gewährleisten. Für alle Prüflinge müssen deshalb so weit wie möglich vergleichbare Prüfungsbedingungen gelten. Dazu muss es Kontrollmöglichkeiten geben, um Prüfungsbetrug zu verhindern. Andererseits wäre mit dem Grundsatz der Verhältnismäßigkeit ein permanenter Videobeobachtungsdruck der ohnehin bereits

## **LDI NRW – Online-Prüfungen**

unter Prüfungsdruck stehenden Prüflinge nicht vereinbar. Notwendig bleiben aber Stichprobenkontrollen. Die Präsenzsituation sollte dabei für das Ausmaß der Überwachung bei Online-Prüfungen als Vergleich im Blick behalten werden

Die Hochschulen können in den Prüfungsordnungen eine Wahlmöglichkeit für die Prüflinge vorsehen, nach der diese selbst festlegen können, ob sie die Online-Prüfung in den Räumlichkeiten der Hochschule oder in ihrem privaten häuslichen Umfeld ablegen möchten (siehe auch unten unter Punkt 3.a).

## Rechtliche Beurteilung im Einzelnen

Die unten aufgeführte Tabelle stellt keine abschließende Auflistung aller in Betracht kommenden Maßnahmen zur Durchführung von Online-Prüfungen dar.

Zur Beurteilung einer Maßnahme müssen insbesondere folgende Gesichtspunkte berücksichtigt werden:

### a. Ziele der Videoaufsicht

- Authentifizierung der Prüflinge
- Vermeidung und Aufdeckung von Täuschungsversuchen zwecks Gewährleistung des prüfungsrechtlichen Grundsatzes der Chancengleichheit bei gleichzeitiger Beachtung der Grundrechte der Prüflinge
- Ermöglichung der Kommunikation der Prüflinge mit dem Aufsichtspersonal.

### b. Maßstab: Verhältnismäßigkeit

- Geeignetheit, Erforderlichkeit und Angemessenheit der Maßnahme
- Abwägung unter Berücksichtigung der Umstände des Einzelfalls.

Hierzu sind u. a. folgende Fragen zu klären: Wird die Online-Prüfung in den privaten Räumlichkeiten der Prüflinge oder in solchen der Hochschule durchgeführt? Welche technischen und organisatorischen Prüfungsbedingungen sind im Einzelfall vorgesehen? Welche Software wird im konkreten Fall eingesetzt und welche datenschutzfreundlichen Voreinstellungen werden vorgenommen?

Im Rahmen der Videoaufsicht ist die eingriffsärmere Maßnahme zu wählen. Zudem sind im ausgewählten Videokonferenzsystem Voreinstellungen vorzunehmen, die die Privatsphäre und den Persönlichkeitsschutz der Prüflinge am effektivsten schützen.

### c. Vergleichssituation: Präsenzklausur

Eine weitergehende Kontrolle, als sie in einer Präsenzsituation möglich wäre, ist bei der Videoaufsicht nicht verhältnismäßig und daher unzulässig.

## Auflistung von Maßnahmen bzgl. der Art und Weise der Durchführung von Online-Prüfungen

### **Vorbemerkungen:**

#### **Betroffenenrechte, Art. 12 ff. DS-GVO**

Vor der Durchführung einer Online-Prüfung sind die Prüflinge nach den Vorgaben der Art. 13 ff. DS-GVO zu informieren und über ihre Betroffenenrechte (Art. 12-21 DS-GVO) in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache aufzuklären.

#### **Verarbeitungsverzeichnis, Art. 30 DS-GVO**

Die Verfahren zur Durchführung von Online-Prüfungen sind in das Verzeichnis über die Verarbeitungstätigkeiten aufzunehmen, vgl. Art. 30 DS-GVO.

#### **Technisch-organisatorische Maßnahmen, Art. 24, 25, 32 DS-GVO**

Es müssen geeignete technische und organisatorische Maßnahmen getroffen werden, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die tabellarische Auflistung unten stellt einen Teil der Umsetzung dieser Verpflichtung dar.

#### **Datenschutz-Folgenabschätzung, Art. 35 DS-GVO**

Vor dem Einsatz eines Verfahrens ist der Verantwortliche nach Art. 35 DS-GVO dazu verpflichtet, eine Datenschutz-Folgenabschätzung durchzuführen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

#### **Angemessene Vorlaufzeit für die Prüflinge**

Den Prüflingen ist die Möglichkeit zu eröffnen, die für die Durchführung einer Online-Prüfung einzusetzende Technik, die Ausstattung sowie die räumlichen Rahmenbedingungen innerhalb eines angemessenen Zeitraums vor der Prüfung zu testen.

A	Maßgebliche Beschreibung der Maßnahme zur Authentifizierung	Beurteilung	Zulässigkeit
A1	Authentifizierung der Prüflinge im virtuellen Prüfungsraum	Eine Authentifizierung mittels Abgleich eines gültigen Lichtbildausweises und dem Gesicht der Prüflinge ist erforderlich. Die Prüflinge sind darauf hinzuweisen, dass die übrigen Daten des gültigen Lichtbildausweises, die nicht für die Authentifizierung notwendig sind, abgeklebt oder auf andere Weise unkenntlich gemacht werden können.	(+)
A2	Authentifizierung der Prüflinge im virtuellen Prüfungsraum vor allen übrigen Prüfungsteilnehmer*innen	Die Authentifizierung der Prüflinge muss einzeln und damit unter Ausschluss der übrigen Prüflinge erfolgen. Die technischen Vorkehrungen hierfür müssen vorgehalten werden, auch bei Prüfungsformaten mit vielen Personen.	(-)
A3	Screenshots oder Aufzeichnungen des Identifikationsdokuments	Screenshots und Aufzeichnungen des gültigen Lichtbildausweises sind nicht zulässig. Es sind technische und organisatorische Maßnahmen zu treffen, die eine ordnungsgemäße Authentifizierung der Prüflinge ohne dauerhafte Speicherung der personenbezogenen Daten aus dem jeweiligen gültigen Lichtbildausweis gewährleisten. Personenbezogene Daten, die technisch notwendig zwischengespeichert worden sind, sind unverzüglich zu löschen.	(-)
A4	Einsetzen von Gesichtserkennungssoftware	Die Verarbeitung biometrischer Daten ist unzulässig. Dies entspricht nicht der Vergleichssituation einer Präsenzklausur. Ein Abgleich mit einem gültigen Lichtbildausweis vor der Kamera ohne Einsatz einer solchen Software reicht aus.	(-)

B	Maßgebliche Beschreibung der Maßnahme zur Durchführung der Videoaufsicht	Beurteilung	Zulässigkeit
B1	Aktivierung der Kamera- und Mikrofonfunktion von eingesetzten Endgeräten	Vergleichbar mit einer Präsenzklausur muss das Aufsichtspersonal in die Lage versetzt werden, auch tatsächlich ihrer Aufsichtsfunktion nachzukommen. Dazu gehört, die Prüflinge samt ihrer unmittelbaren Prüfungsumgebung vor dem Endgerät visuell und akustisch beaufsichtigen zu können.	(+)
B2	Dauerhafte, verdachtsunabhängige oder anlasslose Aufzeichnung von Videoaufnahmen oder anderweitige Speicherung von Bild- oder Tondateien	<p>Eine <b>dauerhafte, verdachtsunabhängige oder anlasslose</b> Aufzeichnung entsprechender Aufnahmen oder anderweitige Speicherung von Bild- oder Tondateien ist nicht zulässig.</p> <p>Allenfalls <b>bei Verdacht des Vorliegens eines Täuschungsversuchs</b> oder bei Hinweisen hierauf kann es erforderlich sein, dass die Aufsichtsführenden erst ab diesem Zeitpunkt die Aufzeichnung zum Zweck des Nachweises von Täuschungsversuchen oder Störungen des Prüfungsablaufs starten.</p> <p>Dies ist unter Berücksichtigung der Umstände des Einzelfalls zu beurteilen. Dabei sind insbesondere die Datenschutzinteressen der Prüflinge, die ohne Täuschungsabsicht an der Prüfung teilnehmen und keine Störungen des Prüfungsablaufs geltend machen, zu berücksichtigen.</p> <p>Die <b>Prüfungsordnung</b> der Hochschule muss eine detaillierte und auf den konkreten Einsatz beschränkte Regelung zu dieser Maßnahme enthalten.</p> <p>Die Prüflinge sind <b>im Vorfeld</b> über diese Maßnahme zu informieren.</p>	Grds. (-)

<p>B3</p>	<p>(Langsamer) 360-Grad-Schwenk durch die Wohnung der betroffenen Person zwecks Feststellung weiterer anwesender Personen oder anderer Hilfsmittel</p>	<p>Der (langsame) 360-Grad-Schwenk durch die Wohnung der betroffenen Person greift grundsätzlich in die Grundrechte der Prüflinge ein.</p> <p>Der <b>anlasslose</b> 360-Grad-Schwenk stellt einen unangemessenen Eingriff in die Grundrechte der Prüflinge dar, der zudem nur bedingt zur Vermeidung von Täuschungsversuchen beiträgt, da dieser lediglich eine kurze Momentaufnahme des Prüfungsraums wiedergeben kann und dieser unmittelbar nach Durchführung des Schwenks wieder verändert werden könnte</p> <p>Allenfalls <b>bei Verdacht des Vorliegens eines Täuschungsversuchs</b> oder bei Hinweisen hierauf kann es erforderlich sein, dass die Aufsichtsführenden erst ab diesem Zeitpunkt einen 360-Grad-Schwenk durch die Wohnung der Prüflinge zum Zweck des Nachweises von Täuschungsversuchen oder Störungen des Prüfungsablaufs vornehmen.</p> <p>Dies ist unter Berücksichtigung der Umstände des Einzelfalls zu beurteilen. Dabei sind insbesondere die Datenschutzinteressen der Prüflinge, die ohne Täuschungsabsicht an der Prüfung teilnehmen und keine Störungen des Prüfungsablaufs geltend machen, zu berücksichtigen.</p> <p>Die <b>Prüfungsordnung</b> der Hochschule muss eine detaillierte und auf den konkreten Einsatz beschränkte Regelung zu dieser Maßnahme enthalten.</p> <p>Die Prüflinge sind <b>im Vorfeld</b> über den jederzeit im Verdachtsfall möglichen 360-Grad-Schwenk zu informieren, damit diese die Gelegenheit haben, den von ihnen jeweils gewählten Prüfungsraum entsprechend „neutral“ zu</p>	<p><b>Grds. (-)</b></p>
-----------	--	--	-------------------------

		gestalten. Darüber hinaus sind die Prüflinge unmittelbar vor der tatsächlichen Durchführung des Schwenks zu informieren (kein heimlicher Schwenk).	
B4	Automatisierte Überwachungsprogramme	<p>Der Einsatz von automatisierten Überwachungsprogrammen (oder sonstiger „KI“-Software), durch die Bild- und Tonaufzeichnungen anhand verschiedener Parameter wie Tastenanschläge oder Kopf-, Körper- und Augenbewegungen der Prüflinge daraufhin automatisiert ausgewertet werden können, ob ein Täuschungsversuch vorgelegen haben könnte, stellen regelmäßig einen besonders schwerwiegenden Eingriff dar, der mangels Vorliegens einer speziellen gesetzlichen Grundlage unzulässig ist.</p> <p>Nur bei der Umsetzung von Massenprüfungen ist der Einsatz von automatisierten Verfahren zumindest in der Verdachtsmeldung <b>ausnahmsweise</b> denkbar. Diese dürfen sich ausschließlich auf die Livebilder beziehen und müssen derart gestaltet werden, dass weder Daten gespeichert werden noch eine automatisierte Entscheidung getroffen wird.</p> <p>Der Einsatz kann etwa so erfolgen, dass durch einen automatischen Hinweis eine Aufsichtsperson benachrichtigt wird, die dieser Meldung nachgeht.</p> <p>Dies ist unter <b>Berücksichtigung der Umstände des Einzelfalls</b> zu beurteilen. Dabei sind insbesondere die Datenschutzinteressen der Prüflinge, die ohne Täuschungsabsicht an der Prüfung teilnehmen und keine Störungen des Prüfungsablaufs geltend machen, zu berücksichtigen.</p> <p>Die <b>Prüfungsordnung</b> der Hochschule muss eine detaillierte und auf den</p>	<b>Grds. (-)</b>

		<p>konkreten Einsatz beschränkte Regelung zu dieser Maßnahme enthalten.</p> <p>Die Prüflinge sind <b>im Vorfeld</b> über den Einsatz einer solchen Software zu informieren.</p>	
B5	Betrachten der Prüflinge in Nahaufnahme (Heranzoomen)	Dies ist zur Erreichung des Zwecks der Online-Aufsicht nicht erforderlich und entspricht zudem nicht den Möglichkeiten während einer Präsenzklausur.	<b>(-)</b>
B6	Einsatz von mehreren Kameras zur Erhöhung der Intensität der Überwachung (z. B. eine weitere Kamera aus einem anderen Blickwinkel)	Dies ist unter Verhältnismäßigkeitsgesichtspunkten nicht erforderlich, da der Einsatz einer Kamera bei der Videoaufsicht einer elektronischen Fernklausur ausreicht, um die Prüflinge vor dem betreffenden Endgerät betrachten und ihr näheres Umfeld überblicken zu können.	<b>(-)</b>
B7	Dauerhafte Übertragung der Bildschirmansicht des für die Online-Prüfung und die Videoaufsicht verwendeten Endgeräts	<p>Dies stellt in der Regel einen unverhältnismäßigen Eingriff dar. In der Präsenzsituation erhält die aufsichtführende Person während der Prüfung keine dauerhafte Einsicht in die Anfertigung der Prüfungsniederschrift der Prüflinge.</p> <p>Allenfalls <b>bei Verdacht des Vorliegens eines Täuschungsversuchs</b> oder bei Hinweisen hierauf kann ein Zugriff auf den Bildschirm der Prüflinge auf Nachfrage/Hinweis durch das Aufsichtspersonal erforderlich sein. Dieser Zugriff hat unbeobachtet von den übrigen Prüflingen zu erfolgen.</p>	<b>Grds.: (-)</b>
B8	Untersagung eines virtuellen Hintergrunds	Zwar haben die Prüflinge im Rahmen der Prüfungsvorbereitung eine Einflussmöglichkeit, an welchem Ort in ihren privaten Räumlichkeiten sie die Prüfung ablegen (z. B. vor einer weißen Wand). Die Hochschule kann aber zurecht den Einsatz eines virtuellen Hintergrundes untersagen.	<b>(+)</b>

		Dies ist erforderlich, um dem Aufsichtspersonal ähnlich wie bei einer Präsenzklausur eine angemessene Kontrolle der Prüflinge durch Einsichtnahme in das direkte Umfeld zu ermöglichen. Ein anlassloser 360-Grad-Schwenk durch den Raum ist allerdings unverhältnismäßig und daher unzulässig (siehe unter B3).	
B9	Sichtbarkeit der übrigen Prüflinge für die einzelnen Prüflinge	<p>Dies stellt einen unverhältnismäßigen Eingriff in die Privatsphäre der Prüflinge dar. Die Sichtbarkeit der Kamerabilder der jeweils anderen Prüflinge für die einzelnen Prüfungsteilnehmenden ist für die Vermeidung bzw. Aufdeckung von Täuschungsversuchen durch das Aufsichtspersonal nicht erforderlich und daher unzulässig.</p> <p>Im Übrigen ist dies nicht vergleichbar mit einer Präsenzklausur, da hier in der Regel eine Einsicht in die privaten Räumlichkeiten der Prüflinge erfolgt.</p> <p>Gleiches gilt für Überprüfungsmaßnahmen durch das Aufsichtspersonal; diese sollten „unbeobachtet“, d.h. getrennt bei den jeweiligen Prüflingen unter Ausschluss der übrigen Prüflinge erfolgen (siehe auch unter B12).</p>	<b>(-)</b>
B10	Ständige Sichtbarkeit des Gesichts, Oberkörpers und Arbeitsplatzes inklusive Prüfungsbogen der Prüflinge	Dies ist erforderlich, um dem Aufsichtspersonal eine angemessene Kontrolle der Prüflinge zu ermöglichen.	<b>(+)</b>
B11	Verhindern eines zweiten Bildschirms, Deaktivierung der Zwischenablage (Copy/Paste), Schließen geöffneter Tabs und neue Tabs verhindern, Deaktivieren eines Rechtsklicks,	Diese Maßnahmen sind geeignet und erforderlich, um Täuschungsversuche zu verhindern.	<b>(+)</b>

## LDI NRW – Online-Prüfungen

	Vollbildschirm erzwingen, Drucken deaktivieren, Löschen des Cache.		
B12	Überprüfung einer oder eines Prüfungsteilnehmenden durch Aufruf des Einzelbildes	Dies ist zu Zwecken der Vermeidung und Aufdeckung von Täuschungsversuchen möglich, soll den jeweiligen Prüflingen aber technisch angezeigt werden, z. B. anhand einer Meldung im Videokonferenzsystem.  Diese Maßnahme sollte unbeobachtet durch die übrigen Prüflinge erfolgen.	<b>(+)</b>

## Empfehlungen der LDI NRW

### 1. Wahlmöglichkeit der Prüflinge

Online-Prüfungen in den durch die Hochschulen zur Verfügung gestellten Räumlichkeiten sind gegenüber Online-Prüfungen im privaten häuslichen Umfeld der Prüflinge in jedem Fall datenschutzfreundlicher, weil sie dem Grundsatz der Datensparsamkeit (vgl. Art. 5 Abs. 1 Buchstabe c DS-GVO) entsprechen und Eingriffe in die Privatsphäre der Prüflinge vermeiden. Online-Prüfungen im privaten häuslichen Umfeld der Prüflinge erfordern stets zusätzliche Datenverarbeitungen, die risikobehaftet sind. Vor diesem Hintergrund sollten die Prüfungsordnungen der Hochschulen vorsehen, dass die Prüflinge eine Wahlmöglichkeit haben und selbst festlegen können, ob sie die Online-Prüfung in den Räumlichkeiten der Hochschule oder in ihrem privaten häuslichen Umfeld ablegen möchten. Es soll vermieden werden, dass sich die Prüflinge gezwungen sehen, an einer Online-Prüfung teilzunehmen, die über dem heimischen Rechner angeboten wird.

### 2. Wo möglich datensparsame Prüfungsformate einsetzen

Besonders datensparsam sind beispielsweise Formate wie open-Book-Ausarbeitungen (=Kurz-Hausarbeit; eine unbeaufsichtigte, schriftliche oder elektronische Prüfung). Wenn die Prüfungssituation keine engmaschige Kontrolle erfordert, sollten solche Prüfungsformate bevorzugt eingesetzt werden. Sie verschaffen den Grundsätzen der Datenverarbeitung nach Art. 5 DS-GVO größtmögliche Geltung und schränken die Grundrechte der Prüflinge am wenigsten ein.

### 3. Einsatz datenschutzgerechter Videokonferenzdienste

Aufgrund der seit dem 1. Dezember 2021 neuen Regelungen im Telekommunikationsgesetz (TKG) ordnen wir Videokonferenzdienste nunmehr im Kern als Telekommunikationsdienste ein, die nach § 29 Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG) unter der Aufsicht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) stehen. Dies gilt jedenfalls, soweit diese Dienste eine interpersonelle Kommunikation ermöglichen und der Benutzerkreis nicht völlig offen ist. Soweit § 3 Nr. 24 TKG für das Vorliegen eines interpersonellen Telekommunikationsdienstes verlangt, dass „die Empfänger von den Personen bestimmt werden, die die Telekommunikation veranlassen oder daran beteiligt sind“, genügt es nach Auffassung der LDI NRW auch, wenn die Videokonferenz dadurch zustande kommt, dass der Veranlasser der Konferenz einen Link zu einem virtuellen Konferenzraum an die Teilnehmer versendet. Schließlich ist auch davon auszugehen, dass Videokonferenzdienste grundsätzlich gegen Entgelt angeboten werden.

In Konsequenz dieser Bewertung ist für die Datenverarbeitung im Rahmen der Erbringung des Telekommunikationsdienstes nicht der Nutzer dieses Dienstes verantwortlich, sondern der Anbieter von Telekommunikationsdiensten. Zu den personenbezogenen Daten, für deren Verarbeitung demnach nicht die Hochschule, sondern der Anbieter von Telekommunikationsdiensten selbst verantwortlich ist, zählen insbesondere die Metadaten (hierzu gehören z.B. IP-Adressen, die übertragene Datenmenge, der Browsertyp, das Betriebssystem und Informationen darüber, wer wann mit wem kommuniziert). Dasselbe gilt für die technischen Übertragungsdaten in Bezug auf den Transport der Inhaltsdaten (Fernmeldegeheimnis).

Diese Änderung hat auch Konsequenzen für die aufsichtsbehördlichen Zuständigkeiten. So ist der BfDI nach § 29 TTDSG für die datenschutzrechtliche Aufsicht über geschäftsmäßig erbrachte Telekommunikationsdienste zuständig. Damit fällt grundsätzlich auch die Aufsicht über Videokonferenzdienste in seine Zuständigkeit (zur Aufsicht über von den Hochschulen selbst erbrachte Videokonferenzdienste s.u.).

Die LDI NRW bleibt zuständig für die datenschutzrechtliche Aufsicht über die Datenverarbeitung der Stellen, die die Videokonferenzdienste nutzen. Diese Stellen, so auch die Hochschulen, sind nach wie vor insbesondere für die Verarbeitung der personenbezogenen Daten im Zusammenhang mit der **Herstellung der Kommunikation** (beispielsweise Verwendung von E-Mail-Adressen zur Übersendung des Besprechungslinks) und die personenbezogenen **Inhaltsdaten** verantwortlich (z. B. für die Video- und Chat-Inhalte), sofern diese durch die Hochschule aufgezeichnet und damit für weitere Zwecke verarbeitet werden. Sie sind daher im Rahmen des Art. 32 DS-GVO verpflichtet, solche Anbieter auszuwählen, die eine der jeweiligen Sensibilität der Daten angemessene Verschlüsselung der Inhalte sowie ein entsprechendes Löschkonzept anbieten. Zudem müssen sie für möglichst **datenschutzfreundliche Voreinstellungen** bei der Nutzung der Dienste sorgen.

Videokonferenzsysteme sollten grundsätzlich so konfiguriert sein, dass zusätzlich zu einer obligatorischen Transportverschlüsselung eine Ende-zu-Ende-Verschlüsselung zwischen den Teilnehmenden erfolgt, so dass auf dem Server nur verschlüsselte Daten verarbeitet werden. Weiterhin sollten die Kamera, das Mikrofon und das Teilen des Bildschirms von Teilnehmenden vor Eintritt in die Konferenz standardmäßig ausgeschaltet sein und nur von den Teilnehmenden selbst aktiviert werden können.

Sofern datenschutzrechtliche Probleme in Bezug auf einen Videokonferenzdienst hinlänglich bekannt sind, sind die Hochschulen als öffentliche Stellen verpflichtet, diese im Rahmen der Auswahl der in ihrem Verantwortungsbereich eingesetzten Videokonferenzdienste zu berücksichtigen und gegebenenfalls auf ihren Einsatz zu verzichten.

Die Hochschulen sind verpflichtet, auch beim Einsatz von Telekommunikationsdiensten auf die Datensparsamkeit zu achten und Einstellungen so zu wählen, dass möglichst wenig Nutzerdaten verarbeitet werden.

### 3.1. Sog. „Misch-Dienste“

Bei „Misch-Diensten“, in denen Elemente von Telekommunikationsdiensten mit anderen Dienstleistungen kombiniert werden (z.B. Videokonferenzdienst mit einem Dokumentenverwaltungssystem) werden in den Verträgen die unterschiedlichen Verantwortlichkeiten zu berücksichtigen sein:

- Die Hochschulen als die den Dienst nutzenden Stellen sind für die Verarbeitung der Inhaltsdaten, also insbesondere für die Verarbeitung der Audio-, Video- und Chat-Inhalte selbst verantwortlich. Sofern der Dienstanbieter Prozesse anbietet, die der Verarbeitung von Inhaltsdaten dienen (z. B. Speicherung/Bearbeitung von Dokumentationen, Speicherung von Video-/Audioinhalten), sind hierüber Auftragsverarbeitungsverträge zu schließen.
- Die Hochschulen müssen hingegen keine Auftragsverarbeitungsvertragsregelungen mit den Dienstleistern für Prozesse treffen, für die sie selbst nicht verantwortlich sind. Dies gilt insbesondere für die Verarbeitung der Metadaten, die dem TKG unterliegen. Aber auch für den Transport der Inhaltsdaten sind die Hochschulen als die den Videokonferenzdienst nutzenden Stellen nicht verantwortlich, sondern der Anbieter von Telekommunikationsdiensten (diesem obliegt die Gewährleistung des Fernmeldegeheimnisses).
- Allerdings ist die den Videokonferenzdienst nutzende Stelle gemäß Art. 32 DS-GVO zur Gewährleistung technischer und organisatorischer Maßnahmen für die Sicherheit der Verarbeitung der Inhaltsdaten verpflichtet. Sie müssen die Inhalte je nach ihrer Sensibilität angemessen verschlüsseln und ein Löschkonzept erstellen. Dies spricht dafür, entsprechende Klauseln in den Vertrag mit dem Anbieter von Telekommunikationsdiensten (nicht zu verwechseln mit dem Auftragsverarbeitungsvertrag nach Art. 28 DS-GVO) aufzunehmen.

### 3.2. Durch die Hochschulen selbst betriebene Videokonferenzdienste

Die Zuständigkeit des BfDI nach § 29 TTDSG bezieht sich nur auf geschäftsmäßig erbrachte Telekommunikationsdienste. Geschäftsmäßig werden Dienste nur erbracht, sofern sie einerseits nachhaltig erbracht und andererseits an außerhalb der

Sphäre des Anbieters liegende Dritten gerichtet sind. Von den Hochschulen selbst betriebene Dienste (hierzu gehören auch E-Mail-Dienste) werden, solange sie ausschließlich durch die jeweilige Hochschule betrieben und durch sie selbst genutzt werden, nicht geschäftsmäßig erbracht.

Daher fallen derartige Dienste nicht in die Zuständigkeit des BfDI nach § 29 Abs. 1 TTDSG. Auch der BfDI teilt diese Einschätzung. Danach ist nicht der BfDI, sondern die LDI NRW die zuständige Aufsichtsbehörde, soweit es sich um rein intern genutzte Dienste der Hochschule handelt. Anders ist es möglicherweise zu beurteilen, wenn den Prüflingen / Mitarbeiter\*innen die private Nutzung der Dienste gestattet wird.

Derzeit wird von der der Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine neue Orientierungshilfe „Datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ erarbeitet, in der diese Fragen vertieft aufgegriffen werden sollen.

## Ausblick

Unabhängig von den Empfehlungen an die Hochschulen, die in der Pflicht sind, durch technische und organisatorische Maßnahmen sicherzustellen, dass der Schutz der verarbeiteten Daten gemäß Art. 32 in Verbindung mit Art. 5 DS-GVO gewährleistet ist, kann im Sinne einer Vereinheitlichung des Datenschutzniveaus eine landesweite Lösung sinnvoll sein.

Wir machen darauf aufmerksam, dass das Bayerische Staatsministerium für Wissenschaft und Kunst eine Verordnung (Bayerische Fernprüfungserprobungsverordnung – BayFEV) vom 16. September 2020) erlassen hat, die – vor die Klammer gezogen – die Voraussetzungen zur Durchführung von Online-Prüfungen für sämtliche Hochschulen regelt (u.a. Regelungen zur Authentifizierung, Videoaufsicht und zum Verhalten bei technischen Störungen). Diese Verordnung stellt bereits eine geeignete Rechtsgrundlage für die Durchführung von Online-Prüfungen und die damit einhergehende Datenverarbeitung dar.

Solange es in NRW eine solche Verordnung nicht gibt, müssen die Hochschulen selbst unter dem Gesichtspunkt der Rechtssicherheit und des Bestimmtheitsgrundsatzes normenklare, datenschutzgerechte Festlegungen treffen und in den Prüfungsordnungen die Eingriffsgrenzen der vorgesehenen Maßnahmen hinsichtlich der Art und Weise der Durchführung von Online-Prüfungen und die mit der jeweiligen Maßnahme verfolgten Zwecke differenziert festlegen.