Team Datenschutz TU Berlin
Hiller Hoffmeier Neiling
18.11.2020

Videoüberwachung von schriftlichen Onlineprüfungen im datenschutzrechtlichen Fokus
(Stand November 2020)

Vorbemerkung:

Diese datenschutzrechtliche Einschätzung bezieht sich auf den generellen Einsatz von Kameras gegenüber den Prüflingen zur Vermeidung von Täuschungsversuchen (= Videoüberwachung) bei Online-Klausuren inkl. Multiple-Choice-Tests, obwohl eine Videoüberwachung an der TU Berlin derzeit nicht vorgesehen ist.
Betrachtet werden hier nur die Herausforderungen, die hinsichtlich des technisch-organisatorischen Ablaufs auftreten können. Vorgaben für die Identitätsprüfung müssen von der Fachabteilung beigesteuert werden. Hier muss insbesondere geklärt werden, in welchen Fällen ein Login mit dem persönlichen TU-Account ausreicht oder ob weitere Maßnahmen erforderlich sind, um „Ghostwriting" zu erkennen. Problematisch wird neben der Nutzung unerlaubter Hilfsmittel auch das „Helfen" weiterer Personen eingeschätzt, die entweder in räumlicher Nähe des Prüflings oder über elektronische Kommunikationsmittel eingebunden werden könnten. Gern prüfen wir auch die diesbezüglich vorgesehenen Maßnahmen auf ihre datenschutzrechtliche Zulässigkeit.

Der prüfungsrechtliche Grundsatz der Chancengleichheit wird daher im Folgenden auch nur selektiv betrachtet und muss abschließend von der Fachabteilung (I B) beurteilt werden.

Rechtsgrundsätze bei der Videoüberwachung:

- Nach ständiger Rechtsprechung des BVerfG stellt jede Form der Videoüberwachung einen Eingriff in das Persönlichkeitsrecht der davon betroffenen Personen dar und Bedarf somit einer **Rechtsgrundlage**, also einer ermächtigenden Rechtsnorm oder einer (freiwilligen) Einwilligung.

- Die Hochschulen haben auch bei Online-Prüfungen den sich aus Art. 3 und 12 GG ergebenen prüfungsrechtlichen Grundsatz der **Chancengleichheit** zu beachten, insbesondere bei der technischen Ausstattung der Prüflinge.

- Beim Einsatz von Videoüberwachung ist stets der Grundsatz der **Verhältnismäßigkeit** zu beachten.

I. Rechtsgrundlagen nach der DSGVO

Als mögliche Rechtsgrundlagen für den Einsatz von Videoüberwachungsmethoden bei Onlineprüfungen könnten die folgenden Normen in Frage kommen:

- die Einwilligung (Art. 6 Abs. 1 lit. a DSGVO),
- die Ausübung der übertragenen öffentlichen Gewalt (Art. 6 Abs. 1 lit. e alt. 2 DSGVO) sowie
- die Wahrung eines öffentlichen Interesses im erforderlichen Umfang (Art. 6 Abs. 1 lit. e alt. 1 DSGVO).

Nicht anwendbar in diesem Zusammenhang ist:

- die Videoüberwachung der öffentlichen Hand gemäß Art. 6 Abs. 1 lit. e DSGVO iVm § 20 BlnDSG, da diese ausschließlich für öffentlich zugängliche Bereiche (Abs. 1) oder zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Vermeidung von Straftaten (Abs. 3) erfolgen darf. Eine Überwachung des privaten Bereichs ist von dieser Vorschrift nicht abgedeckt.
- das berechtigte Interesse nach Art. 6 Abs. 1 lit. f DSGVO. Diese Norm findet keine Anwendung für Behörden im Rahmen Ihrer Aufgabenerfüllung (Art. 6 Abs. 1 Satz 2 DSGVO).

a. Einwilligung

Die Einwilligung zur Videoüberwachung bei Online-Prüfungen muss immer freiwillig erfolgen. In jedem Einzelfall ist dabei ein mögliches Machtgefälle zwischen der Hochschule und den Studierenden zu prüfen und zu vermeiden. Nach Erwägungsgrund 43 Satz 1 DSGVO ein solches Ungleichgewicht grundsätzlich immer anzunehmen, wenn es sich bei der datenverarbeitenden Stelle um eine Behörde handelt.

Insofern sind die Anforderungen an eine wirksame Einwilligung sehr hoch. Nach unserer Auffassung ist eine Einwilligung nur zulässig, wenn eine die Chancengleichheit wahrende Prüfungsalternative angeboten wird, was in der Regel nicht möglich sein wird.
Ein weiteres Problem stellt in diesem Zusammenhang die Tatsache dar, dass die Einwilligung datenschutzrechtlich jederzeitig und uneingeschränkt ohne Angabe von Gründen für die Zukunft widerrufen werden darf, was aber nach Prüfungsrecht einen angetretenen Fehlversuch auslösen würde.

> **Die Einwilligung ist als Rechtsgrundlage für die Videoüberwachung von Onlineprüfungen somit ungeeignet.**

b. Ausübung der übertragenen öffentlichen Gewalt bzw. Wahrung des öffentlichen Interesses im erforderlichen Umfang

aa. Art. 6 Abs. 1 lit. e DSGVO iVm mit § 6b BerlHG i.V.m. § 1 Nr. 47 StudDatVO

Als Rechtsgrundlage könnte Art. 6 Abs. 1 lit. e DSGVO i.V.m. mit § 6b BerlHG i.V.m. § 1 Nr. 47 StudDatVO (Verarbeitung personenbezogener Daten im Zusammenhang mit elektronischer Prüfung) in Betracht kommen.

Gemäß Erwägungsgrund 41 Satz 2 DSGVO muss die entsprechende Rechtsgrundlage oder Gesetzgebungsmaßnahme klar und präzise sein und ihre Anwendung für die Rechtsunterworfenen

gemäß der Rechtsprechung des Gerichtshofs der Europäischen Union und des Europäischen Gerichtshofs für Menschenrechte vorhersehbar sein.

> **Demnach ist das Fehlen der Maßnahme "Videoüberwachung" in § 1 Nr. 47 StudDatVO aus Sicht des Datenschutzes als rechtskritisch anzusehen.**

bb. § 5 Abs. 12 S. 2 SARS-CoV-2-Infektionsschutzverordnung
Eine Rechtsgrundlage für Anwendung von Videoüberwachungsmaßnahmen von Online-Prüfungen könnte sich auch aus § 5 Abs. 12 S. 2 SARS-CoV-2-Infektionsschutzverordnung (Stand: 10/2020) ergeben. Danach haben die Hochschulen ihren Lehrbetrieb im Wintersemester 2020/21 ab dem 02.11.2020 grundsätzlich im Online-Format und nicht im Präsenzbetrieb durchzuführen.

Allerdings dürfen Prüfungen gemäß Satz 3 dieser Verordnung unter Beachtung der grundsätzlichen Pflichten, der Schutz- und Hygieneregeln sowie der jeweils in den Hochschulen geltenden besonderen Bestimmungen in Präsenzform durchgeführt werden.

Mit dem Berliner Stufenplan für den Hochschulbetrieb unter Pandemiebedingungen
wird die Durchführung von Präsenzprüfungen weiter eingeschränkt. In Stufe 2 dürfen diese noch eingeschränkt, in der Stufe 3 (mit Ausnahme von Zulassungs- und Abschlussprüfungen) grundsätzlich nicht mehr abgehalten werden.

> **Auch hier fehlt es an der aufgrund der Eingriffstiefe (Grundrecht!) erforderlichen Nennung der konkreten Maßnahme „Videoüberwachung" in der Rechtsgrundlage.**

cc. Art. 6 Abs. 2 DSGVO i.V.m. § 32 Abs. 8 BerlHG
Gemäß Art. 6 Abs. 2 DSGVO können die Mitgliedstaaten „spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen…". Vorgaben über eine erforderliche Wertigkeit der Vorschrift innerhalb einer Normenhierarchie fehlen jedoch.

Insofern könnte die Hochschule entsprechend der Ermächtigungsnorm des § 32 Abs. 8 BerlHG die Möglichkeit und die Voraussetzungen für den Einsatz elektronischer Prüfungsformate schaffen, wovon die TU in § 44 Absatz 1 Satz 2 AllgStuPO Gebrauch gemacht hat.

> **Videoüberwachung ist aber <u>kein</u> notwendiger Bestandsteil von Prüfungsformaten. Sie stellt einen erheblichen Grundrechteingriff dar, der nach gängiger Auffassung ausdrücklich durch (Landes-)Gesetz geregelt werden müsste[1].**

c. weitere Rechtsgrundlagen und Fazit

Eine weitere Rechtsgrundlage kommt nicht in Betracht.

> **Fazit: Videoüberwachung ist mangels Rechtsgrundlage unrechtmäßig.**

[1] Eine Klage eines aufgrund unrechtmäßiger Videoüberwachung ausgeschlossenen Prüflings könnte u.U. einen Schadensersatzanspruch gegen die Hochschule auslösen. Dieser könnte sich beispielsweise auf die Kosten, die eine weiteres Semester verursacht oder gar entgangene Einkünfte aufgrund eines verzögerten Berufseintritt belaufen.

Insofern müssen andere Mittel zur Kontrolle hinsichtlich Täuschungsversuchen eingesetzt werden.

II. Chancengleichheit

Technische Probleme können die Wahrung der Chancengleichheit gefährden.

Bei der Gewährleistung gleicher technischer Voraussetzungen durch die Hochschule können insbesondere Probleme auftreten durch die:

- unterschiedliche Schnelligkeit und Persistenz der verschiedenen Internetzugänge,
- unterschiedliche Leistungsfähigkeit der zur Prüfung benutzten Rechner, wie Kameraausstattung, Betriebssystem, Arbeitsspeicher oder CPU sowie
- Zuordnung der Verantwortung für technische Probleme während der Online-Prüfung zwischen der Hochschule und den Studierenden.

III. Verhältnismäßigkeit

Gemäß Abs. 3 Satz 2 Satz 1 a.a.O. muss die Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die der verantwortlichen Stelle übertragen wurde.

Erforderlich ist ein Mittel, soweit kein milderes, gleich geeignetes Mittel zur Verfügung steht.
Ein Mittel ist **geeignet**, wenn es die Zweckerreichung zumindest fördert. Das Merkmal der Geeignetheit setzt somit nicht voraus, dass das verfolgte Ziel stets und vollumfänglich erreicht wird. Vielmehr ist ausreichend, dass das eingesetzte Mittel die Wahrscheinlichkeit erhöht.

Bei (unzulässiger) Videoüberwachung wird oft auf abweichendes Verhalten geprüft, bspw. ob der*die zu Prüfende den Fokus auf die Online-Klausur hat, anderweitig kommuniziert oder im Internet nach Lösungen sucht.

Bei der Klausur-Kontrolle ohne Videoüberwachung müssen andere Kontrollmittel herangezogen werden, z.B.

- eine verdächtig lange Unterbrechung der Schreib-Aktivität bei der Online-Klausur.
- Änderung der Klausurmodalitäten:
  - Open-Book-Klausuren
  - verschiedene Varianten der gleichen Klausur (andere Reihenfolge der Fragen, unterschiedliche Werte etc)

Es ist zu beachten, dass als gleich geeignetes, **milderes Mittel**, immer die Durchführung von Präsenzprüfungen anzusehen ist, so dass dieser nach Möglichkeit der Vorrang zu geben ist. Dort ist es für die Aufsichtspersonen regelmäßig deutlich einfacher zu erkennen, wenn ein Prüfling nicht erlaubte Hilfsmittel verwendet oder sich mit anderen Klausurteilnehmern austauscht. Zudem werden im Rahmen einer Präsenzprüfung im Vergleich zur Überwachung von Online-Prüfungen viel weniger personenbezogene Daten automatisch oder im Rahmen eines Dateisystems verarbeitet.

Unter den derzeitigen Pandemiebedingungen sind Präsenzprüfungen leider ausgeschlossen.

IV. Ergebnis

Derzeit ist eine Videoüberwachung von Online-Klausuren nicht zulässig. Soweit eine solche geplant ist, bedarf es einer landesgesetzlichen Rechtsgrundlage.

Erforderliche Maßnahmen

- § 32 BerlHG ist durch den Landesgesetzgeber um Videoüberwachung zu erweitern

- Eine hochschulweiten Prüfungsordnung nach § 32 Abs. 8 BerlHG zur Regelung einheitlicher sowie detaillierter rechtlicher und technischer Vorgaben für Online-Prüfungen ist zu erlassen. Dabei ist der Einsatz von Gesichtsauswertungstools sowie das Aufzeichnen und Speichern jeglicher Audio- und Videosequenzen zu verbieten.

  Zur Minimierung eines Eingriffs in das Persönlichkeitsrecht der Prüflinge durch eine Videoüberwachung ist für jedes Modul zu prüfen, inwieweit anstelle einer online zu überwachenden Klausur die Umwidmung in eine mündliche- bzw. Open-Book-Online-Prüfung möglich und rechtlich zulässig ist.

- Es sind begleitende technische Maßnahmen, z.B. Logging von IP-Adressen während der Prüfung, die im Verdachtsfall nachträglich herangezogen werden können (z.B. bei Verdacht eines örtlich getrennten Ghostwriters), zu nutzen. Solche Maßnahmen sind auf ihre Rechtmäßigkeit in Bezug auf Prüfungsrecht und Datenschutz vorab zu prüfen und genehmigungspflichtig.

- Die Studierenden sind im Vorfeld umfassend über die Datenverarbeitung im Rahmen ihrer Prüfung und Prüfungskontrolle zu informieren, Art. 13 DSGVO.

- Die zur Prüfung eingesetzten Tools müssen vorher das gesetzlich vorgeschriebene Genehmigungsverfahren sowie eine Datenschutzprüfung durchlaufen haben (Derzeit sind an der TU ausschließlich Tests in ISIS und Open-Book-Klausuren mit Upload erlaubt).

V. Aspekt: Identifizierung von Prüflingen

Ein weiterer wichtiger Aspekt ist die korrekte Identifizierung der Prüflinge, die sichergestellt werden muss. Bei Online-Prüfungen sind technische Maßnahmen dazu zwingend erforderlich, u.a.:

- Hauptidentifizierung über den TU-Account
- Sicherstellung der Identität über 2-Faktor-Authentifizierung mit TU-Login und weiterem Faktor wie z.B. TAN / mTAN oder Token
- Kamerabasiertes Identifikationsverfahren (Web-Ident) für mindestens den Account (z.B. mittels Ausweis)

[Weiterführender Hinweis: Soweit andere Fälle von Datenerhebung über kamerabasierte Systeme beabsichtigt sind, ist das Team Datenschutz zwingend im Vorfeld einzubinden.]