E-Assessment NRW

Handlungsempfehlung zu Anforderungen an das Prüfungssystem und die Datenverarbeitung (Authentizität, Integrität, Vertraulichkeit)

Aus dem Grundgesetz und dem Datenschutzgesetz NRW ergeben sich bestimmte Anforderungen an das Prüfungssystem und die Datenverarbeitung, um die Authentizität, Integrität und Vertraulichkeit einer Prüfungsleistung zu gewährleisten.

Diese Handlungsempfehlung stellt die rechtlichen Grundlagen dar, erläutert die Vor- und Nachteile verschiedener Möglichkeiten der Verarbeitung von Prüfungsdaten und verweist auf konkrete Beispiele bei bestehenden Prüfungssystemen.

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken

BERGISCHE UNIVERSITÄT WUPPERTAL

Hochschule Ostwestfalen-Lippe
University of Applied Sciences

Hochschule Niederrhein
University of Applied Sciences

UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Inhaltsverzeichnis

Haftungsausschluss

Diese Handlungsempfehlung dient ausschließlich der Information und nicht der Beratung im Einzelfall. Sie basiert weitgehend auf einem rechtswissenschaftlichen Gutachten, das im Auftrag des Projektes E-Assessment NRW von Prof. Dr. Nikolaus Forgó, Simon Graupe und Julia Pfeiffenbring erstellt und 2016 unter dem Titel *Rechtliche Aspekte von E-Assessments an Hochschulen* publiziert wurde. Bei konkreten rechtlichen Fragen wenden Sie sich bitte an die zuständige Stelle Ihrer Hochschule oder lassen Sie sich anwaltlich beraten. Die Autoren/innen und das Projekt E-Assessment NRW übernehmen keine Haftung.

E-Assessment NRW (2017)

unter dem Dach von: DH-NRW gefördert durch: Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

1. Einführung

Neben den verfassungsrechtlichen Grundlagen, welche die Gestaltung der Prüfungsordnung betreffen, ergeben sich aus dem Datenschutzgesetz NRW auch bestimmte Anforderungen an das Prüfungssystem und die Datenverarbeitung, um die Authentizität, Integrität und Vertraulichkeit einer Prüfungsleistung zu gewährleisten.

So muss das Prüfungssystem im Hinblick auf informationstechnische Sicherheit derart beschaffen sein, dass es das Recht auf **informationelle Selbstbestimmung** berücksichtigt, eine Ausprägung des allgemeinen Persönlichkeitsrechts nach **Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG**. Datenverarbeitungen wie die Erhebung von Name, Matrikelnummer oder pseudonymisierter Prüfungskennziffer sind rechtfertigungsbedürftig und müssen sich am Grundsatz der Erforderlichkeit orientieren (Forgó et al., 2016, S. 12).[1]

Um dieses Grundrecht gewährleisten zu können, muss zunächst die Authentizität der Prüfungsergebnisse sichergestellt werden, indem eine zweifelsfreie Identifikation des Prüfungsteilnehmers erfolgt und die Prüfungsleistung dem Prüfungsteilnehmer eindeutig zugeordnet wird. Bei elektronischen Prüfungsleistungen ist der eindeutige Identitätsnachweis einer Person nicht allein durch den Abgleich eines Studierendenausweises in Kombination mit einer Unterschrift, wie im Falle einer schriftlichen Prüfung, gegeben (Forgó et al., 2016, S. 20f.).

Weiterhin muss das Grundrecht auf **Vertraulichkeit und Integrität informationstechnischer Systeme** (IT-Grundrecht) gewährleistet sein, welches ebenfalls eine Ausprägung des allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ist. Die Integrität des informationstechnischen Systems kann besonders dann gefährdet sein, wenn die Prüfungsteilnehmer für die Prüfung private Geräte verwenden (*Bring Your Own Device*). Ein heimlicher Zugriff auf persönliche Daten der Prüfungsteilnehmer durch die verwendete Software muss verhindert werden (Forgó et al., 2016, S. 12f.).

Ebenso muss die Integrität der Daten gewährleistet werden, also das fehlerfreie Funktionieren der Hard- und Software sowie das fehlerfreie Senden, Verarbeiten und Archivieren der Prüfungsdaten. Daten dürfen nach dem Abschluss der Prüfung nicht (weder durch technische Fehlfunktionen noch durch menschliche Manipulation) verfälscht werden können. Die Vertraulichkeit der erhobenen Daten muss dementsprechend ebenfalls sichergestellt werden, damit Unbefugte sie nicht verändern oder überhaupt Prüfungsleistungen einsehen können.

Im Folgenden werden Empfehlungen für das Prüfungsamt formuliert, um im Falle einer gerichtlichen Prüfung die Authentizität und Integrität einer Prüfungsleistung ausreichend nachweisen zu können. Dabei ist zwischen elektronischen Prüfungen unter Aufsicht und Prüfungen ohne Aufsicht zu unterscheiden.

1 Nordrhein-westfälische Hochschulen können sich an den Erlaubnisvorschriften zur Datenerhebung des Datenschutzgesetzes NRW (ins besondere §§ 12 und 13 DSG NRW) orientieren (Forgó et al., 2016, S. 12). Abgerufen von: https://recht.nrw.de/lmi/owa/br_text_anzeigen?vid=3520071121100436275, zuletzt am 16.08.2017.

2. Elektronische Prüfungen unter Aufsicht

Da nach der Durchführung einer elektronischen Prüfung keine Privaturkunde vorliegt,[2] sollte die Prüfungsbehörde andere Beweise generieren, welche die Unanfechtbarkeit der Prüfung garantieren. Die grundsätzliche Notwendigkeit einer Sicherung der Authentizität und Integrität der Prüfungs-leistung sollte aus der Prüfungsordnung hervorgehen, jedoch ohne Festlegung genauer Regeln, da diese vom jeweiligen Stand der Technik abhängig sind.

2.1. Anforderungen an das Prüfungssystem

Um die Integrität der Prüfungsleistung zu gewährleisten, muss die einwandfreie Funktionsfähigkeit des Prüfungssystems sichergestellt sein. Dazu gehören die Wartung und Erneuerung der Hardware, das Aktualisieren der Software sowie das Bereitstellen ausreichender technischer Geräte für alle Prüfungsteilnehmer. Keinesfalls dürfen Prüfungsteilnehmer während der Prüfung durch Funktionsmängel benachteiligt werden. Technische Ausfälle oder ähnliche Vorkommnisse müssen durch eine Verlängerung der Prüfungsdauer ausgeglichen werden.

Zur prinzipiellen Funktionsfähigkeit des Prüfungssystems gehört auch, dass das System Änderungen der Eingabe während der Prüfung gestattet. Solche Änderungen bzw. ein Springen zwischen den Aufgaben sind in einer Papierklausur stets möglich und sollten daher auch in einer elektronischen Prüfung vorgesehen sein. Dies ist zur Sicherung der Chancengleichheit notwendig, gerade auch dann, wenn das elektronische Prüfungssystem die Reihenfolge der Fragestellungen auf Wunsch des Prüfers zur Verhinderung von Täuschungsversuchen bei jedem Prüfungsteilnehmer verändert (Forgó et al., 2016, S. 21f.).

In diesem Kapitel werden unterschiedliche Möglichkeiten zur Feststellung der Identität der Prüfungsteilnehmer und der Integrität und Originalität der Prüfungsleistung vorgestellt. Jede dieser Maßnahmen kann die rechtliche Absicherung erhöhen, jedoch keine absolute Sicherheit im Sinne einer Erfolgsgarantie im Klagefall bieten, da Gerichte stets einzelfallbezogen entscheiden.

2.2. Nachweis der Identität des Prüfungsteilnehmers und der Integrität der Prüfungsleistung

2.2.1. Ausweiskontrolle

Die Aufsicht kann die Identität der Prüfungsteilnehmer durch eine Einlasskontrolle und den Abgleich des Studierendenausweises mit Lichtbild (alternativ: Lichtbild des Personalausweises) mit der Liste der zur Prüfung zugelassenen Studierenden eindeutig feststellen.

Zusätzlich wird die Zuweisung eines festen Bearbeitungsplatzes empfohlen, für den auch ein personalisierter Account mit Passwort zur Anmeldung erstellt werden kann. Alternativ können sich die Prüfungsteilnehmer mit ihrem jeweiligen Benutzernamen und einem einheitlichen Passwort anmelden, das speziell für die Klausur festgelegt wurde.

2 Ein Prüfungsdokument ist dann als Privaturkunde einzustufen, wenn es vom Prüfling handschriftlich unterzeichnet wurde. Vgl. § 416 ZPO: „Privaturkunden begründen, sofern sie von den Ausstellern unterschrieben oder mittels notariell beglaubigten Handzeichens unterzeichnet sind, vollen Beweis dafür, dass die in ihnen enthaltenen Erklärungen von den Ausstellern abgegeben sind.“ Abgerufen von: www.gesetze-im-internet.de/zpo, zuletzt am 13.09.2017.

Während der Prüfung kann die Identität der Prüfungsteilnehmer durch die Aufsicht festgestellt werden, indem Name und Matrikelnummer auf dem dauerhaft am Bearbeitungsplatz ausgelegten Studierendenausweis mit den Angaben auf dem Monitor verglichen werden (Forgó et al., 2016, S. 22).

2.2.2. Log-Datei

In einer Log-Datei werden – je nach Ausgestaltung des Prüfungssystems – alle oder bestimmte Prozesse bzw. Eingaben auf einem Computersystem protokolliert. Die reine Log-Datei ist jedoch aufgrund ihrer Dateieigenschaft im Nachhinein veränderbar und somit kein Beweis der Integrität der Prüfungsleistung. Zusätzlich müssten die Protokollaufzeichnungen elektronisch signiert und mit einem Zeitstempel versehen werden (Forgó et al., 2016, S. 22f.).

2.2.3. IP-Adresse in Verbindung mit dem Loginnamen des Prüfungsteilnehmers und der Log-Datei

Die IP-Adresse wird in Verbindung mit dem Loginnamen des Prüfungsteilnehmers und der Log-Datei gespeichert. Außerdem sollte die Prüfungsbehörde die Log-Datei mit einem Zeitstempel und Hashwert signieren (Forgó et al., 2016, S. 25).

Generell gilt: Alle Daten sollten bis zur Unanfechtbarkeit der Prüfung aufbewahrt werden. Enthält die Prüfungsordnung keine Prüfungsprotokollpflicht, liegt es im Ermessen des Prüfers, welche Aufzeichnungen – einschließlich der Erstellung von Protokolldateien – er anfertigt. Im Sinne des effektiven Rechtsschutzes sollte daher in der Prüfungsordnung festgelegt sein, ob ein Prüfungsprotokoll anzufertigen ist und welchen Mindestinhalt es haben muss (Forgó et al., 2016, S. 25). Eine Protokolldatei kann dabei kein schriftliches Prüfungsprotokoll ersetzen, da nicht jeder detaillierte Vorgang wie z. B. Unterbrechungen durch Toilettengänge oder Täuschungsversuche protokolliert werden können (Forgó et al., 2016, S. 24).

2.3. Nachweis der Originalität der Prüfungsleistung

2.3.1. Qualifizierte elektronische Signatur

Eine elektronische Prüfung wird durch ihren Ausdruck zu einem schriftlichen Dokument. Durch eine Unterschrift erhält sie Urkundenqualität und ist somit eine Privaturkunde, welche die Originalität der Prüfungsleistung zweifelsfrei nachweist. Soll ein solcher Systembruch vermieden werden, ist die qualifizierte elektronische Signatur nach **§ 2 Nr. 3 SigG** eine geeignete Methode des eindeutigen Nachweises. Sie besteht zusätzlich zur einfachen elektronischen Signatur (eingescannte Unterschrift) aus einem Hashwert (Prüfsumme), der an die zu unterschreibende Datei gehängt wird. Nachträglich können keine Veränderungen vorgenommen werden, ohne den Hashwert zu verändern.

Diese Methode ist allerdings aufwändig, da die qualifizierte elektronische Signatur von Zertifizierungsdiensteanbietern erstellt werden muss und die Prüfungsteilnehmer schriftlich in die Datenweitergabe an den Anbieter einwilligen müssen (Forgó et al., 2016, S. 28-30).

2.3.2. Mehrfachbestätigung

Im Vergleich zum analogen Prüfungsverfahren ist die Mehrfachbestätigung der endgültigen Übermittlung einer Prüfungsleistung durch den Prüfungsteilnehmer, welcher die Speicherung der Prüfungsleistung in ein nicht mehr veränderbares Dateiformat folgt, der Abgabe der schriftlichen Klausur gleichzusetzen. In Kombination mit einer Ausweiskontrolle und dem Nachweis der Funktionsfähigkeit des Prüfungssystems durch die Prüfungsbehörde kann

die Mehrfachbestätigung eine sinnvolle Methode zum Nachweis der Integrität und Authentizität einer Prüfung sein. Außerdem informiert die Mehrfachbestätigung den Prüfungsteilnehmer eindeutig darüber, dass die Bearbeitung der Prüfung beendet ist (Forgó et al., 2016, S. 30).

2.3.3. Zeitstempel und Hashwert

Ein Hashwert gibt eine große Eingabemenge komprimiert in kleinen Ausgabemengen wieder. Kleinste Änderungen an einer Datei erzeugen einen anderen Hashwert. Dieser Wert wird durch einen Zeitstempelserver mit einem Zeitstempel versehen. Ohne qualifizierte elektronische Signatur entspricht die Datei jedoch keiner Privaturkunde. Um sich rechtlich abzusichern, könnten Teilnehmer daher einen Ausdruck des Hashwertes unterschreiben (Forgó et al., 2016, S. 30f.).

2.3.4. Videoaufzeichnungen der Prüfungsteilnehmer

Ein Nachweis der Authentizität und Integrität der Prüfungsleistung könnte auch durch eine Videoaufzeichnung der Prüfungsteilnehmer erfolgen. Da ein solches Vorgehen jedoch stark in das Grundrecht auf informationelle Selbstbestimmung eingreift und der Nachweis durch Aufsichtspersonal mindestens ebenso gut erbracht werden kann, ist davon abzuraten (Forgó et al., 2016, S. 31f.).

3. Elektronische Prüfungen ohne Aufsicht

Bei elektronischen Prüfungen ohne Aufsicht ist eine Gewährleistung der Authentizität und Integrität der Prüfungsleistung sehr schwierig bis unmöglich. Auch ist es kaum möglich, Täuschungsversuche nachzuweisen und gegen diese vorzugehen. Im Folgenden werden Ansätze zur Lösung dieser Probleme vorgestellt, die jedoch allesamt keine ausreichende Sicherheit bieten. Ausgehend vom aktuellen Stand der Technik ist daher derzeit von der Durchführung elektronischer Prüfungen ohne Aufsicht abzuraten.

3.1. PIN-/TAN-Verfahren

Mithilfe des PIN-/TAN-Verfahrens soll die Identität eines Prüfungsteilnehmers nachgewiesen werden, indem dieser sich bei Prüfungsbeginn mit einer persönlichen Identifikationsnummer (PIN) im Prüfungssystem anmeldet und am Prüfungsende eine entsprechende Transaktionsnummer (TAN) zum Absenden der Prüfung eingibt. Ein eindeutiger Nachweis der Authentizität der Prüfungsleistung ist auf diese Weise jedoch unmöglich, da die Prüfungsleistung auch von einer anderen Person erbracht werden könnte. Täuschungsversuche können somit nicht nachgewiesen werden (Forgó et al., 2016, S. 33).

3.2. Einsatz von Dongles

Auch das Verwenden eines individuellen Dongles, z. B. eines USB-Sticks, kann die Identität eines Prüfungsteilnehmers nicht eindeutig nachweisen (Forgó et al., 2016, S. 33).

3.3. Unterschriebene Ausdrucke

Unterschriebene Ausdrucke können nur in Kombination mit Ausweiskontrollen die eindeutige Identität eines Geprüften nachweisen. Diese Kontrolle entfällt jedoch bei Prüfungen ohne Aufsicht (Forgó et al., 2016, S. 33).

3.4. Kombination der genannten Nachweise mit einem elektronischen Fingerprint

Auch durch eine Kombination der vorstehend genannten Nachweise mit einem elektronischen Fingerprint kann nicht eindeutig gezeigt werden, dass die Person, die den Fingerprint durchführt, identisch mit der Person der Prüfungsleistung ist (Forgó et al., 2016, S. 33f.).

4. Weiterführende Hinweise

1. **Durchführung von E-Assessments an der Universität Bremen**
   Informationen zur Sicherung von Authentizität und Integrität bei elektronischen Prüfungen an der Universität Bremen sind abrufbar unter:
   http://www.eassessment.uni-bremen.de/recht.php#id, zuletzt abgerufen am 04.10.2017.

2. **Bericht zur datenschutzkonformen Nutzung von E-Learning-Verfahren an der Universität Kassel**
   Im Rahmen der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Forschungszentrum für Informationstechnikgestaltung (ITeG) der Universität Kassel wurde 2009 ein Abschlussbericht zur datenschutzkonformen Nutzung von E-Learning-Verfahren an hessischen Universitäten veröffentlicht. Abrufbar unter:
   https://www.uni-kassel.de/einrichtungen/fileadmin/datas/einrichtungen/scl/LLukas/Abschlussbericht_Datenschutz_im_E-Learning.pdf, zuletzt abgerufen am 04.10.2017.

3. **Sicherheit bei E-Examinations an der Freien Universität Berlin**
   Informationen zum Sicherheitskonzept der FU Berlin sind abrufbar unter:
   http://www.e-examinations.fu-berlin.de/e-examinations/sicherheit/index.html, zuletzt abgerufen am 04.10.2017.

5. Endnoten

Forgó, Nikolaus, Graupe, Simon, & Pfeiffenbring, Julia (2016). *Rechtliche Aspekte von E-Assessments an Hochschulen. Gutachten im Auftrag des Verbundprojektes E-Assessment NRW.* Abgerufen von der Universität Duisburg-Essen: http://duepublico.uni-duisburg-essen.de/servlets/DocumentServlet?id=42871, zuletzt am 20.06.2017.

Roßnagel, A., & Schnabel, Chr. (2009) *Datenschutzkonforme Nutzung von E-Learning-Verfahren an hessischen Hochschulen.* Abschlussbericht der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Forschungszentrum für Informationstechnikgestaltung (ITeG) der Universität Kassel.

Zivilprozessordnung in der Fassung der Bekanntmachung vom 5. Dezember 2005 (BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781), die zuletzt durch Artikel 12 des Gesetzes vom 5. Juli 2017 (BGBl. I S. 2208) geändert worden ist. Abgerufen von: www.gesetze-im-internet.de/zpo, zuletzt am 16.08.2017.