

Christin Deinert/Daniel Hannuschke
HS Magdeburg-Stendal/HS Merseburg



Handreichung zur Archivierung von ePrüfungen

Handreichung zur Archivierung von ePrüfungen

Diese Handreichung versteht sich als Anregung, einen Prozess zur Archivierung von elektronischen Prüfungen (ePrüfungen) im Land Sachsen-Anhalt (LSA) transparent und nachvollziehbar zu gestalten. Sie soll Interessierten einen Impuls geben, um eine strukturierte, nachvollziehbare und rechtskonforme Ablage der digitalen Prüfungsunterlagen sicherzustellen.

Die ordnungsgemäße Archivierung von ePrüfungen ist aus mehreren Gründen unerlässlich. Zum einen verlangen gesetzliche Vorgaben und Prüfungsordnungen eine sichere und dauerhafte Aufbewahrung von Prüfungsdokumenten, um die Nachvollziehbarkeit und Überprüfbarkeit der Prüfungsleistungen zu gewährleisten. Zum anderen müssen datenschutzrechtliche Anforderungen, insbesondere im Hinblick auf den Schutz personenbezogener Daten der Prüfenden und der Prüflinge, strikt eingehalten werden. Darüber hinaus trägt eine einheitliche Archivierung zur Qualitätssicherung im Prüfungsprozess bei und unterstützt eine effiziente Verwaltung der Prüfungsunterlagen.

Durch die Beachtung dieser Anforderungen wird sichergestellt, dass die Integrität und Verfügbarkeit der digitalen Prüfungsunterlagen auch langfristig gewährleistet ist und damit rechtliche sowie organisatorische Standards erfüllt werden.

1 Anforderungen an die Archivierung von ePrüfungen

Im Zuge der zunehmenden Digitalisierung von Prüfungsprozessen gewinnen Fragen der rechtssicheren und datenschutzkonformen Archivierung von elektronischen Prüfungen an Bedeutung. Die nachfolgenden Ausführungen skizzieren die wesentlichen Anforderungen an die Archivierung von ePrüfungen an Hochschulen im Land Sachsen-Anhalt und sollen eine praxisorientierte Orientierungshilfe für die Umsetzung bieten.

1.1 Rechtliche Rahmenbedingungen

Die Archivierung von ePrüfungen muss im Einklang mit geltenden rechtlichen Vorgaben erfolgen. Hierzu zählen insbesondere:

- **Datenschutzrechtliche Vorgaben:** Die Verarbeitung und Speicherung personenbezogener Daten im Rahmen von ePrüfungen unterliegt der Datenschutz-Grundverordnung (DSGVO) sowie dem Landesdatenschutzgesetz Sachsen-Anhalt. Es ist sicherzustellen, dass nur die zur Zweckerfüllung notwendigen Daten erhoben, verarbeitet und gespeichert werden.
- **Aufbewahrungsfristen:** Prüfungsunterlagen sind entsprechend der hochschulrechtlichen Vorgaben und der einschlägigen Prüfungsordnungen für eine bestimmte Dauer aufzubewahren. In der Regel beträgt die Aufbewahrungsfrist mindestens fünf Jahre nach Abschluss des Prüfungsverfahrens, kann jedoch je nach Hochschule, Studiengang und Prüfungsordnung variieren.
- **Rechts- und Verfahrenssicherheit:** Die Archivierung muss so erfolgen, dass Unterlagen im Bedarfsfall (z. B. bei Widerspruchsverfahren) inhaltlich und technisch unverändert sowie nachvollziehbar zur Verfügung stehen.

1.2 Archivierungskriterien

Für die rechtssichere Dokumentation des Prüfungsverlaufs sind bestimmte Inhalte zwingend zu archivieren. Dazu zählen unter anderem:

- **Prüfungsdaten:** Inhalte und Aufgabenstellungen der ePrüfung.
- **Ergebnisse:** Die erreichten Leistungen der Prüflinge, ggf. mit Bewertungsvermerken.

- Prüfungsprotokolle: Dokumentation von Ablauf und etwaigen Besonderheiten der Prüfung (z. B. bei mündlichen ePrüfungen oder bei technischen Störungen).
- Log-Files: Protokolle technischer Abläufe während der Prüfung (z. B. Login-Zeiten, Unterbrechungen, Abgabezeitpunkte).
- Die Archivierung kann kursbezogen (z. B. für alle Teilnehmenden eines Moduls) oder personenbezogen (pro Studierende*n) erfolgen, muss jedoch die Nachvollziehbarkeit und Zuordnung der Prüfungsergebnisse gewährleisten.

1.3 Zugriffsrechte

Der Zugang zu archivierten ePrüfungsdaten ist auf einen eng begrenzten Personenkreis zu beschränken. Um den Datenschutz und Vertraulichkeit zu gewährleisten, sind differenzierte Zugriffsregelungen notwendig. Mögliche berechnigte Nutzergruppen sind:

- Mitglieder der Prüfungsausschüsse
- Prüfungsämter: Für die administrative Verwaltung und die rechtliche Absicherung von Prüfungsprozessen.
- Lehrende des betreffenden Moduls: Für die Durchführung, Nachbereitung und ggf. Nachkorrektur von Prüfungen.
- Weitere berechnigte Personen (z. B. IT-Administrator*innen, Datenschutzbeauftragte) gemäß Software-Verfahrensverzeichnis.

2 Möglichkeiten zur Archivierung von ePrüfungen

Dieses Kapitel beschreibt beispielhaft verschiedene Möglichkeiten, um elektronische Prüfungen zu archivieren.

2.1 Archivierung auf einem (externen) Speichermedium

Zur Sicherung und dauerhaften Aufbewahrung von ePrüfungen bietet sich die Archivierung auf externen Speichermedien als praktikable Option an. Moderne Lernmanagementsysteme (LMS) verfügen in der Regel über integrierte Exportfunktionen, die eine Ausgabe von Prüfungsdaten in standardisierte Dateiformate, etwa PDF oder XML, ermöglichen. Insbesondere der Export in PDF-Dokumente, die anschließend digital signiert werden, bietet eine rechtssichere Grundlage für die Archivierung, da Inhalte so gegen nachträgliche Veränderungen geschützt sind.

Eine zusätzliche Möglichkeit zur manipulationssicheren Speicherung stellt das WORM-Prinzip (Write Once – Read Many) dar. Hierbei handelt es sich um ein Verfahren, bei dem Daten einmalig geschrieben und anschließend nur noch gelesen werden können. Dies gewährleistet eine unveränderbare Ablage abgeschlossener Prüfungen und ist ein entscheidender Aspekt im Hinblick auf rechtliche Anforderungen und Nachweispflichten. WORM-Archivierung kann sowohl hardwarebasiert (z. B. auf speziellen optischen Datenträgern oder Speicherarrays) als auch softwaregestützt (z. B. über zertifizierte Archivierungssoftware) umgesetzt werden. Die Auswahl des Speichermediums sollte unter Berücksichtigung von Zugriffssicherheit, Langzeitverfügbarkeit und datenschutzrechtlicher Konformität erfolgen.

2.2 Archivierung in einer elektronischen Studierendenakte

Ein weiterer sinnvoller Weg zur strukturierten Ablage von ePrüfungen ist die Integration in eine elektronische Studierendenakte (bspw. in der Software HISinONE). Diese Akte fungiert als zentrales Repository für alle prüfungsrelevanten und personenbezogenen Dokumente einer*s Studierenden. Die Überführung der Prüfungsergebnisse und -unterlagen aus dem Lernmanagementsystem in die Studierendenakte kann manuell oder, falls verfügbar, automatisiert über API-Schnittstellen erfolgen.

Dabei ist es wichtig, dass die exportierten Dokumente eindeutig einer Person sowie einer konkreten Prüfung zugeordnet werden können. Eine saubere Dokumentation und Metadatenstruktur (z. B. Angabe von Prüfungsdatum, Modultitel, Verantwortlichen) erleichtert die spätere Nachvollziehbarkeit. In Systemlandschaften mit vorhandener Campusmanagement- oder

Archivierungssoftware sollte geprüft werden, inwiefern eine systemübergreifende Integration möglich ist. Auch hier ist auf die Einhaltung von Datenschutzvorgaben und Zugriffsregelungen zu achten, insbesondere im Hinblick auf die personenbezogenen Inhalte der Studierendenakte.

2.3 Archivierung in einem Dokumentenmanagementsystem (DMS)

Ein Dokumentenmanagementsystem (DMS) bietet eine strukturierte und revisionssichere Möglichkeit zur Archivierung von ePrüfungen. Durch zentrale Ablage, Suchfunktionen und automatisierte Prozesse kann die langfristige Verwaltung digitaler Prüfungsdokumente effizient gestaltet werden. Die Integration von ePrüfungen in ein DMS setzt eine klare Definition des Archivierungsprozesses voraus.

1. Archivierungsprozess

- **Erhebung der Prüfungsdaten:** Die Erfassung der ePrüfungen kann entweder automatisiert über Schnittstellen (z. B. API-Anbindungen an das Lernmanagementsystem oder eine Prüfungsplattform) oder manuell durch den Upload exportierter Prüfungsunterlagen erfolgen. Dabei ist darauf zu achten, dass die zu archivierenden Daten in einem kompatiblen und standardisierten Format (z. B. PDF/A, XML, CSV) vorliegen, um die Langzeitlesbarkeit und Integrität der Informationen sicherzustellen.
- **Metadaten:** Für eine strukturierte Ablage und spätere Auffindbarkeit der Prüfungsdokumente sind geeignete Metadaten erforderlich. Dazu zählen unter anderem:
 - o Name und Matrikelnummer der*s Studierenden
 - o Prüfungsdatum
 - o Modul- oder Veranstaltungstitel
 - o Name der prüfenden Lehrperson
 - o Prüfungsart (z. B. Klausur, mündliche Prüfung)
 - o Note oder Status der Prüfung (bestanden/nicht bestanden)
- **Archivierung im DMS:** Die Speicherung kann personenbezogen (pro Studierende*n) oder kursbezogen (pro Lehrveranstaltung) erfolgen, je nach Struktur und Anforderungen der Hochschule. Wichtig ist, dass die gewählte Archivierungsstruktur eine eindeutige Zuordnung und Nachvollziehbarkeit der Prüfungsunterlagen ermöglicht.
- **Zugriffssteuerung und Berechtigungen:** Zugriffsrechte im DMS sollten rollenbasiert vergeben und technisch abgesichert sein. Berechtigte Nutzergruppen sind z. B. Prüfungsämter, Prüfungsausschüsse und ggf. die prüfenden Lehrpersonen. Es ist sicherzustellen, dass personenbezogene Daten nur von autorisierten Personen eingesehen werden können – idealerweise durch Nutzung hochschulinterner Authentifizierungsdienste und Berechtigungskonzepte.
- **Aufbewahrungsfristen und Datenvernichtung:** Die Archivierung im DMS muss den gesetzlich und hochschulrechtlich vorgeschriebenen Aufbewahrungsfristen entsprechen (in der Regel mindestens fünf Jahre, ggf. abweichend laut Prüfungsordnung) entsprechen. Nach Ablauf dieser Fristen sind die Daten rechtssicher und datenschutzkonform zu löschen. Dies kann durch automatisierte Löschroutinen oder durch manuelle Löschprozesse geschehen. Eine optionale Überführung in ein Langzeitarchiv (z. B. zentrales Hochschularchiv) ist ebenfalls möglich und sollte frühzeitig mit den zuständigen Stellen abgestimmt werden.

2. Support-Struktur

Ein effektiver und sicherer Einsatz eines DMS zur Archivierung von ePrüfungen setzt voraus, dass alle Beteiligten entsprechend geschult sind und bei Bedarf auf technische sowie organisatorische Unterstützung zurückgreifen können.

3. Beispielhafter Ablauf der Archivierung in einem DMS

Um die Archivierung von ePrüfungen nachvollziehbar und praxisnah darzustellen, wird im Folgenden ein typischer Ablauf skizziert. Dieser orientiert sich an den wesentlichen Schritten von der Prüfung bis zur langfristigen Datenhaltung im DMS:

1. Durchführung der ePrüfung
Der*die Studierende nimmt an der digitalen Prüfung über eine Prüfungsplattform oder ein Lernmanagementsystem teil. Während der Prüfung werden alle prüfungsrelevanten Daten automatisch erfasst.

2. Erfassung und Verschlüsselung der Daten
Die im Rahmen der ePrüfung generierten Daten (z. B. Prüfungsantworten, Protokolle, Log-Files) werden aus dem Prüfungs- oder Lernsystem exportiert und in das DMS überführt. Idealerweise erfolgt die Übertragung verschlüsselt, um die Vertraulichkeit der Daten zu gewährleisten.
3. Anreicherung mit Metadaten
Zur späteren Identifikation und strukturierten Ablage werden die Prüfungsdaten mit relevanten Metadaten ergänzt. Dazu gehören beispielsweise der Name des*r Studierenden, das Prüfungsdatum, die prüfende Lehrperson sowie Angaben zur Prüfungsart und zum Modul.
4. Strukturierte Archivierung
Die angereicherten Daten werden in einem geordneten Archivierungssystem abgelegt, etwa in einem nach Studiengängen, Prüfungszeiträumen oder Studierenden strukturierten Ordner- bzw. Ablagesystem innerhalb des DMS. Dabei ist auf eine klare und einheitliche Ablagestruktur zu achten, um den Zugriff sowie die langfristige Verwaltung zu erleichtern.
5. Definition von Zugriffsrechten
Der Zugriff auf die archivierten Daten wird rollenspezifisch gesteuert. Nur autorisierte Personen, wie bspw. Prüfungsämter, Prüfungsausschüsse oder die jeweilige prüfende Lehrperson, erhalten Leserechte auf die betreffenden Dokumente. Die technische Umsetzung erfolgt über das Berechtigungssystem des DMS.
6. Regelmäßige Datensicherung und Fristenkontrolle
Die archivierten Daten werden in regelmäßigen Abständen durch automatische Sicherungsroutinen geschützt. Zusätzlich erfolgt mindestens einmal jährlich eine Überprüfung der Einhaltung gesetzlicher Aufbewahrungsfristen. Nach Ablauf der Fristen werden die Daten gemäß den geltenden datenschutzrechtlichen Vorgaben rechtssicher gelöscht oder in ein zentrales Langzeitarchiv überführt, sofern dies vorgesehen ist.