

Tipps für den Datenschutz in der Lehre

Grundsätzlich müssen Sie in Ihrem Verantwortungsbereich die geltenden Datenschutzregelungen einhalten. Im Wesentlichen ist zu beachten, dass das Erheben, Speichern, Übermitteln und Löschen von Daten nur mit schriftlicher Einwilligung der Betroffenen zulässig ist oder sich auf eine Rechtsgrundlage stützen muss. Da im Lehralltag eine schriftliche Einwilligung in der Regel nicht vorliegt, muss sichergestellt sein, dass eine entsprechende Rechtsgrundlage vorliegt (dies kann z. B. das Hochschulgesetz sein).

Virtuelle Lernumgebungen

Bei der Durchführung von Lehrveranstaltungen mit Hilfe von Lernmanagementsystemen (LMS) - als vollständiger Online-Kurs oder als Blended Learning -Veranstaltung - sollten Sie sich die Mühe machen, die einzelnen Rollen und die damit verbundenen Rechte, z. B. Lese- und Schreibzugriffe oder das Erstellen und Löschen von Objekten wie Dokumenten und Ordnern, differenziert zu vergeben. Je nach Kursart und Teilnehmerstruktur kann eine eher hierarchische oder eine eher offene Rechtevergabe praktiziert werden – beide haben Vor- und Nachteile. Die hierarchische Rechtevergabe – viele Rechte für die Kursleitung, wenig Rechte für die Teilnehmer – kann vor unbefugtem Kopieren, Manipulieren oder Löschen der in das LMS eingestellten Daten und Dokumente schützen. Allerdings erfordert diese Vorgehensweise einen gewissen Zusatzaufwand bei der Planung der Lehrveranstaltung: Es muss überlegt werden, wer welche Rechte zur Bearbeitung der gestellten Aufgaben benötigt und diese müssen innerhalb der Lernumgebung definiert werden. Zudem kann dadurch die Möglichkeit zur spontanen Bildung von Arbeitszusammenhängen eingeschränkt sein. Bei der offenen Rechtevergabe entfällt ein Teil der administrativen Betreuung des Kurses: Allen Beteiligten werden die gleichen umfassenden Rechte eingeräumt. Dadurch können sich spontane, wechselnde Arbeitszusammenhänge u. U. besser entwickeln. Allerdings besteht hier die Gefahr, dass – absichtlich oder unabsichtlich – Dokumente oder Einstellungen manipuliert und so schlimmstenfalls Arbeitsergebnisse vernichtet werden.

Online-Prüfungen

Bei der Durchführung von Online-Prüfungen sollten alle Nutzer- und Testdaten, Antworten und Auswertungen in anonymisierter Form gespeichert werden. Die Übertragung aller Daten sollte über eine verschlüsselte Verbindung, z. B. SSL, erfolgen, um Manipulationen an den Daten während der Übertragung zu verhindern. Entsprechende Funktionen werden von vielen Prüfungsgeneratoren bereitgestellt.

Veröffentlichung von Informationen im Internet

Bei der Veröffentlichung von Informationen im Internet, z. B. auf einer seminarbegleitenden Webseite, sind hinsichtlich des Datenschutzes einige Punkte zu beachten. Handelt es sich um ein frei zugängliches Angebot, dürfen keine Teilnehmer- oder Notenlisten veröffentlicht werden. Auch die Anonymisierung mit Hilfe der Matrikelnummer – üblich beim Aushang solcher Listen in den Räumen der Hochschulen – reicht nicht aus. Möchten Sie personengebundene Daten auf einer Internetseite veröffentlichen, müssen Sie entweder die schriftliche Einwilligung der Betroffenen einholen oder aber den Zugriff auf die Informationen einschränken. Eine Möglichkeit besteht darin, den Zugriff nur über die Registrierung mit einem Passwort zu erlauben. Die Anmeldung sollte dann über eine verschlüsselte Verbindung abgesichert werden. Dabei ist zu beachten, dass der registrierte Nutzer nur Zugriff auf seine persönlichen Daten erhält und nicht etwa die Gesamtlisten angezeigt bekommt. Wenden Sie sich an das Rechen-

oder Medienzentrum Ihrer Hochschule, um einen solchen Zugang einzurichten.

Auch bei der Nutzung von Kommunikationswerkzeugen wie z. B. Weblogs oder Foren ist darauf zu achten, dass keine Informationen veröffentlicht werden, die im Hinblick auf den Datenschutz bedenklich sind. Bieten Sie im Rahmen einer Lehrveranstaltung entsprechende Tools an, müssen Sie die dort eingestellten Informationen regelmässig kontrollieren und bei Verstößen gegen Datenschutzregelungen löschen oder anonymisieren.

Präsentationen

Häufig sieht man in Veranstaltungen oder auf Tagungen Präsentationen, in denen personengebundene Daten für alle gut lesbar auf die Leinwand geworfen werden. So kommt es z. B. vor, dass ein Bericht über die Evaluation einer Online-Lehrveranstaltung mit den Namen der Teilnehmer, die von ihnen zu verschiedenen Zeitpunkten erledigten Aufgaben etc. illustriert wird. Womöglich vergisst der Vortragende zusätzlich, nach Abschluss seiner Präsentation die Dateien vom Präsentationsrechner zu löschen und ermöglicht so Unbefugten den Zugriff auf die sensiblen Daten. Eine einfache Möglichkeit, die personengebundenen Daten zu schützen und trotzdem nicht auf Illustrationen verzichten zu müssen, ist das Unkenntlichmachen der entsprechenden Bereiche durch Unschärfefilter, die in vielen Bildbearbeitungsprogrammen integriert sind.

Letzte Änderung: 11.06.2015

Zitation

e-teaching.org (2015). Tipps für den Datenschutz in der Lehre. Zuletzt geändert am 11.06.2015. Leibniz-Institut für Wissensmedien: https://www.e-teaching.org/technik/datenhaltung/datenschutz/tipps_lehre/index_html. Zugriff am 17.02.2019