Ansätze zur Entwicklung datenschutzkonformer E-Learning-Plattformen

Kai-Uwe Loser, Thomas Herrmann

Informations- und Technikmanagement am
Institut für Arbeitswissenschaft
und Datenschutzbeauftragte der
Ruhr-Universität Bochum

{kai-uwe.loser; thomas.herrmann}@rub.de

Abstract: Bei der Entwicklung der aktuell verfügbaren E-Learning-Plattformen hat die Berücksichtigung von Datenschutzanforderungen nur unzureichend stattgefunden. Der vorliegende Beitrag betrachtet das Thema vor dem Hintergrund der rechtlichen Gegebenheiten, aber auch aus Sicht der Ergebnisse der Privacy Diskussion im Gebiet der CSCW. Insgesamt werden dabei Anforderungen an und Lösungsansätze für datenschutzkonforme E-Learning-Plattformen erarbeitet. Vertiefend wird auf die Problematik der Umsetzung der Datenminimierung von Nutzungsprotokollierungen eingegangen für die auf der Basis einer empirischen Untersuchung Lösungen aufgezeigt werden.

1. Einleitung

An nahezu allen Hochschulen werden inzwischen für die Durchführung der Lehre internetbasierte Systeme angeboten, die das E-Learning unterstützen. Typische Beispiele sind Moodle als Open-Source-Plattform, Blackboard als marktführendes kommerzielles Produkt oder EWS als Eigenentwicklung. Weitere prominente Vertreter sind StudIP oder ILIAS. Beim aktuellen Stand der Technik derartiger Lernmanagementsysteme (LMS) fällt auf, dass bei der Anforderungsanalyse, bei der Ausgestaltung und bei der Einführung eine systematische Berücksichtigung von Datenschutzanforderungen nicht stattfindet. Bei den in vielen Bundesländern erforderlichen Vorabkontrollen oder Audits kommt es daher während Einführung oder Überprüfung solcher Systeme regelmäßig zu gravierenden Problemen. Die Hochschulen vermeiden die Vorabkontrollen, weil der Betrieb der Systeme allenfalls mit sehr beschnittenem Funktionsumfang rechtlich zulässig wäre. Die Relevanz des Datenschutzes wurde durch die E-Learning-Community inzwischen erkannt, und einzelne Lösungsbestandteile sind identifiziert worden [HH08]. Insbesondere hat [Ei08] bereits die Frage der Vertraulichkeit im System Moodle vertieft betrachtet.

Vor dem Hintergrund des Datenschutzes ergeben sich verschiedene konfliktäre Konstellationen. Zu berücksichtigen sind insbesondere einerseits die gewünschte Transparenz des Verhaltens der Teilnehmer: zum Beispiel wollen Studierende wissen, ob ihre Kommilitonen bei Teamarbeitskonstellationen schon Beiträge zu einer gemeinsamen Ausar-

beitung eingestellt haben, oder Dozenten möchten nachvollziehen, inwieweit Übungsaufgaben zu einer Vorlesung gelöst wurden, wie schnell Studierende auf die Verteilung der Aufgaben reagieren etc. Andererseits werden für die Realisierung dieser Art von Transparenz so viele personenbeziehbare Ereignisse in einer Detailliertheit (Ereignis, Objekt, Zeitstempel) protokolliert oder Daten undifferenziert zugreifbar gemacht, dass die Erforderlichkeit als wesentlicher Grundsatz datenschutzrechtlicher Konformität nicht mehr nachvollziehbar ist. Die Anforderung, das Ausmaß der Datenerfassung, -speicherung und -zugreifbarkeit in einem Maße zu begrenzen, dass die sinnvolle Kooperation und Interaktion bei Lehr-/Lernprozessen datenschutzkonform erfolgen kann, ist nicht trivial zu realisieren. An dieser Stelle sei auch erwähnt, dass Forschung als Erhebungszweck gerade auch im Sinne explorativer Studien die Erhebung von weit mehr Daten erlauben kann, als die Nutzung in der Breite vieler Lehrveranstaltungen an einer Hochschule. Technische Grundbausteine zur Lösung der Probleme sind zwar im Umfeld von Privacy-Enhancing Technologies, Awareness-Mechanismen und rollenbasierter Zugriffsregelungen vorhanden, sie sind aber in den meisten Lernmanagementsystemen nicht konsequent implementiert. Vielmehr wird mit Hinblick auf die Testphasen der Software eine weitgehende Datentransparenz realisiert, die dann aufgrund fehlender Konfigurationsmöglichkeiten nicht angemessen reduziert werden kann. Gerade die Konfigurierbarkeit der Systeme zum Zweck einer Reduktion personenbezogener Daten stellt eine besondere Herausforderung dar, die vor allem auf der Usability-Ebene (Steuerbarkeit und Nachvollziehbarkeit) zu weiteren beachtenswerten Anforderungen führt.

Die in diesem Beitrag genannten Probleme sind einerseits durch die Analyse von Systemen an den Hochschulen der Ruhr-Allianz (insbesondere Blackboard und Moodle) entstanden und sind durch Diskussion mit anderen Hochschuldatenschützern und Datenschutzkontrollbehörden vertieft worden. Auf der Basis dieser Analyse, die deutliche Schwächen gezeigt hat, wurde eine empirische Untersuchung durchgeführt, um sich durch Befragung von Nutzern der Frage der Erforderlichkeit für die Lehre strukturiert zu nähern. Im folgenden Abschnitt wird vorab zunächst der aktuelle Entwicklungsstand häufig eingesetzter E-Learning-Systeme dargestellt. In Abschnitt 3 wird der Hintergrund der Datenschutzthematik anhand der Privacy-Diskussion im Bereich CSCW und CSCL vertieft. Dem wird im vierten Abschnitt eine systematische Problembeschreibung nach Datenschutzprinzipien entgegengestellt. Dort werden jeweils Ansätze für technische und organisatorische Maßnahmen aufgezeigt, die zu einer Lösung beitragen können. Vertieft wird diesbezüglich unsere Forschung zur Bestimmung der Datenerhebung unter Berücksichtigung der Erforderlichkeit. Der abschließende Ausblick konzentriert sich auf die dringendsten Forschungsfragen.

2. Charakterisierung der E-Learning-Plattformen

Die E-Learning-Plattformen sind größtenteils aus Basissystemen, wie z.B. Dokumentenmanagement- oder Content-Management-Systemen heraus entstanden und anschließend schrittweise um weitere Funktionalität ergänzt worden. Bei der Weiterentwicklung lassen sich die Entwickler der Systeme von offenen Plattformen aus dem Internet inspirieren. Funktionen wie Diskussionsforen, Instant Messaging, Wikis oder Selbstdarstel-

lungen sind aus entsprechenden Plattformen übernommen. Aktuell geht die Tendenz sogar zu einer Einbindung externer Web 2.0 Plattformen, was aus Datenschutzsicht weitere Fragen aufwirft, aber nicht im Rahmen dieses Beitrags vertieft werden kann. Eine Übersicht derzeit gängiger Funktionen ist in Abbildung 1 dargestellt. Bei der Integration der vielfältigen neuen Funktionen, die den Nutzern aus dem Internetalltag bekannt sind, wurde aber meist ein wesentlicher Aspekt für den Datenschutz nicht ausreichend gewürdigt: die häufig im Netz zu unterstellenden symmetrischen Beziehungen zwischen Benutzern sind in Hochschulen zwar ebenfalls zu finden, aber sind auch durch asymmetrische Machtkonstellationen zu ergänzen (s. Abschnitt 3).

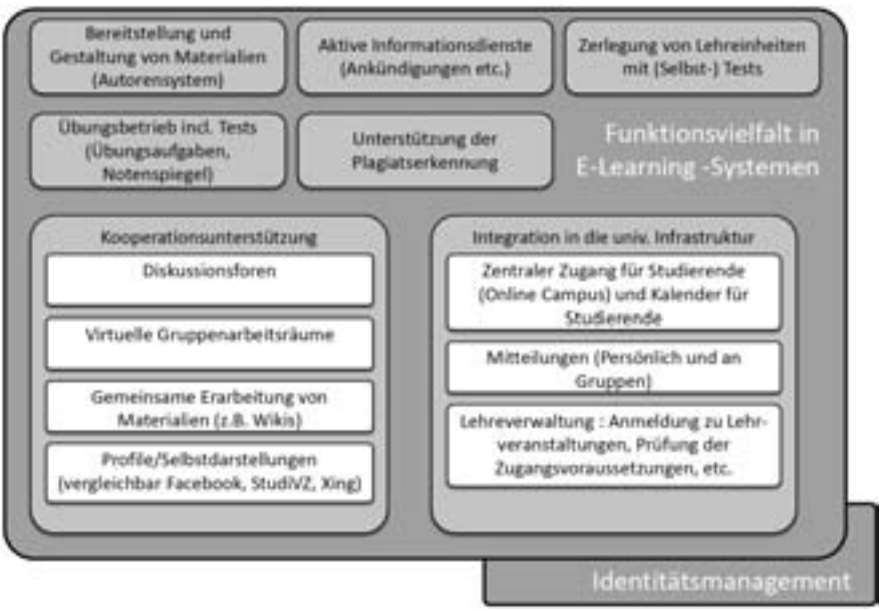

Abbildung 1: Funktionsvielfalt in E-Learning-Plattformen

Wie unsere Auswertung von Lehrveranstaltungen an zwei Hochschulen gezeigt hat, basiert die praktische Nutzung der E-Learning-Plattformen an Präsenzhochschulen derzeit zu mehr als 90% der durchgeführten Veranstaltungen lediglich auf den „Content-Management-Funktionen“: über die Systeme werden einem eingeschränkten Nutzerkreis von Studierenden Informationen und Materialien im Rahmen etwa einer Vorlesung auf einfache und bekannte Weise zur Verfügung gestellt. Nur sehr wenige Lehrende nutzen hingegen weitergehende Funktionen im Rahmen spezialisierter didaktischer Konzepte, wie sie zum Beispiel im Kontext von Computer Supported Collaborative Learning [KHM02] behandelt werden. Meist sind das dann seminarähnliche Situationen, in denen kleinere Gruppen über die Kooperationsmöglichkeiten von E-Learning-Plattformen bei der gemeinsamen Erarbeitung von Inhalten unterstützt werden. Diese Verteilung in der tatsächlichen Nutzung der Systemfunktionalitäten ist in der Konfigurierbarkeit der Systeme derzeit nicht angemessen abgebildet. In der Regel folgt daraus, dass wesentlich mehr und detailliertere Daten erhoben und verarbeitet werden, als für die besonders häufigen Einsatzszenarien tatsächlich erforderlich ist. Was gängige Einsatzszenarien

derzeit sind und wie der dazu erforderliche Datenumfang aussieht, wird in Abschnitt 5 vertieft.

In den Systemen werden für diese Funktionen unterschiedliche Datenarten verarbeitet. So lässt sich etwa zwischen inhaltlichen Daten (Inhalt einer Klausur, eines Übungsblattes), Protokolldaten der Nutzung oder Konfigurationen, die ein Teilnehmer vorgenommen hat, trennen. Dazu kommen Daten, die direkt eine Person beschreiben (Name, Adresse, Studienverlauf etc.), die teilweise aus anderen Systemen an Hochschulen übernommen werden. Daten können gespeichert sein oder nur transient im System auftreten. Die Protokolldaten werden durch die Awarenessmechanismen (s.u) aggregiert, indem etwa mehrere Events entlang der Zeitachse zu einer Aussage zusammengefasst werden (mehrmaliges Öffnen einer Datei zur Aussage „hat die Datei geöffnet“) oder das Verhalten mehrerer Personen aggregiert wird (Übungsgruppe X hat mit der Bearbeitung von Y begonnen). Letzteres trägt zumindest teilweise zu einer Anonymisierung bei.

3. Privacy in CSCW-Systemen

Mit Hinblick auf die internationale Forschung liegt die in Lernmanagement-Systemen (LMS) vorhandene Funktionalität dem Gebiet des Computer Supported Cooperative Work (CSCW) nahe und wenn breite Kooperation unterstützt wird, wird das Thema im Bereich Computer Supported Collaborative Learning (CSCL) vertieft. Während in den 90er Jahren eine intensive Diskussion zu Privacy-Anforderungen im Bereich CSCW geführt wurde (als initialen Beitrag kann man hier [Cl93] werten), wurde dem Thema in der CSCL-Diskussion bislang nur geringe Beachtung geschenkt. In den letzten Jahren hat sich die Privacy-Diskussion stärker auf den Bereich der Web-Applikationen verlagert (s. z.B. [RBE03], [WGT08]).

Die CSCW-orientierte Privacy-Diskussion wurde insbesondere in Verbindung mit sogenannter Awareness-Funktionalität relevant. Dabei soll die Awareness [DB92], [JSP02] über die Aktivitäten der anderen, mit denen man kooperiert und deren Verhalten für die eigenen Arbeitsschritte relevant ist, technisch unterstützt werden. Typische Beispiele sind Benachrichtigungsfunktionen (Notification), die mitteilen, ob neue Inhalte eingestellt wurden, ob an einem Dokument etwas geändert wurde etc. Awareness-Funktionalität liefert auch für LMS wesentliche Beiträge: Dozenten wollen die Aktivitäten der Studierenden nachvollziehen, also ob zum Beispiel Lernmaterialen abgerufen wurden, ob Übungsaufgaben bearbeitet werden, ob Zusammenarbeit stattfindet; Studierende wollen erkennen, ob neue Lehrmaterialien zur Verfügung stehen, ob Kommilitonen Nachrichten in dem System hinterlegt haben, wann von anderen Dinge bearbeitet wurden, wann Übungsaufgaben zugreifbar sind etc. Awareness-Funktionalität muss dazu Ereignisse protokollieren, sie für die Awareness-Zwecke in eine geeignete Darstellung bringen und sie an die relevanten Adressaten verteilen bzw. abrufbar halten.

Es ist offensichtlich, dass damit die Speicherung und Verarbeitung personenbezogener Daten einhergeht. Diesbezüglich haben [BS93] drei Privacy-Prinzipien formuliert: Control, Feedback und Equality. Im Vergleich zu dem in Europa etablierten Prinzip der

informationellen Selbstbestimmung kann „Control“ mit dem Recht zu bestimmen, wer was über einen weiß, verglichen werden, das sich gesetzlich in dem Grundsatz der „Verbotsvermutung mit Erlaubnisvorbehalt“ und in den „Betroffenenrechten“ niederschlägt (s. Abschnitt 4). „Feedback“ bedeutet, dass für den Fall, dass personenbezogene Daten verarbeitet werden, dass man wissen können muss, wer was über einen weiß, wie es z.B. in dem „Transparenzprinzip“ deutlich wird. „Equality“ nimmt eine Sonderrolle ein, die so nicht im Datenschutzrecht repräsentiert ist: Andere sollen die gleiche Art von Daten über mich mit Hilfe eines elektronischen Mediums zur Kenntnis nehmen können, wie ich über sie mittels des gleichen Mediums erfahren kann. Wer also in einer Audio-Video Verbindung kein Bild von sich selbst anbietet, könnte demgemäß auch das Bild des anderen nicht sehen; wer bei seinen empfangenen E-Mails eine Empfangsbestätigung unterdrückt, könnte auch keine Empfangsbestätigung von anderen erhalten. Die Realisierung von Control, Feedback und Equality hängt im Einzelnen sowohl von den jeweiligen Funktionen ab (siehe Abschnitt 2) als auch von der Art der personenbezogenen Daten, die verarbeitet werden.

Die CSCW-orientierte Privacy-Diskussion unterstellt, dass zwischen den Nutzern symmetrische Beziehungen in dem Sinne bestehen, dass kein Machtungleichgewicht zwischen ihnen herrscht, das dem Einen Sanktionsgewalt gegenüber dem Anderen einräumt. Das Kriterium „Equality“ geht typischerweise von solchen Konstellationen aus. Symmetrische Verhältnisse spiegeln sich in den Rollen wieder, wie sie zwischen Studierenden wahrgenommen werden können. Demgegenüber gibt es jedoch in E-Learning-Plattformen hinsichtlich der Nutzung personenbezogener Daten auch asymmetrische Konstellationen, bei denen die eine Seite die andere sanktionieren kann: Student vs. Dozent; Student vs. Tutor, Student vs. Hochschulverwaltung; Student als Bürger vs. Staat (z.B. Ausländerbehörde, die die Aufenthaltsgenehmigung vom Studienfortschritt abhängig macht). Da sich in asymmetrischen Sozialbeziehungen Datenschutzprobleme in stärkerem Maße zu Ungunsten der Betroffenen auswirken, wird im Folgenden auf Rechtsprinzipien eingegangen, die sich für diesen Kontext entwickelt haben.

Der Erfolg von E-Learning-Systemen basiert zu einem großen Teil auf der persönlichen Motivation zur Nutzung der Systeme, die wiederum auch von dem Vertrauen zwischen allen Beteiligten abhängt. Die Verstärkung der asymmetrischen Verhältnisse durch übermäßige Kontrollmöglichkeiten in den E-Learning-Plattformen ist diesbezüglich eher schädlich. Vielmehr sollte man verstärkt darüber nachdenken in den symmetrischen Verhältnissen zwischen den Studierenden untereinander durchaus Einsichtnahme zu ermöglichen (bspw. Zeitstempel von Beiträgen), Lehrende hingegen haben wiederum eingeschränkten Zugriff auf Daten und erhalten stattdessen anonymisierte Zusammenstellungen oder zusammengefasste Daten. Dabei sind aber in jedem Fall grundlegende Datenschutzerfordernisse schon zum Zeitpunkt der Erhebung zu beachten.

4. Beachtung von Datenschutzprinzipien

Aus der rechtlichen Perspektive im europäischen Raum haben sich über die letzten Jahrzehnte sieben Prinzipien entwickelt, die bei verschiedenen Gesetzen und rechtlichen Rahmenbedingungen übergreifend zu beachten sind (vgl. [Bi07]):

1.) Verbotsvermutung mit Erlaubnisvorbehalt (Rechtmäßigkeit)
2.) Zweckbindung
3.) Betroffenenrechte
4.) Löschung
5.) Sicherheit und Kontrolle
6.) Transparenz
7.) Datenvermeidung und Erforderlichkeitsgrundsatz

Gemäß diesen Regelungen ergeben sich verschiedene Probleme, die Anlässe und Ansätze zur Verbesserung der E-Learning-Systeme aus der Datenschutzperspektive ergeben.

Rechtmäßigkeit, Zweckbindung und Betroffenenrechte

Mit **Rechtmäßigkeit** (auch „Verbotsvermutung mit Erlaubnisvorbehalt“) ist gemeint, dass jede Einschränkung des Rechts auf informationelle Selbstbestimmung eine gesetzliche Grundlage benötigt. Die Verarbeitung personenbezogener Daten ist also grundsätzlich verboten, wenn sie nicht explizit erlaubt ist. Die verschiedenen in Frage kommenden Rechtsgrundlagen können an dieser Stelle nicht vertieft dargestellt werden und sind eher unabhängig von der Technik zu schaffen. Rechtsgrundlagen legen die Zwecke der Erhebung und Verarbeitung fest. Eine mögliche Rechtsgrundlage könnte die Einwilligung (Freiwillige Nutzung) sein. Eine echte Freiwilligkeit wird im Verhältnis Lehrender zu Student allerdings nicht zu unterstellen sein, da der Student Sanktionen befürchten muss (s. Abschnitt 3). Andere Rechtsgrundlagen (v.a. Lehr- und Prüfungsordnungen) sind hier erforderlich.

Das **Zweckbindungsprinzip** beschreibt, dass Daten grundsätzlich nicht zu anderen als den Zwecken verwendet werden dürfen, zu denen sie ursprünglich erhoben wurden, es sei denn, es liegen gesetzlich bestimmte Ausnahmesituationen vor, die in der Regel eine Abwägung der Interessen der Betroffenen berücksichtigen. In der Praxis der Lernmanagementsysteme werden die Zwecke häufig unhinterfragt erweitert. Was ursprünglich nur Lehrezwecke beinhaltete, wurde durch die Nutzung für Prüfungszwecke ergänzt, weitere Zweckerweiterungen umfassen die Nutzung der Daten für die Evaluation und natürlich werden weiterhin auch Forschungszwecke verfolgt. Alle diese möglichen Zwecke müssen vor Beginn der Datenerhebung festgelegt und für alle Beteiligten transparent sein.

Betroffenen werden generell bestimmte **Rechte** eingeräumt, die in den Systemen umsetzbar sein müssen. Umzusetzen sind in der Regel Auskunft, Berichtigung, Sperrung und Löschung. Auch die Umsetzbarkeit dieser Rechte ist in den Systemen durchaus problematisch. Insbesondere die Löschung kann bei einer Nutzung auf freiwilliger Basis aufgrund inhaltlicher Erwägungen schwer zu realisieren sein. Beispielsweise müssten Beiträge in Diskussionsforen bei Widerruf der Einwilligung gelöscht oder anonymisiert werden, was zumindest mit hohem Aufwand verbunden ist und Informationen unbrauchbar machen kann. Das wird grundsätzlich vereinfacht je mehr Funktionen auch anonym genutzt werden können.

Löschung

Die Umsetzung der generellen Löschungsverpflichtung ist ein weiteres nicht ausreichend berücksichtigtes Thema. Selten sind in den Systemen bereits Überlegungen und Lösungen für angemessene Löschkonzepte zu finden. Meist existiert nur die Möglichkeit, selektiv einzelne Beiträge oder aber einen Kurs als Ganzes zu löschen, was häufig dazu führt, dass Daten unnötigerweise lang aufgehoben werden müssen. Verständlicherweise nutzen Lehrende eine vorangegangene Veranstaltung als Basis zur Konfiguration einer inhaltsgleichen Folgeveranstaltung. Beispielsweise wären das Anonymisieren von Diskussionsbeiträgen oder das automatische Löschen von Inhaltsbereichen, die nicht wiederverwendet werden sollen, Funktionen, mit denen die datenschutzrechtlichen Löschanforderungen besser erfüllt werden könnten. Auch sind zeitgesteuerte Automatismen erforderlich.

Sicherungsmaßnahmen

Die erhobenen Daten sind in jedem Fall ausreichend durch **technische und organisatorische Maßnahmen** abzusichern. Bei den Sicherungsmaßnahmen werden häufig zunächst die Systemintegrität und technische Missbrauchsmöglichkeiten betrachtet [Ec03]. Die besonderen Anforderungen an den Schutz der personenbezogenen Daten innerhalb der Systeme werden dabei schnell übersehen. Insbesondere die Durchsetzung von ausschließlich erforderlichen Kenntnisnahmen von personenbezogenen Daten ist hier zu nennen (Vertraulichkeit als Sicherungsziel). Jeder Nutzer sollte nur die Daten einsehen können, die für seine Aufgabe erforderlich sind. Für Moodle wurden Anforderungen an die Vertraulichkeit bereits weitgehend in [Ei08] betrachtet.

Identitätsmanagement: Mit der wachsenden Verbreitung von Identity-Management-Systemen an Hochschulen sind bereits LMS verbessert worden. Das ist zwar größtenteils eher mit dem Ziel der Optimierung von Arbeitsabläufen geschehen, jedoch trägt das auch dem Aspekt Rechnung, dass im Gegensatz zu öffentlichen Plattformen im E-Learning an Hochschulen direkte unvermittelte Beziehungen vorhanden sind: Lehrende kennen ihre Studierenden und müssen diese auch kennen, um später Leistungsbewertungen abgeben zu können. Verfahren des Identity-Managements werden aber hinsichtlich des Datenschutzes nicht in vollem Umfang ausgeschöpft. Wenn, wie bei der einfachen Verteilung der Vorlesungsunterlagen, die eindeutige Identifizierung einer Person im Nutzungsprozess nicht erforderlich ist, ist es beispielsweise auch möglich mit anonymen Berechtigungen zu arbeiten ([Ch85]; [We05]). Dabei wird die Berechtigung selbst durch das Identity-Management-System geprüft und vergeben, für das E-Learning selbst ist die Person aber nicht erkennbar. Die Nutzung selbst ist dann nicht mehr personenbeziehbar. In diesem Bereich sind bereits Umsetzungslösungen diskutiert worden [Fr06].

Berechtigungskonzepte: In den E-Learning-Plattformen sind Berechtigungen zur Nutzung von Funktionalität und zur Einsicht von Daten bereits häufig flexibel einstellbar. Diesbezüglich liegen die Defizite eher in der Praxis der Lehrenden. Professoren erachten es häufig als selbstverständlich, dass ihre vermeintlich weitreichende Verantwortlichkeit mit weitgehenden Berechtigungen einhergehen muss, obwohl sie tatsächlich selbst selten im System aktiv sind. Stattdessen stellen oftmals studentische Hilfskräfte Dateien ein

oder erfassen Ergebnisse von Übungen. Hilfskräfte sollen als tatsächliche Akteure andererseits hingegen möglichst unerkannt bleiben, dürfen aber in der Regel alle Daten einsehen. Obwohl technisch häufig auch anders möglich, besitzen in der Praxis oft alle Personen oder Rollen, die an der organisatorischen Durchführung beteiligt sind, umfassende Berechtigungen im System. Problematisch ist dann die Konstellation, die sich daraus ergibt, dass studentische Hilfskräfte typischerweise an einem Lehrstuhl in der eigenen Fakultät arbeiten und dann unter den genannten Bedingungen leicht die Möglichkeit haben, die Leistungsdaten von Kommilitonen einzusehen. Hier ist zunächst zu fordern, dass jeweils rollenbezogen ganz spezifische Berechtigungen vergeben werden. Die technischen Möglichkeiten werden in der Praxis zu selten genutzt. Eine Analyse der tatsächlich vergebenen Rollen Mitte 2006 an einer Hochschule hat ergeben, dass von 2194 Veranstaltungen 33% mehr als einen Kursleiter mit vollen Berechtigungen haben, während Veranstaltungen mit Nutzern mit eingeschränkteren Rechten nur in 21% der Veranstaltungen zu finden sind. Dazu kommt, dass zu dem Zeitpunkt die Weitergabe der Passworte leicht war. Es ist davon auszugehen, dass auf nicht erkennbarem Wege noch eine ganze Reihe von Veranstaltungen durch mehr als eine Person mit vollen Berechtigungen verwaltet worden sind.

Hier sind einerseits organisatorische Regelungen zu treffen, die die Umsetzung ermöglichen. Andererseits sind aber auch weitere technische Aspekte zu betrachten. Beispielsweise sind die konkreten Berechtigungen und Beschränkungen, die mit der Vergabe einer Rolle verbunden sind, oft für Nutzer nicht leicht vorhersehbar. Um Problemen auszuweichen, werden dann allzu schnell umfassende Berechtigungen vergeben. Hier fehlen ausreichende Informationen im System, die verständlich klar machen, was ein Nutzer im System ausführen kann und wo Beschränkungen liegen werden. Ein weiterer Ansatz ist es, Rollen miteinander zu verschränken, um spezifischen Problemen Rechnung zu tragen. Studentische Mitarbeiter, die gleichzeitig Studenten in dem Fach sind, in dem die betreute Lehrveranstaltung durchgeführt wird, sind regelmäßig als problematisch anzusehen. Durch eine systemunterstützte spezifische Rollenzuordnung wären hier noch Verbesserungen zu erreichen. Das System kann die genannte Konstellation bemängeln oder auch Detailinformationen wie Prüfungsergebnisse vor dem Zugriff sperren.

Transparenz

Weiterhin gilt es, **Transparenz** bei den Betroffenen zu schaffen. Dies verlangt einerseits eine weitreichende Informierung der Nutzer (Datenschutzerklärung). Im Detail sollten erhobene Daten und Verarbeitungsschritte für Betroffene nachvollziehbar sein. Es besteht derzeit das Problem, dass in den Systemen für Nutzer nicht transparent ist, wer welche Daten einsehen kann oder gar eingesehen hat. Verlässliche Informationen darüber, wer wann welche Daten einsehen konnte oder es auch getan hat, können auch das Verhalten der Lehrenden für den Datenschutz positiv beeinflussen. Die Beobachtbarkeit des Beobachtungsprozesses kann zur zurückhaltenderen Nutzung bestimmter Funktionen beitragen. Es könnte auch ein System-Feature sein, dass solche Rechtfertigungen explizit abgelegt werden, bevor eine Auswertung des Lernendenverhaltens erfolgt.

Erforderlichkeit und Datenminimierung

Der Grundsatz der **Erforderlichkeit** beschreibt, dass die Daten nur in einem minimal erforderlichen Umfang überhaupt erhoben werden dürfen. Aus diesem Grundsatz ergibt sich auch eine Verpflichtung zu datenschutzfreundlichen Lösungen und zur Datenminimierung (§ 3a BDSG und die einschlägigeren und entsprechenden Normen in Landesdatenschutzgesetzen). Weiterhin sind Kenntnisnahmen, Übermittlungen und Datenverarbeitungsschritte nur im absolut erforderlichen Rahmen erlaubt. Auch die Aufbewahrungsdauer von Daten richtet sich nach der Erforderlichkeit der Daten. Die Umsetzung dieses Grundsatzes wird im folgenden Abschnitt vertiefend betrachtet.

5. Erforderlichkeit und Datenminimierung für die Lehre

Zur Prüfung der Erforderlichkeit und daraus motivierten Datenminimierung ist es wesentlich die Nutzung und die Informationsbedarfe zur Aufgabenerfüllung eingehender zu betrachten. Auf der Basis von fünf Interviews mit verschiedenen Nutzergruppen des Hauptsystems an der Hochschule der Autoren wurde diese Frage vertiefend betrachtet. Für die Frage der Minimierung sind besonders die Protokolldaten relevant, die Grundlage für Awareness-Funktionalität ist.

Aufzeichnung von Nutzerverhalten für Awareness

Der Erforderlichkeitsgrundsatz ist gerade für die Protokollierung von Nutzerverhalten zur Realisierung der Awareness-Mechanismen derzeit nur sehr unzureichend berücksichtigt worden. Diese Form der Protokollierung ist von Protokollen in anderen Systemtypen (Betriebssysteme, Datenbankanwendungen) deutlich zu unterscheiden. Dort betrachtet man die Protokollierung eher als ein Anhängsel des Systems. Protokollierung ist oft nicht unbedingt für die Kernfunktionalität erforderlich, sondern es werden konkrete Nebenziele erreicht (z.B. Revisionssicherheit, Fehlererkennung, etc.). Die zur Sicherung und Datenschutzverbesserung solcher Logfiles existierenden Lösungen (z.B. [Me06]) sind beim E-Learning nicht einsetzbar, da Aufzeichnungen von Nutzerverhalten integraler Bestandteil der Awareness-Funktionen sind.

Die Implementierung der Awareness-Funktionen sieht meist eine Aufzeichnung von Nutzerverhalten ohne Betrachtung der möglichen oder gar erforderlichen späteren Nutzung vor. Vielfach werden prinzipiell alle Aktionen aufgezeichnet, damit sie für die spätere Verwendung zur Verfügung stehen. Gängig sind hier weiterhin systemweite Einstellungen. Man kann also in der Systemkonfiguration meist das Logging entweder vollständig abschalten oder vollständig beibehalten. Vollständiges Abschalten würde zwar zu einer rechtlich nicht zu beanstandenden Konstellation führen, allerdings würde man dabei auf viele der sinnvollen Funktionen verzichten, die für komplexere Einsatzszenarien auch erforderlich sein können.

Um zu entscheiden welche Funktionen (und damit welche Daten) erforderlich sind, sind die Einsatzszenarien vertieft zu betrachten. Bei der überwiegenden Zahl der Vorlesungen

und Veranstaltungen würde man mit einem sehr eingeschränkten Funktionsumfang sehr gut auskommen, bei dem dann auch nur im eingeschränkten und erforderlichen Umfang Nutzerverhalten erhoben werden dürfte. Dass ein bestimmter Student einer großen Vorlesung den Foliensatz der letzten Einheit abgerufen hat, ist praktisch ohne Belang. Weiterhin erscheinen für solche Szenarien eher anonyme Diskussionsforen geeignet, da sie vor allem dazu dienen, Rückfragen gegenüber dem Dozenten zu stellen. „Da werden eh nur die schlauen Fragen gestellt. Die dummen werden doch woanders diskutiert." – ein wörtliches Zitat eines Studenten, das daraufhin deutet, dass unter den Bedingungen fehlender Anonymität viele für den Lehrenden brauchbare Rückmeldungen unterbleiben.

Jedoch werden die Systeme auch in wenigen Veranstaltungen weitergehend genutzt. Dort werden angepasste didaktische Konzepte [KHM02] erprobt und gerade diese Veranstaltungen sind dann auch auf die weitergehenden Funktionen, die Awareness ermöglichen, angewiesen. Beispielsweise ist es in kooperativen Szenarien für Studierende sinnvoll, direkt zu sehen, was Kommilitonen verändert haben, seitdem man selbst zuletzt in der E-Learning-Plattform aktiv war, wenn das gemeinsame Erarbeiten von Inhalten Teil des didaktischen Konzeptes ist. Für solche Veranstaltungen können Systemfunktionalitäten, die auf detaillierte Protokollierungen angewiesen sind, erforderlich sein.

Veranstaltungsbezogene Konfiguration der erhobenen Daten

Was den Plattformen zunächst offensichtlich fehlt, ist eine flexible Konfiguration der Verhaltensaufzeichnung auf verschiedenen Ebenen: die geringeren Datenerhebungsbedarfe für Vorlesungen müssen ebenso einstellbar sein, wie umfassendere Bedarfe für komplexe Szenarien, wie Teamwork in Übungsgruppen etc. Eine veranstaltungsbezogene Einstellbarkeit der Datenerhebung wäre gegenüber dem aktuellen Stand der Systemoptionen bereits ein großer Schritt, jedoch wäre es noch viel wünschenswerter, die gesamte Konfigurierbarkeit so umzustellen, dass die Erhebung durch die Nutzung von Funktionen erst ausgelöst wird. Aus Datenschutzsicht ist die Datenerhebung immer vom eigentlichen Zweck ausgehend zu motivieren. Diesem Weg folgend ist es erforderlich, erst beim (zulässigen) Einschalten einer (Benachrichtungs-) Funktion die dazu nötige Aufzeichnung von Ereignissen einzuschalten.

Um die Erforderlichkeit beurteilen zu können, wurde von der praktischen Anwendung ausgegangen. In fünf Interviews mit Lehrenden und Beratungspersonen ist der Einsatz des LMS betrachtet worden, um tatsächlich existierende Erforderlichkeiten zu erheben. In der Analyse zeigte sich, dass die komplexe Summe der Anwendungen (vgl. Abb. 1) gruppierbar ist, und für diese Gruppen bei der Nutzung derselben Funktionalität unterschiedliche Erforderlichkeiten in jeweils unterschiedlichen Kontexten bestehen. Beispielsweise kann ein Diskussionsforum in einer Seminarveranstaltung, wo Inhalte über ein solches Forum kollaborativ erarbeitet werden sollen, gegenüber anderen Teilnehmern genaue Zeiten und Autoren offenbaren, wohingegen ein Forum, dass in erster Linie als Kommunikationskanal zwischen Lehrenden und einer Vorlesung dient, sinnvoll auch anonym betrieben werden kann. Für die weitere Konzeption wurden Cluster von Systemmodulen (Szenarien) gebildet, die auf der Basis der Empirie als zusammengehörend ermittelt wurden (s. Tabelle 1). Ziel bei diesen Gruppierungen ist es, die Selektionen bei

der Konfiguration zu vereinfachen und aus dem Einsatzzweck heraus zu motivieren. Unabhängig von einem konkreten System wurde auf der Basis dieser Szenarien ein Systeminterface (vergleichbar eines Wizards) entworfen, das es Lehrenden ermöglichen soll eine für die Zwecke angemessene und datenschutzkonforme Konfiguration des Systems vorzunehmen. Im Detail enthalten einige der Module Varianten, wo einzelne technische Bestandteile hinzu- oder abgeschaltet werden können.

1. Dokumentenverteilung	Einfache Vorlesungen, in denen Studierende Vorlesungsinformationen anonym abrufen können
2. Umfassende Vorlesungsbegleitung	Für Vorlesungen (im wesentlichen anonyme Nutzung) mit Übungsbetrieb (personenbezogene Nutzung)
3. Ideensammlung	Informationssammlung und Bewertung mit anonymer oder personenbezogener Nutzungsmöglichkeit
4. Kooperatives Texte verfassen	Collaborative Writing : Gemeinsames Erstellen von Dokumenten (Personenbezogene Nutzung)
5. Referatsvorbereitung	Forum und Dokumentaustausch, Abgaben an Dozierende
6. Arbeitsgruppen und Projektarbeit	Gemeinsame Dokumentenerstellung in geschütztem Arbeitsraum (Forum) mit abschließender Abgabe an Dozierende
7. Sprachlernen	Spezielle Module für das Sprachlernen, Personenbezogen
8. Vorbereitungskurs	Anonymer auf WBT basierender selbstgesteuerter Lernprozess.

Tabelle 1: Gruppierung von Einsatzzwecken

In einem praktischen System könnten „Policies“ für diese Szenarien die Standardfälle definieren. Jeder Lehrende kann also anhand seiner Erfordernisse den Einsatz planen, dabei werden die Datenschutzanforderungen gewahrt. Selbstverständlich kann für die dann übrigbleibenden Einzelfälle eine individuelle Lösung auch mit individueller Beratung konfiguriert werden. Die Analyse der tatsächlichen Nutzung der Systeme zeigt, dass das aktuell wenige Einzelfälle sind, für die dieser Aufwand zu rechtfertigen ist.

6. Zusammenfassung und weitere Entwicklungen

Dieser Beitrag beschreibt Datenschutzgrundlagen und Hinweise für Lösungen von existierenden Datenschutzproblemen. Detailliert wurde aufgezeigt, wie der Datenumfang in den Systemen auf das Erforderliche beschränkt werden kann, wobei aber der einzelne Lehrende weiterhin die Entscheidungen für seine Veranstaltungen trifft. Es existiert eine Reihe von weiteren technischen Bausteinen zur Behebung der Probleme. Teilweise kann auf verfügbare technische Lösungen zurückgegriffen werden. Allerdings sind die verschiedenen Lösungsansätze zu einem konsistenten Gesamtsystem zu verbinden. Grundlagen und Bausteine sind dabei ein weitgehendes Identity Management (z.B. vergleichbar Shibboleth), ein ausgefeiltes rollenbasiertes Berechtigungssystem (überlappende orthogonale Rollen), Transparenz der Transparenz, Kontrollmechanismen und ergono-

mische Verbesserungen (bspw. bzgl. der Nachvollziehbarkeit von Folgen von Systemeinstellungen).

Neben diesen Lösungsansätzen, die aus der Betrachtung der rechtlichen Rahmenbedingungen im europäischen Raum entstanden sind, kann die Berücksichtigung der Symmetrien und Asymmetrien und die angemessene Gestaltung für diese sozialen Strukturen die Motivation zur Nutzung der Systeme fördern.

Literaturverzeichnis

[Bi07] Bizer, J. (2007): Sieben goldene Regeln des Datenschutzes. Datenschutz und Datensicherheit 31(5), 350-356.

[BS93] Bellotti, V.; Sellen, A. (1993): Design for Privacy in Ubiquitous Computing Environments. Third European Conf. Computer-Supported Cooperative Work ECSCW'93 (Milano, Italy), 77-92. Dordrecht, Kluwer.

[Ch85] Chaum D. (1985): Security without Identification: Transaction Systems to make Big Brother Obsolete. Communications of the ACM, 28(10):1030–1044, October 1985.

[Cl93] Clement, A. (1993): Working in (and on) the Electronic Fischbowl? Privacy Aspects of Multi-Media Communications. NetWORKing 1993: 123-132

[DB92] Dourish, P.; Bellotti, V. (1992): Awareness and coordination in shared workspaces. ACM Press: New York, NY, USA.

[Ec03] Eckert, C. (2003): Sicherheit und E-Learning. Beitrag zum Workshop „E-Learning: Beherrschbarkeit und Sicherheit“. TU Ilmenau. Juli 2003.

[Ei08] Eibl, C. J. (2008): Vertraulichkeit persönlicher Daten in Lern-Management-Systemen. Seehusen, S.; Lucke, U. & Fischer, S., ed. (2008): DeLFI 2008, Lübeck, Germany, Vol. 132, GI, pp. 317-328.

[Fr06] Franz, E., Böttcher, A., Wahrig, H., Borcea-Pfitzmann, K.: Access Control in a Privacy-Aware eLearning Environment. In: Proceedings of AReS 2006, Workshop on Security in eLearning (SEL), Vienna, April 2006.

[HH08] Hansen, J. & Hatteh, N. (2008), Datenschutz beim E-Learning - Zum Verhältnis von Kontrolle und Vertrauen in der Informationsgesellschaft. in: Seehusen, S.; Lucke, U. & Fischer, S., eds.: DeLFI 2008, Lübeck, Germany, Vol. 132, GI, 2008, pp. 329-340.

[JSP02] Jang, C.-Y.; Steinfeld, C.; Pfaff, B. (2002): Virtual team awareness and groupware support: an evaluation of the TeamSCOPE system. In: International Journal of Human-Computer Studies 56(1). S. 109-126.

[Me06] Meints, M. (2006): Protokollierung bei Identitätsmanagementsystemen, Anforderungen und Lösungsansätze. Datenschutz und Datensicherheit 30(5), S. 204

[KHM02] Koschmann, T.; Hall, R. & Miyake, N. (2002): CSCL2: Carrying Forward the Conversation. Lawrence Erlbaum Associates.

[RBE03] Rezgui, A.; Bouguettaya, A.; Eltoweissy, M. (2003): Preserving Privacy in the Web: Facts, Challenges and Solutions. IEEE Security&Privacy, Vol. 1, No. 62003.

[Ki04] von Kiedrowski, J. (2004): Open-Source-Software – E-Learning zum Nulltarif? In: Hohenstein, A.; Wilbers, K. (Hrsg.): Handbuch E-Learning. S. 1–15.

[We05] Welch, V., Barton, T., Keahey, K., Siebenlist, F. (2005): Attributes, Anonymity, and Access: Shibboleth and Globus Integration to Facilitate Grid Collaboration, Proceedings of the 4th Annual PKI R&D Workshop, 2005.

[WGT08] Int. Working Group on Data Protection in Telecommunications (2008): Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten – Rom Memorandum, 43. Sitzung, März 2008, Rom.