Datenschutz, Datensicherheit und ethische Aspekte in der Lehrevaluation

Meinald T. Thielsch, Christian Meese und Martin Salaschek
Westfälische Wilhelms-Universität Münster, Institut für Psychologie

Bei Lehrevaluationen investieren wir viel Zeit in die Konstruktion guter Befragungsinstrumente, das Erreichen hoher Rücklaufquoten oder die Rückmeldung der Ergebnisse. Wir fassen unsere Maßnahmen in breite Evaluationsmodelle zusammen und versuchen, sinnreiche Konsequenzen abzuleiten (vgl. Thielsch & Hirschfeld, 2011). Dabei sollten wir jedoch drei zentrale Aspekte keinesfalls aus den Augen verlieren: Datenschutz, Datensicherheit und die ethische Dimension unseres Handelns in der Evaluation. Eine Berücksichtigung dieser Aspekte ist nicht nur rechtlich essentiell (vgl. Bundesdatenschutzgesetz, BDSG), sondern wird auch die Akzeptanz einer Evaluation maßgeblich fördern. Daher wollen wir auf diese Gesichtspunkte im Folgenden nacheinander eingehen und abschließend eine Checkliste zur praktischen Umsetzung anbieten.

Datenschutz und Datensicherheit

Womöglich am wichtigsten ist beim Datenschutz stets die Aufklärung und Sensibilisierung aller Beteiligten hinsichtlich der Datensicherheit. Besonderes Augenmerk ist hierbei auf die Datenerhebung, -verarbeitung und -archivierung zu legen.
Insgesamt kann und sollte eine Vielzahl von Maßnahmen ergriffen werden, um die Sicherheit und Integrität von Evaluationsdaten zu gewährleisten. Es mag trivial klingen, doch die sichersten Daten sind die, die nicht erhoben werden. Ein erster Schritt sollte daher schon im sparsamen Erheben von Daten bestehen – es sollte nur erfasst werden, was wirklich für die Auswertung benötigt wird. Hier lohnt es sich auch, bestehende Systeme kritisch zu hinterfragen: Werden Variablen nicht in die Auswertung einbezogen, so erzeugen sie bei der Erhebung unnötigen Aufwand und machen Datensätze unübersichtlicher. Besonders bei allen personenbezogenen Daten ist zu prüfen, ob eine Erhebung notwendig ist, da mit deren Missbrauch meist der größte Schaden angerichtet werden kann; ein Abwägen zwischen Komfort und Sicherheit ist hier unabdingbar. So kann die Speicherung von Nutzerkennungen zwar dem/der Evaluierenden dazu dienen, bei einer Onlineevaluation personalisiert alle belegten Veranstaltungen aufzuführen, jedoch auch für eine Rückverfolgung von Evaluationen auf Personen missbraucht werden. Die Verwendung von (pseudonymisierenden) Prüfsummen – sogenannten Hashs – kann das verhindern.

Datenerhebung und -verarbeitung

In der Datenerhebung und -verarbeitung mag man zunächst denken, dass Online-Evaluationen (vgl. Gumpinger, 2008) besondere Aufmerksamkeit beim Datenschutz erfordern. Da in der Regel aber die Daten aus Paper-Pencil-Befragungen digitalisiert werden, gehen Fragen der Datensicherheit weit über Online-Spezifika oder eine zugriffsgeschützte Lagerung und Verarbeitung von Papierfragebögen hinaus. Ebenso müssen die technischen Systeme selbst sicher gemacht werden. Hierzu sollten folgende Maßnahmen ergriffen werden:

- Eine sichere Datenübertragung ist zu gewährleisten, das heißt: Bei Online-Erhebungen sichere Verbindungen über https:// nutzen, bei Offline-Erhebungen unberechtigten Zugriff (was die evaluierte Person einschließt) verhindern. Unverschlüsselte Datenübertragungen erleichtern das „Mitlesen“ des Datenverkehrs bei der Übertragung (z. B. in Drahtlosnetzwerken) erheblich.
- Direkt anschließend an die Erfassung und Speicherung ist für eine sichere Verschlüsselung sensibler Daten zu sorgen, bspw. mit der kostenfreien Open-Source Software Truecrypt (http://www.truecrypt.org/). Keinesfalls dürfen sensible Daten unzureichend verschlüsselt gespeichert werden.
- Sichere Passwörter sind grundsätzlich zentral bei der digitalen Arbeit. Sie sollten komplex genug sein um sogenannte Brute-Force-Angriffe möglichst aussichtslos zu machen (Tipps z. B. unter http://de.wikipedia.org/wiki/Passwort) – das bedeutet derzeit eine Passwortlänge von mindestens 20 Zeichen, die nicht sinnvoll zusammenhängen und Sonderzeichen sowie Zahlen, Klein- und Großbuchstaben mit einschließen. Auch die Verschlüsselung von Daten ist wertlos, wenn das entsprechende Passwort leicht zu knacken ist. Auf den „Mehrfacheinsatz“ von Passwörtern für verschiedene Datenquellen (z. B. Betriebssystempasswort und Datensatzverschlüsselung) ist unbedingt zu verzichten, da bei Kompromittierung eines einzelnen Passworts mehrere Datenquellen unsicher geworden wären. Passwörter sollten regelmäßig geändert werden (i.d.R. mindestens einmal jährlich, bei häufig genutzten Passwörtern auch öfter) bzw. für neue Datensätze neue Passwörter gesetzt werden, die sich durch mehr als z. B. eine Jahreszahl unterscheiden.
- Die Softwaresicherheit der verwendeten Computer muss hergestellt werden, konkret: Alle relevanten Programme und das Betriebssystem sind auf dem neusten Stand zu halten; bei Bedarf sollten entsprechende Firewalls und Virenscansoftware eingesetzt werden.

- Alle Beteiligten sollten, wann immer möglich, die Zugriffsrechte auf Daten jeweils an die Nutzergruppen anpassen und zielgenau einschränken. Hierbei ist unbefugten Dritten ein Zugriff zu erschweren, z. B. über einen automatischen Kennwortschutz für die verwendeten Arbeitsplatzrechner. So sperrt sich automatisch ein Computer, an dem gerade nicht gearbeitet wird, nach einer bestimmten Zeit (z. B. 2 Minuten Inaktivität) und verhindert dadurch einen zufälligen Zugriff.
- Kein blindes Vertrauen in Benutzer bzw. verwendete Software. Kleine Fehler in der verwendeten Erhebungssoftware können große Sicherheits- oder Integritätsrisiken für die erhobenen Daten zur Folge haben. Wo möglich sollte daher verbreiteter Open-Source Software der Vorzug vor neuen Programmierungen gegeben werden (vgl. Köhntopp, 2000).

Datenaufbewahrung und -archivierung

Die Archivierung der erhobenen Evaluationsdaten ist ebenfalls eine Phase, die Beachtung erfordert. Bevor Daten nach Ablauf der gültigen Aufbewahrungsfristen vernichtet und gelöscht werden können sind mehrere Punkte zu beachten: Personendaten sollten anonymisiert oder pseudonymisiert sein, die Daten bzw. Zuordnungslisten für Pseudonyme grundsätzlich zugriffssicher gelagert werden. Selbstverständlich darf zu keinem Zeitpunkt eine Weitergabe der Daten an Dritte erfolgen. So erhalten beispielsweise Lehrende keine Originalfragebögen oder Rohdaten mit demographischen Angaben der Studierenden, Einzeldaten werden zusammengefasst oder anonymisiert berichtet. Zu einem guten Datenarchiv gehört aber auch ein funktionierendes Datenmanagement. Das heißt, es werden regelmäßige (verschlüsselte) Backups erstellt und dabei auch ortsunabhängige Sicherungskopien (beispielsweise am Arbeitsplatz und bei einem Anbieter von Cloudspeicher) angelegt. Alle relevanten Arbeitsschritte bleiben durch stetige Protokollierung (z. B. mit Hilfe von Checklisten) nachvollziehbar.

Ethische Aspekte

Ethische Aspekte sind in der Evaluation doppelt relevant – müssen doch die Interessen sowohl der Evaluierten als auch der Evaluierenden geschützt werden. Dabei wird den Evaluierenden Anonymität zugesichert, potentiell könnten diese jedoch z. B. durch Fachsemester-Angaben oder offene Kommentare in der Datenauswertung identifizierbar werden. Daher ist es wichtig bspw. nur dann eine Evaluation auszuwerten, wenn eine

ausreichende Menge an Daten vorliegt. In ihren Standards für Evaluation sagt die DeGEval (DeGEval – Gesellschaft für Evaluation e.V., 2008): „Evaluationen sollen so geplant und durchgeführt werden, dass Sicherheit, Würde und Rechte der in eine Evaluation einbezogenen Personen geschützt werden.“ Dies schließt eine unparteiische, faire und vollständige Evaluation ebenso ein wie die Transparenz von Verfahren und Ergebnissen.
Gerade Online-Lehrevaluationen stellen eine zusätzliche inhaltliche und technische Herausforderung dar: Aufgrund der teilweise unkontrollierbaren Bedingungen der Datenerhebung und der Identität der Befragten sind hier Maßnahmen zur Überprüfung der Datenqualität wichtig. So sollten die Daten auf untypische Antwortmuster oder -zeiten (sog. *data forensic*) und offene Nennungen auf unangemessene Äußerungen geprüft werden (z. B. mit automatischen Bashwordchecks, also der automatischen Suche nach unangebrachten oder beleidigenden Äußerungen oder anhand von sehr geringer Varianz in den Antwortmustern trotz einiger anders gepolter Items). Hinsichtlich ethischer Aspekte empfiehlt sich insbesondere bei Online-Erhebungen ein Blick in die einschlägige Literatur (bspw. Dzeyk, 2001). Online-Erhebungen bieten anderseits für derartige Kontrollen eine Reihe von technischen Vorteilen (vgl. Thielsch & Weltzin, 2012), angefangen mit Kontrollskripten in den Erhebungsmasken bis hin zur einfachen Durchsuchbarkeit der digital vorliegenden Nennungen.

Verschiedene weitere Maßnahmen sollten zum Schutz der Evaluierenden insbesondere in der Datenerhebungsphase ergriffen werden:

- Grundsätzlich müssen ausreichende Informationen zur jeweiligen Evaluation und deren Zielen gegeben werden.
- Die Freiwilligkeit der Teilnahme aller Evaluierenden ist sicherzustellen.
- Ein Ansprechpartner sollte für Rückfragen und Probleme benannt werden
- Eine explizite Einverständniserklärung (informed consent) in die Datenverwendung oder die Möglichkeit eines freiwilligen Selbstausschlusses der eigenen Daten aus der Evaluation sollte gegeben sein.
- Werden bei einer Online-Erhebung zusätzliche nonreaktive Daten der Befragten erhoben oder Daten im Längsschnitt verknüpft werden, muss explizit darauf hingewiesen werden.

Hinsichtlich der ethischen Bedingungen, aber auch zur Sicherstellung eines positiven Evaluationsklimas empfiehlt es sich, an das verantwortungsvolle Handeln aller Beteiligten zu

appellieren. Es ist hilfreich, den verschiedenen Statusgruppen in der Evaluation gleichermaßen Netiquette und zentrale Feedbackregeln nahe zu legen (Beispiele aus unserer Arbeit finden sich unter http://www.uni-muenster.de/PsyEval). Evaluation lebt hierbei von einer umfassenden Information aller Beteiligten.

Checkliste zu Datenschutz, Datensicherheit und ethischen Aspekten in Evaluationen

Allgemeines:

- ☐ Wurden alle beteiligten Personen hinsichtlich Datenschutz, Datensicherheit und ethischen Fragen ausreichend informiert und sensibilisiert?
- ☐ Wurden alle Beteiligten umfassend über Ablauf und Ziele der jeweiligen Evaluation informiert?

Datenerhebung:

- ☐ Werden nur Daten erhoben, die für die Auswertung benötigt werden?
- ☐ Ist eine sichere Datenerhebung gewährleistet (online: sichere Verbindungen, offline: kein unerlaubter Zugriff auf Fragebögen)?
- ☐ Sind Ansprechpartner für Rückfragen benannt?
- ☐ Ist über eventuelle Datenverknüpfungen oder nonreaktive Erhebungen ausreichend informiert worden?
- ☐ Gibt es einen informed consent, bzw. die Möglichkeit eines freiwilligen Selbstausschlusses?
- ☐ Werden Daten grundsätzlich sicher verschlüsselt gespeichert?
- ☐ Sind alle relevanten Passwörter sicher?
- ☐ Sind die verwendeten Computersysteme sicher?
- ☐ Sind die Zugriffsrechte eindeutig und korrekt gesetzt?

Datenverarbeitung- und Aufbewahrung:

- ☐ Werden Daten hinsichtlich ihrer Qualität geprüft (z. B. Bashword-Checks, Checks für untypische Antwortmuster oder Speicherfehler)?
- ☐ Werden Daten grundsätzlich nur anonymisiert weitergegeben?
- ☐ Werden regelmäßige und ortsunabhängige Backups angelegt?
- ☐ Sind alle Arbeitsschritte nachvollziehbar protokolliert?

Literatur

Bundesdatenschutzgesetz (BDSG). Verfügbar unter: http://www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf (Abruf am 10. Juli 2012)

DeGEval – Gesellschaft für Evaluation e.V. (2008) (Hrsg.). *Standards für Evaluation*, (4. unveränderte Auflage). Mainz.

Dzeyk, W. (2001). Ethische Dimensionen der Online-Forschung. *Kölner Psychologische Studien, Jahrgang VI, Heft, 1,* 1-30. Verfügbar unter http://kups.ub.uni-koeln.de/volltexte/2008/2424/ (Abruf am 10. Juli 2012)

Gumpinger, M. (2008). *Online Lehrevaluationssysteme: Anforderungen und Implementation am Beispiel des Medizinischen Curriculums*. München: Unveröffentlichte Dissertation. Verfügbar unter http://edoc.ub.uni-muenchen.de/8382/1/Gumpinger_Marc.pdf (Abruf am 10. Juli 2012)

Köhntopp, K., Köhntopp, M & Pfitzmann, A. (2000). Sicherheit durch Open Source? Chancen und Grenzen. *Datenschutz und Datensicherheit 9/2000,* Verfügbar unter http://semper.schunter.org/sirene/publ/KoeKP_00.pdf (Abruf am 10. Juli 2012)

Thielsch, M. T. & Hirschfeld, G. (2011). Integration und Konsequenzen von Hochschulevaluationen in der Praxis. In: M. Krämer, S. Preiser & K. Brusdeylins (Hrsg.). *Psychologiedidaktik und Evaluation VIII* (S. 289-297). Aachen: Shaker-Verlag.

Thielsch, M. T. & Weltzin, S. (2012). Online-Umfragen und Online-Mitarbeiterbefragungen. In M. T. Thielsch & T. Brandenburg (Hrsg.), *Praxis der Wirtschaftspsychologie II* (S. 109-127). Münster: MV Wissenschaft.

Kontaktadresse

Dr. Meinald T. Thielsch
Westfälische Wilhelms-Universität Münster
Institut für Psychologie
Fliednerstr. 21
48149 Münster
http://www.uni-muenster.de/psyeval

Zitation dieses Beitrags

Thielsch, M. T., Meese, C. & Salaschek, M. (2012). Datenschutz, Datensicherheit und ethische Aspekte in der Lehrevaluation. In M. Krämer, S. Dutke & J. Barenberg (Hrsg.): *Psychologiedidaktik und Evaluation IX* (S. 395 - 400). Aachen: Shaker.