Internationale Arbeitsgruppe für
Datenschutz in
der Telekommunikation

675.54.9

Arbeitspapier zum Thema E-Learning-Plattformen

61. Meeting, 24.–25. April 2017, Washington D.C. (USA)

Einführung

1. E-Learning-Plattformen erfreuen sich weltweit wachsender Beliebtheit. Sie ermöglichen die Einrichtung eines „virtuellen Kursraumes“, in dem Lehrkräfte Lernmaterialien zur Verfügung stellen und Leistungsüberprüfungen durchführen können. Zudem fördern viele dieser Plattformen kollaboratives Lernen und ermöglichen die Kommunikation zwischen Lernenden und Lehrenden. E-Learning-Plattformen werden immer stärker in das Curriculum eingebunden, sodass ihre Nutzung schon bald gang und gäbe sein wird.

2. Bis vor Kurzem beschränkte sich die Leistungsbeurteilung der Lernenden und die damit verbundene Datenerhebung fast ausschließlich auf Prüfungsergebnisse und Anwesenheit. Mit dem zunehmenden Einsatz von E-Learning-Plattformen wächst die Menge an personenbezogenen Daten, die über die Lernenden zur Verfügung stehen. Diese reichen von Informationen über die Nutzung von Lernmaterialien und die Bearbeitung von Aufgaben (beispielsweise die Zeit, die investiert oder benötigt wurde, um die Aufgabe durchzulesen) bis hin zur Unterrichts-/Kursteilnahme und sonstigen bildungsbezogenen Aktivitäten (z. B. Benotung). Je stärker der Unterricht auf virtuellen Kursräumen oder elektronischen Geräten basiert, desto spezifischere und umfassendere digitale Daten werden über die Lernenden sowie ihr Verhalten und ihre Leistungen generiert. Zudem könnte die große Menge an digitalen Daten über Schüler und Studierende sowie deren Verhalten die Nachfrage nach einer verstärkten Datennutzung im Bildungsbereich ankurbeln, z. B. in Form von „Learning Analytics“[1].

3. Auf Universitätsebene bieten viele Einrichtungen – oft in Partnerschaft mit Privatunternehmen – bereits sogenannte „Massive Open Online Courses“ (MOOCs) an, bei denen sich Teilnehmerinnen und Teilnehmer für Universitätskurse einschreiben können, die online abgehalten werden. Solche Kurse finden nicht in traditionellen Kursräumen statt und mit ihnen geht häufig

[1] Learning Analytics kann bezeichnet werden als „das Messen, Sammeln, Analysieren und Auswerten von Daten über Lernende und ihren Kontext mit dem Ziel, das Lernen und die Lernumgebung zu verstehen und zu optimieren“, Learning and Academic Analytics, G. Siemens, 5. August 2011, http://www.learninganalytics.net/?p=131

Sekretariat
Berliner Beauftragte für
Datenschutz und Informationsfreiheit
Friedrichstr. 219
10969 Berlin
Tel.: +49 30 13 88 90
Fax: +49 30 21 55 050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

eine grenzüberschreitende Erhebung von personenbezogenen Daten der Teilnehmerinnen und Teilnehmer einher[2]. Die digitalen Plattformen erfassen jede einzelne Interaktion zwischen dem/der Lernenden, der Lehrkraft und der Lernumgebung. Häufig wird weder den Lernenden noch den Lehrkräften klar sein, was mit den erhobenen Daten genau geschieht.

4. Die Sensibilität der digitalen Daten von Schülern und Studierenden sollte keinesfalls unterschätzt werden. Personenbezogene Daten zum Lernverhalten können als besonders sensibel angesehen werden, da diese Daten Informationen zu den Interessen und Fähigkeiten der Lernenden, ihrer Merkfähigkeit, ihrer Schnelligkeit bei der Aufgabenbearbeitung und ihrer Lernbereitschaft umfassen. Im Rahmen von Datenanalysen könnten diese Daten auch genutzt werden, um Prognosen in Bezug auf die berufliche Zukunft und Karrierechancen der Lernenden zu treffen[3]. In einigen Staaten der USA beispielsweise werden Daten aus dem primären und sekundären Bildungsbereich – also vom Kindergarten bis zum 12. Schuljahr („K-12“) – mit Arbeitnehmerdaten verknüpft[4]. Bestimmte E-Learning-Plattformen nutzen die von den Schülern und Studierenden erfassten Daten für neuartige Analysen (z. B. um Legasthenie prognostizieren zu können) und in einigen Fällen für kommerzielle Zwecke[5]. Durch die zunehmende Digitalisierung von Schüler- und Studierendenakten und den Einsatz neuer Analysetechniken sind die Lernenden einer allgegenwärtigen Beobachtung ausgesetzt, die die Grundrechte der Privatsphäre und der geistigen Freiheit massiv bedrohen können.

5. In den meisten Fällen werden die Daten, die im Zusammenhang mit E-Learning-Plattformen verarbeitet werden, nicht bei der Schulverwaltung gespeichert. Viele Bildungseinrichtungen beauftragen externe Cloudanbieter mit der Speicherung und Verarbeitung der Schüler- und Studierendendaten. Cloudgestützte Plattformen bergen jedoch zusätzliche Datenschutz- und Sicherheitsrisiken[6]. Ein besonderes Problem kann sich aus der Kontrollverteilung zwischen den Lehranstalten und den Anbietern von E-Learning-Plattformen ergeben.[7] Die

---

[2] Steve Kolowich: „*Are MOOC-Takers 'Students'? Not When It Comes to the Feds Protecting Their Data“,* THE CHRONICLE OF HIGHER EDUCATION, 3. Dezember 2014, http://chronicle.com/article/Are-MOOC-Takers-Students-/150325.

[3] Singapur beispielsweise arbeitet an der Entwicklung einer „Total Online Learning Solution“, die Aus- und Weiterbildungs- mit Lerndaten kombiniert. Jedem Schüler wird bereits im Kindergarten ein sogenannter „Learning Record Store“ zugewiesen, der alle Lerndaten erfasst; vgl. Frankfurter Allgemeine Zeitung (FAZ) vom 28. Januar 2016, S. 9: „Fürs Überleben lernen wir. Was Unternehmen aus Lerndaten ableiten können“.

[4] Siehe beispielsweise National Center for Education Statistics: „*SLDS Topical Webinar Summary: Linking K12 Education Data to Workforce“*, 28. August 2014; https://nces.ed.gov/programs/slds/pdf/Linking_K12_Education_Data_to_Workforce_August2014.pdf.

[5] Niederländische Datenschutzaufsichtsbehörde (College bescherming persoonsgegevens): Fall z2013-00795, 14. Juli 2014. Schlussfolgerungsbericht: „Onderzoek CBP naar de verwerking van persoonsgegevens door Snappet“ (https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013_snappet.pdf)

[6] Vgl. Arbeitspapier *Cloud Computing – Fragen des Schutzes der Privatsphäre und des Datenschutzes – „Sopot Memorandum“* – 51. Sitzung, 23.–24. April 2012, Sopot (Poland), S. 1–3; https://datenschutz-berlin.de/attachments/875/Sopot_Memorandum.12.6.12.pdf

[7] Ariel Bogle: *What the Failure of inBloom Means for the Student-Data Industry*, SLATE, 24. April 2014; http://www.slate.com/blogs/future_tense/2014/04/24/what_the_failure_of_inbloom_means_for_the_student_data_industry.html.

Anbieter legen nämlich oft standardmäßige Geschäftsbedingungen fest, die ihnen mitunter sehr viel Spielraum für die Nutzung der Daten zu ihren eigenen Zwecken einräumen – und die oftmals nicht mit der Bildungsmission der Einrichtung vereinbar sind. Zudem könnten bestimmte Anbieter nicht gewillt sein, wesentliche Pflichten zu erfüllen (z. B. im Zusammenhang mit der Datensicherheit) oder sich an Beschränkungen zu halten (beispielsweise in Verbindung mit grenzüberschreitenden Datenübermittlungen), was jedoch unerlässlich ist, um das erforderliche Maß an Schutz gewährleisten zu können.

Umfang

6. Im Rahmen dieses Dokuments wird „E-Learning“ als Nutzung technischer Instrumente und Medien verstanden, die die Kommunikation von Wissen, die Wissensentwicklung sowie die Interaktion zwischen Lehrkräften, Lernenden und Lehranstalten technisch unterstützt. E-Learning-Plattformen beziehen in der Regel eine Vielzahl von Geräten (z. B. Computer und Tablets), Datenverarbeitungs- sowie Nutzungsmodellen (Präsenzschulungen, Onlinekurse usw.) und Akteuren (beispielsweise Lernende, Bildungseinrichtungen, Plattformanbieter und Anwendungsanbieter) ein.

7. Dieses Arbeitspapier beleuchtet die größten Datenschutzrisiken, die E-Learning-Plattformen für die Lernenden bergen, und stellt Empfehlungen für Lehranstalten, Anbieter von E-Learning-Plattformen und Datenschutzbehörden bereit. Mögliche Datenschutzrisiken für Lehrkräfte im Zusammenhang mit der Nutzung von E-Learning-Plattformen (z. B. Leistungsbewertung von Lehrkräften) werden nicht berücksichtigt. Im Zentrum dieses Arbeitspapiers steht die zunehmende Nutzung von E-Learning-Plattformen in der Primar- und Sekundarbildung.

Datenschutzrisiken für die Lernenden

Unrechtmäßige Verarbeitung und fehlende Transparenz

8. In Gesetzen im Schul- und Bildungsbereich werden neue technologische Trends bei Lernverfahren sowie der erweiterte Umfang und die umfassenderen Zwecke der Datenverarbeitung im Zusammenhang mit E-Learning und Learning Analytics oft nicht hinreichend berücksichtigt. Ob die Einwilligung als gültige Rechtsgrundlage angesehen werden könnte, ist ebenfalls fraglich. Eine wirksame Einwilligung muss freiwillig erteilt werden, was im Bildungskontext nur schwer garantiert werden kann – vor allem, wenn die Nutzung von E-Learning-Plattformen verpflichtend ist. Deshalb könnte die Erfassung und Analyse von Schüler- und Studierendendaten in einigen Rechtssystemen ohne die nötige Rechtsgrundlage erfolgen, wenn die Gesetzgeber die Rechte zum Schutz der Privatsphäre und die Datenschutzrechte bei der Datenverarbeitung im Rahmen von E-Learning-Plattformen und Learning Analytics nicht ausreichend abgesichert haben.

9. Die Erhebung oder Nutzung von Schüler- und Studierendendaten erfolgt unter Umständen ohne Wissen der Lehrkräfte, Bildungseinrichtungen, Eltern oder Lernenden. Darüber hinaus sind den Lernenden, Eltern oder Lehrkräften die an

der Datenverarbeitung beteiligten Akteure meist nicht bekannt. Der Mangel an Transparenz wirkt sich direkt auf die Frage der Rechtmäßigkeit der Verarbeitung und des Grundsatzes der Verarbeitung nach Treu und Glauben aus.

Übermäßige Datenerhebung

10. Die Lernenden könnten von einer übermäßigen Erhebung personenbezogener Daten betroffen sein. Es könnten sehr persönliche oder sensible Informationen über sie erfasst sein, wie etwa Standortinformationen, Gesundheitszustand, Schlafverhalten oder Aktivitäten in sozialen Netzwerken[8]. Sportlehrer könnten beispielsweise Tracking- und Auswertungstools einsetzen, die auch gesundheitsbezogene Gewohnheiten und Verhaltensweisen außerhalb des Unterrichts überwachen. Bildungseinrichtungen könnten bei ihren Anstrengungen zur Bekämpfung von Cybermobbing versucht sein, die Aktivitäten der Schüler und Studierenden in sozialen Netzwerken zu beobachten. Mit solchen Aktivitäten würden sie unangemessen in das Privatleben der Schüler und Studierenden eingreifen. In diesen Zusammenhängen ist es wichtig, den Verhältnismäßigkeitsgrundsatz zu beachten, insbesondere wenn es um Maßnahmen geht, die sich auf Aktivitäten von Schülern und Studierenden außerhalb des Bildungskontextes erstrecken.

11. Im Zusammenhang mit Learning Analytics kann der Umfang an Informationen, die über die Lernenden angefordert werden, sogar noch größer sein. Bestimmte Analysetools nutzen Informationen über Aktivitäten in sozialen Netzwerken, Protokolle von Online-Spielen, Online-Communitys und von physiologischen Sensoren erfasste Daten, wie etwa Eye-Tracking- oder Motion-Capture-Daten. Hierbei können Datensätze zu kognitiver Entwicklung, sozialem Lernen, Diskursverläufen, Interaktionen in einem Netzwerk, Lernpfade in Kursen, Ausbau von Kompetenzen und Verhalten bei der Suche nach Hilfe von Interesse sein[9].

Profiling und automatisierte Entscheidungsfindung

12. Die Art und Menge der mithilfe von E-Learning-Plattformen erfassten Daten erleichtert statistische Analysen und die Erstellung von Profilen. Dies kann zur Folge haben, dass die Lernenden zunehmend auf Grundlage von Gruppenprofilen und nicht mehr aufgrund ihrer individuellen Entwicklung bewertet werden.

13. Bildungseinrichtungen haben zudem keine Kontrolle über die Algorithmen, die im Rahmen von Learning-Analytics-Verfahren genutzt werden und sie überlassen es den Anbietern der E-Learning-Plattformen festzulegen, was die Clickstream-Daten der Schüler und Studierenden über ihren Wissensstand aussagen. Das bedeutet, dass die Lehrkräfte Entscheidungen auf Grundlage von Interpretationen treffen müssen, die sie nicht überprüfen können.

---

8 Khaliah Barnes: *Student Data Collection Is Out of Control*, N.Y. TIMES, 25. September 2014; http://www.nytimes.com/roomfordebate/2014/09/24/protecting-student-privacy-in-online-learning/student-data-collection-is-out-of-control.

9 „Editorial: Datasets for Learning Analytic“, *Journal of Learning Analytics*, *3* (3), 307–311, 2016; http://dx.doi.org/10.18608/jla.2016.32.15

14. E-Learning-Anbieter und andere Unternehmen nutzen die von den Lernenden erfassten Daten, um subjektive Einschätzungen über deren „Geselligkeit“ und „Enthusiasmus“ zu treffen[10]. Die menschlichen Tätigkeiten innewohnende Fehleranfälligkeit bei der Datenerzeugung und auch Systementwicklung können zu ungerechten Ergebnissen für die Lernenden führen, insbesondere für Angehörige von Gruppen, die bereits in der Vergangenheit Diskriminierungen erlebt haben. Folgerungen und Beurteilungen in Bezug auf die Lernenden, die nichts mit akademischer Leistung zu tun haben, könnten die Betroffenen stigmatisieren und ihre Bildungschancen einschränken.

15. Eltern, Schüler und Studierende haben unter Umständen weder Zugriff auf die Daten, die für die Entscheidungsfindung herangezogen werden, noch auf Informationen über den Prozess der Entscheidungsfindung (Funktionsweise der Analysen) oder die Schlussfolgerungen, die den in Bezug auf den Lernenden getroffenen Entscheidungen zugrunde liegen (z. B. bei der Benotung oder Feststellung potenzieller Lernschwierigkeiten). Dies gilt vor allem für den Einsatz von proprietären Algorithmen, deren Methodik undurchschaubar ist, oder für Systeme, die selbstlernend konzipiert sind, sodass selbst die Entwickler des Systems möglicherweise nicht mehr nachvollziehen können, wie eine bestimmte Beurteilung zustande kommt.

16. Problematisch ist es zudem, wenn es an Mechanismen fehlt, die die Beachtung von Treu und Glauben im Entscheidungsfindungsprozess gewährleisten und die Lernenden und Eltern die Möglichkeit geben, die Beurteilungen anzufechten[11].

Schleichende Funktionserweiterung

17. Privatunternehmen, die mithilfe von E-Learning-Plattformen Daten über die Lernenden erheben, könnten diese Informationen außerhalb des Bildungsbereichs für Data-Mining-Zwecke nutzen[12]. So könnten die Daten beispielsweise genutzt werden, um in der Welt außerhalb der Bildungseinrichtung Entscheidungen über die Zukunftschancen der Lernenden zu treffen, z. B. in Bezug auf Beruf, Wohnmöglichkeiten und Kreditwürdigkeit[13].

---

[10] Natasha Singer: *Deciding Who Sees Students' Data*, N.Y. TIMES, 5. Oktober 2013; http://www.nytimes.com/2013/10/06/business/deciding-who-sees-students-data.html?pagewanted=all

[11] Siehe Marc Rotenberg und Khaliah Barnes: *Student and Data Privacy*, N.Y. TIMES, 3. Mai 2014; http://www.nytimes.com/2014/05/04/business/students-and-data-privacy.html

[12] Google beispielsweise gab zu, E-Mails von Lernenden gelesen zu haben, die das Unternehmen über seine beliebte Plattform Google Apps for Education erfasst hatte. Vgl. Benjamin Herold: *Google Under Fire for Data-Mining Student Email Messages*, EDUCATION WEEK, 26. März 2014; http://www.edweek.org/ew/articles/2014/03/13/26google.h33.html.

[13] In den USA werden beispielsweise bereits Rabatte für gute Leistungen angeboten: So werden anhand der Noten der Lernenden Rabatte bei Autoversicherungen berechnet. Siehe beispielsweise STATE FARM: *Coverage Options That Fit You;* https://www.statefarm.com/insurance/auto/discounts.

Unzureichende Sicherheit

18. Bildungseinrichtungen und Anbieter von E-Learning-Plattformen könnten es versäumen, die von den Lernenden erfassten Daten angemessen zu schützen[14]. Schüler- und Studierendendaten sind immer wieder von Datenlecks betroffen, unabhängig davon, ob sie von der Bildungseinrichtung selbst gespeichert oder an private Anbieter bzw. staatliche Stellen übermittelt werden[15]. Derartige Datenlecks können beispielsweise durch die Nutzung unsicherer Anmeldeverfahren, eine schlechte Konfiguration der Plattform oder anderweitiges menschliches Versagen verursacht werden. Lernende, Lehrkräfte und Administratoren könnten zudem motiviert sein, Sicherheitsvorkehrungen für ihre eigenen Daten (oder die Daten anderer) zum Zwecke des Missbrauchs zu umgehen (z. B. zur Änderung von Noten).

Mangelnde Rechenschaft

19. Gibt es keine klare Verteilung der Rollen und Verantwortlichkeiten an die im Zusammenhang mit dem Einsatz einer E-Learning-Plattform beteiligten diversen Akteure, könnte dies dazu führen, dass weder die Bildungseinrichtungen noch die Anbieter von E-Learning-Plattformen die notwendigen Maßnahmen ergreifen, um Datenschutz- und Datensicherheitsrisiken zu minimieren.

20. Für die Eltern und Lernenden gibt es ggf. keinen zentralen Ansprechpartner, der sich um die Risiken des Schutzes der Privatsphäre und des Datenschutzes kümmert.

Anpassungszwang

21. Das Wissen, dauerhaft beobachtet zu werden, und die Angst vor einem künftigen Missbrauch oder vor der Offenlegung der Daten können eine abschreckende Wirkung haben und die schöpferische Entfaltung und Ausdrucksfähigkeit während der geistigen Entwicklung eines Kindes behindern. Die Lernenden fühlen sich unter Umständen gezwungen, traditionelle Normen zu befolgen, und schrecken vor der Entwicklung innovativer Ideen zurück, da sie befürchten, ihre unkonventionelle Herangehensweise könnte dokumentiert und ihnen dann später irgendwann vorgehalten werden.

---

[14] Siehe z. B. Natasha Singer: *Uncovering Security Flaws in Digital Education Products for School Children*, N.Y. TIMES, 8.Februar 2015, auf Seite B1, *verfügbar* unter: http://www.nytimes.com/2015/02/09/technology/uncovering-security-flaws-in-digital-education-products-for-schoolchildren.html; *D.C. Special-Education Students' Confidential Info Was Publicly Accessible for Years*, WTOP (4. Februar 2015, 5:15 Uhr Ortszeit), http://wtop.com/dc/2015/02/d-c-special-education-students-confidential-info-publicly-accessible-years/; Benjamin Herold: *Danger Posed by Student-Data Breaches Prompts Action*, EDUCATION WEEK, 22. Januar 2014; http://www.edweek.org/ew/articles/2014/01/22/18dataharm_ep.h33.html

[15] Natasha Singer: *Data Security Is a Classroom Worry, Too*, N.Y. TIMES, 22. Juni 2013, auf Seite BU1, *verfügbar unter:*http://www.nytimes.com/2013/06/23/business/data-security-is-a-classroom-worry-too.html

Empfehlungen für Bildungseinrichtungen und Anbieter von E-Learning-Plattformen

22. Trotz der Herausforderungen, die die Nutzung von E-Learning-Plattformen in Bezug auf den Datenschutz mit sich bringt, ist es möglich, diese Arten von Plattformen zu nutzen, ohne bedeutende datenschutzrechtliche Grundsätze zu verletzen. Die Arbeitsgruppe gibt Bildungseinrichtungen und E-Learning-Anbietern die folgenden Empfehlungen, um den beschriebenen Datenschutz- und Sicherheitsrisiken vorzubeugen.

23. Bildungsanstalten sollten bei der Auswahl von E-Learning-Plattformen darauf achten, dass die Anbieter ausreichende Garantien vorsehen, die sicherstellen, dass die Privatsphäre und die Datenschutzrechte der Lernenden in angemessenem Maße geschützt sind.

24. Sowohl Bildungseinrichtungen als auch Plattformanbieter sollten sich über die für sie geltenden rechtlichen Rahmenbedingungen des Datenschutzes sowie über vorhandene Orientierungshilfen informiert halten, die beispielsweise von Datenschutzbehörden herausgegeben werden[16].

25. Bildungseinrichtungen müssen die Einwilligung der Eltern einholen, sofern erforderlich.

26. Bildungseinrichtungen und Anbieter von E-Learning-Plattformen sollten nur so viele Daten von Schülern und Studierenden erheben, wie zur Erreichung des spezifischen Zweckes notwendig ist.

27. Bildungseinrichtungen und E-Learning-Anbieter sollten sicherstellen, dass die Zwecke, zu denen sie Daten erheben, klar festgelegt sind. „Bildungszwecke“ und „Bildungsqualität“ sind beispielsweise sehr schwammige Begriffe, die eine übermäßige Datenerhebung zulassen. Eine gezieltere Erfassung z. B. kann dadurch erreicht werden, dass spezifiziert wird, dass die Datenerhebung erforderlich ist, um „die Lesekompetenz von Fünftklässlern zu fördern“ oder „die Leistung von Oberstufenschülern in Physik zu verbessern“.

28. Bildungseinrichtungen und Anbieter von E-Learning-Plattformen sollten ihre jeweiligen Rollen, Verantwortlichkeiten und Rechte klar zuweisen. Bildungseinrichtungen sollten sicherstellen, dass in der Vereinbarung mit dem E-Learning-Anbieter festgelegt wird, dass dieser Schüler- und Studierendendaten nur gemäß den Anweisungen der Bildungseinrichtung verarbeiten darf. Auch

---

16 So hat die spanische Datenschutzbehörde z. B. vor Kurzem einen Bericht veröffentlicht, in dem die Ergebnisse einer amtlichen Untersuchung von Cloud-Diensten im Bildungsbereich zusammengefasst sowie für alle relevanten Akteure eine Reihe von Empfehlungen bereitgestellt wird. Dabei wird auf Themen wie Sicherheit, Speicherort, Vertragsklauseln, die Beziehung zwischen verantwortlicher Stelle und Auftragsverarbeiter sowie Informationen für Benutzer, Cloud-Dienste und mobile Apps eingegangen. Vgl. http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Inspeccion_cloud_educacion.pdf (in spanischer Sprache). Zudem hat die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder jüngst eine Orientierungshilfe für die Nutzung von E-Learning-Plattformen in Schulen herausgegeben, vgl. https://datenschutz-berlin.de/attachments/1220/OH_Lernplattform_neu.pdf.

Themen wie Datensicherheit, Ort der Datenverarbeitung und die Möglichkeit, unabhängige Audits durchzuführen, sollten berücksichtigt werden[17].

29. Anbieter von E-Learning-Plattformen sollten Schüler- und Studierendendaten nur für die explizit von der Bildungseinrichtung genehmigten Zwecke erheben, nutzen oder übermitteln. Zudem sollten Plattformanbieter die von Schülern und Studierenden erhobenen Daten nicht länger aufbewahren, als es für die Erfüllung der zulässigen Bildungszwecke erforderlich ist[18].

30. Studierende und Eltern haben ein Recht auf leicht zugängliche und klare Informationen über Datenschutz- und Sicherheitspraktiken. Bildungseinrichtungen und E-Learning-Anbieter sollten Informationen über die Kategorien der erhobenen Daten, die Zwecke, zu denen die Daten verarbeitet werden, die an der Verarbeitung beteiligten Akteure, die Dauer der Datenspeicherung und getroffene Sicherheitsvorkehrungen öffentlich bereitstellen.

31. Bildungseinrichtungen müssen sicherstellen, dass sie die volle Kontrolle über Bewertungen oder Beurteilungen im Zusammenhang mit Studierenden behalten, insbesondere im Falle automatisierter Entscheidungsfindung.

32. Bildungseinrichtungen, Plattformanbieter und andere beteiligte Unternehmen sollten bei der Nutzung von Algorithmen und Profilen, die die Entscheidungsfindung beeinflussen könnten, auf lückenlose Transparenz achten. Studierende und Eltern müssen über alle verwendeten Systeme zur automatisierten Entscheidungsfindung oder über sonstige regelbasierte Systeme sowie über die den Entscheidungen zugrundeliegenden Schlussfolgerungen aufgeklärt werden.

33. Algorithmen, Protokolle, Designs und Implementierungen sollten für externe Überprüfungen und/oder Tests zur Verfügung gestellt werden. Offene Audits oder Prüfungen, die von vertrauenswürdigen Instanzen durchgeführt werden, können Gewissheit darüber bringen, dass die E-Learning-Technologie tatsächlich alle versprochenen Merkmale aufweist und keine ungerechten oder diskriminierenden Ergebnisse abliefert.

34. Bildungseinrichtungen und Anbieter von E-Learning-Plattformen sollten datenschutzfördernde Techniken (Privacy Enhancing Technologies (PET)) einbauen, die die Erhebung personenbezogener Daten von Schülern und Studierenden auf ein Minimum beschränken oder ganz verhindern. Wenn möglich, sollten Daten gemäß den Grundsätzen der Datenminimierung, des Datenschutzes durch Technik und der datenschutzfreundlichen Voreinstellungen pseudonymisiert, anonymisiert oder gelöscht werden. Bildungseinrichtungen sollten in Betracht ziehen, die Nutzung der Plattform nur unter Verwendung eines

---

17 Nähere Informationen finden Sie im Arbeitspapier *Cloud Computing – Fragen des Schutzes der Privatsphäre und des Datenschutzes - „Sopot Memorandum“* - der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation, 51. Sitzung, 23.–24. April 2012, Sopot (Poland), S. 3–6; https://datenschutz-berlin.de/attachments/875/Sopot_Memorandum.12.6.12.pdf

18 Siehe auch Student Privacy Pledge: „K-12 School Service Provider Pledge to Safeguard Student Privacy“; https://studentprivacypledge.org/wp-content/uploads/2014/09/Student-Privacy-Pledge-V1.pdf.

Pseudonyms zu erlauben und die echten Namen der Lernenden nicht an den Plattformanbieter weiterzugeben.

35. Bei der Erhebung von Schüler- und Studierendendaten sollten die Datenverantwortlichen die Aufbewahrungsfristen für die verschiedenen Kategorien von Daten explizit festlegen und anwenden um zu gewährleisten, dass die Daten nicht länger als nötig gespeichert werden.

36. Lernende und Eltern sind berechtigt, Zugang zu den Schüler- bzw. Studierendenakten und zu anderen gespeicherten personenbezogenen Daten (z. B. Informationen zum Verhalten) zu erhalten und zu korrigieren, unabhängig davon, wer die Informationen erhebt oder verwaltet.

37. In Bezug auf automatisierte Einzelentscheidungen sollten die Lernenden Zugang zu der Entscheidung und die ihr zugrundeliegenden Schlussfolgerungen erhalten. Es müssen spezifische Verfahren vorgesehen sein, die zu einer Überprüfung von Entscheidungen durch einen Menschen führen, wenn eine andere Sicht eingebracht, Gegendarstellungen vorgebracht oder Entscheidungen angefochten werden.

38. Die Bildungseinrichtungen sollten Situationen vermeiden, in denen sich die Betroffenen gefangen fühlen, etwa wenn die Verarbeitung personenbezogener Daten durch Plattformanbieter eine Black-Box für Schüler und Studierende darstellt, die den Betroffenen keinerlei Transparenz und Kontrolle bietet. Anbieter von E-Learning-Plattformen sollten die Portabilität von Daten in strukturierten, maschinenlesbaren und offenen Formaten ermöglichen (z. B. im Falle eines Schulwechsels).

39. Schüler und Studierende treffen gelegentlich – ohne sich ausreichend informiert zu haben – schlechte Entscheidungen, die sie im Erwachsenenalter beeinträchtigen können. Das Konzept des Rechts auf Vergessenwerden wurde bereits in einigen gesetzlichen Regelwerken berücksichtigt, um die negativen Konsequenzen schlechter Entscheidungen zu minimieren. Bildungseinrichtungen sollten die Schüler und Studierenden über ihre Rechte aufklären und ihr Bewusstsein für mehr Achtsamkeit bei der Veröffentlichung und Weitergabe personenbezogener Daten schärfen. E-Learning-Anbieter sollten Tools integrieren, die eine effektive Ausübung des Rechts auf Vergessenwerden ermöglichen.

40. Bildungseinrichtungen und Plattformanbieter sollten die Daten von Schülern und Studierenden nur in der Form erheben, nutzen und übermitteln, wie es der Kontext zulässt, in dem die Lernenden die Daten bereitstellen. Daten, die sich auf die Nutzung der E-Learning-Plattform beziehen, sollten für keine unvereinbaren anderen Zwecke verwendet oder zur Verfügung gestellt werden.

41. Bildungseinrichtungen sollten eine Datenschutz-Folgenabschätzung und eine Risikoanalyse durchführen, bevor sie eine E-Learning-Plattform einsetzen, sowie die auf Grundlage der dabei ermittelten Ergebnisse notwendigen technischen und organisatorischen Maßnahmen treffen, bevor und solange sie die Dienste einer

solchen Plattform in Anspruch nehmen. Die technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit sollten kontinuierlich überwacht und optimiert werden.

42. Bildungseinrichtungen und E-Learning-Anbieter sollten eine Zwei-Faktor-Authentifizierung beim Anmeldevorgang für Administratoren und Lehrkräfte verwenden, um dem Missbrauch durch gestohlene Passwörter vorzubeugen. Es sollten Richtlinien für Zugriffskontrolle und Protokollierungen festgelegt und durchgesetzt werden um sicherzustellen, dass der Zugriff auf personenbezogene Daten angemessen verwaltet und kontrolliert wird. Der Zugang zu personenbezogenen Daten sollte auf dem sogenannten „Need-to-know-Prinzip" (Kenntnis nur bei Bedarf) basieren.

43. E-Learning-Anbieter sollten Bildungseinrichtungen, Studierende, Schüler und deren Eltern sowie die zuständigen Aufsichtsbehörden im Falle einer Datenschutzverletzung gemäß der jeweils geltenden gesetzlichen Meldepflicht benachrichtigen[19].

Empfehlungen für Datenschutzbehörden

44. Datenschutzbehörden sollten ihre Anstrengungen zur Bewusstseinsschärfung verstärken und Bildungseinrichtungen beraten. So könnten sie beispielsweise die Anwendung von Grundsätzen des Datenschutzes durch Technik bei E-Learning-Anbietern fördern und gleichzeitig ihre Aufsichts- und Kontrolltätigkeiten intensivieren (z. B. durch Durchführung von groß angelegten Datenschutzprüfungen, sogenannten „Privacy Sweeps").

45. Die für den Datenschutz zuständigen Behörden sollten die Implementierung von Verhaltensregeln und Datenschutz-Zertifizierungsverfahren sowie die Erstellung eines angemessenen Rahmenwerks und geeigneter Tools für Datenschutz-Folgenabschätzungen unterstützen, um die Entwicklung datenschutzfreundlicher Lösungen zu fördern.

Empfehlungen für politische Entscheidungsträger

46. Wo es an klaren gesetzlichen Regelungen für die Erhebung, Verarbeitung und Nutzung von Schüler- und Studierendendaten fehlt, sollten solche Regeln festgelegt werden.

47. Werden in bestehenden Gesetzen neue technologische Trends bei Lernverfahren sowie der erweiterte Umfang und die umfassenderen Zwecke der Datenverarbeitung im Zusammenhang mit E-Learning sowie die darauf basierenden Entscheidungen nicht hinreichend berücksichtigt, sollten die Gesetze dahingehend überarbeitet werden[20].

---

[19] Siehe beispielsweise die Festlegungen der OECD bezüglich des Meldens von Datenschutzverstößen im „The OECD Privacy Framework", OECD 2013, verfügbar unter: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[20] EPIC hat ein Rahmenwerk mit dem Titel „Student Privacy Bill of Rights" entworfen, das auf traditionellen Datenschutzgesetzen aufbaut. Vgl. EPIC: *Student Privacy Bill of Rights*,

48. Außerdem sollten politische Entscheidungsträger dafür sorgen, dass der Datenschutz zum Bestandteil von Studienprogrammen und Lehrplänen wird[21].

https://epic.org/privacy/student/bill-of-rights.html. Das Rahmenwerk„Student Privacy Bill of Rights“ hat zahlreiche Bestimmungen aus der Richtlinie 95/46/EG und der Konvention Nr. 108 des Europarates übernommen, einschließlich der Zweckbestimmung, den Anforderungen an die Datensicherheit und der Pflicht zur Gewährleistung der Richtigkeit von Daten für diejenigen, die die Daten speichern. Siehe Khaliah Barnes: *Why a 'Student Privacy Bill of Rights' is Desperately Needed*, WASHINGTON POST, 6. März 2014; https://www.washingtonpost.com/blogs/answer-sheet/wp/2014/03/06/why-a-student-privacy-bill-of-rights-is-desperately-needed.

[21] ICDPPC 38, „Resolution for the Adoption of an International Competency Framework on Privacy Education”, Marrakesch 2016; https://icdppc.org/wp-content/uploads/2015/02/Resolution-2016-on-Privacy-education.pdf.