Daniel Schiffner (Hrsg.): Proceedings of DeLFI Workshops 2018
co-located with 16th e-Learning Conference of the German Computer Society (DeLFI 2018)
Frankfurt, Germany, September 10, 2018

Data-Protection-Compliant Learning Analytics for the Use of External Resources in Learning Portals in Schools

Jan Renz, Dominik Glandorf, Christoph Meinel

Abstract: Learning Analytics becomes more expressive by combining results of various educational resources. However, the usage of a single resource might generate sensitive personal data. To facilitate the application of a broad range of learning tools with regard to data protection, school clouds are able to pseudonymise user identities. This work examines the impact on both the legal and technology when using educational resources pseudonymised. It reports on experiences with a prototypical implementation created collaborating with resource providers. Finally, it takes a look at the required market conditions for data-minimising and cooperative learning analytics.

Datenschutzkonforme Learning Analytics bei Einbindung externer Materialen in Lernportale im schulischen Umfeld

Jan Renz[1], Dominik Glandorf[2], Christoph Meinel[3]

Abstract: Learning Analytics werden durch die Kombination der Ergebnisse verschiedener Lerntools aussagekräftiger. Doch bereits die Analysen eines Tools erzeugen sensible personenbezogene Daten. Um den Einsatz einer Vielzahl von Lerntools an Schulen zu erleichtern und trotzdem Datenschutz zu gewährleisten, können Schul-Clouds die Identität von Nutzern pseudonymisieren. Diese Arbeit untersucht sowohl die datenschutzrechtlichen als auch technischen Auswirkungen einer pseudonymisierten Nutzung von Lerntools. Sie berichtet von Erfahrungen mit einer prototypischen Umsetzung mit kollaborierenden Tool-Anbietern. Schließlich zeigt sie auf, welche Bedingungen im Markt der Lerntools für datensparsame und kooperative Learning Analytics geschaffen werden müssen.

Keywords: Schule, Learning Analytics, Datenschutz, Pseudonymisierung, xAPI, OER

1 Einführung

Fast jeder deutsche Schüler ist online.[4] Gleichzeitig ist die durchschnittliche Internetanbindung von deutschen Schulen schlechter als die eines durchschnittlichen Privathaushaltes, und das obwohl hier hunderte Nutzer statt nur einiger weniger versorgt werden.[5] Doch diese technisch-infrastrukturellen Rahmenbedingungen stellen nur eine der Ursachen dar, warum die Kluft zwischen digitaler Lebenswirklichkeit und Schulalltag immer breiter wird. Den Schulbuchverlagen ist es bislang genauso wie OER-Produzenten (Open Educational Resources) nicht gelungen, die Digitalisierung der Schulen effizient voranzutreiben.

Digitalisierung hat den Auftrag domänenspezifische Vorteile und Mehrwerte zu erschließen und zu generieren. Im schulischen Kontext sind dies bspw. einfacher Zugriff, Interaktivität, Binnendifferenzierung und die damit verbundene Möglichkeit zum „Fordern und Fördern“. Durch diese Anforderungen ergibt sich der Einsatz von Learning Analytics. Im Markt der digitalen Lerninhalte führt dies dazu, dass die interessanten und zukunftsweisenden Angebote keine digitale Variante von im Wesen analogen Inhalten sind, sondern die Mehrwerte der digitalen Welt tatsächlich ausreizen: Individualisierung, Interaktivität und eine nutzungsspezifische Adaptivität. So erkennen Lerntools durch intelligenten Einsatz von Learning Analytics den Fortschritt des Lernenden und bieten

[1] Universität Potsdam, Hasso-Plattner-Institut, jan.renz@hpi.de
[2] Universität Potsdam, Hasso-Plattner-Institut, dominik.glandorf@student.hpi.de
[3] Universität Potsdam, Hasso-Plattner-Institut, christoph.meinel@hpi.de
[4] 98\%, Quelle: Deutsches Institut für Vertrauen und Sicherheit im Internet., 2014
[5] Quelle: Eigene Auswertung in Kooperation mit iServ

einen auf seine Bedürfnisse zugeschnittenen Lernpfad an. Damit können sie Lehrer im Klassenzimmer durch wertvolle Informationen über die spezifischen Stärken und Schwächen der Lernenden unterstützen. Doch dazu müssen diese interaktiven Lerntools Daten über den Lernenden erfassen und speichern.

In Folge dessen kommt es zur Verarbeitung von personenbezogenen Daten, sodass zwischen der Schule und jedem Anbieter dieser Lerntools komplexe Auftragsdatenverarbeitungsverträge entstehen und von jedem Lerner und ggf. seinen Erziehungsberechtigten dem Anbieter ein Einverständnis erklärt werden muss. Dies verkompliziert den Einsatz moderner digitaler Lehrmittel ungemein und behindert gleichermaßen beide Seiten, die Nutzer und die Anbieter. Selbst wenn in den jeweiligen Schul-Gesetzen die Nutzung von digitalen Lernplattformen eingeschlossen wäre, so fehlt darin die Datenweitergabe an Dritte, also die Anbieter der Lerntools. Daher müssen Lösungen gefunden werden, die es den Inhalteanbietern ermöglicht, mit ihren Lerntools und Inhalten Schülern ganz individuell fordern und fördern zu können, ohne dazu vor hochkomplizierten Vertragssituationen mit umfangreichen Zustimmungserfordernissen zu stehen. Die aktuell stattfindenden Initiativen zur Errichtung von Cloud-Lösungen für die schulische Nutzung, wie sie in [Me17] beschrieben werden, bieten die Chance moderne und zukunftsweisende Konzepte zu implementieren.

2 Anonyme und interne Learning Analytics

Im Datenschutz wird zwischen der Anonymität und Pseudonymität eine deutliche Unterscheidung gemacht[6]. Grundsätzlich gilt die Datenschutz-Grundverordnung (DS-GVO) nur für personenbezogene (also nicht-anonyme) Daten, wie in ErwG 26 erläutert wird:

[...] Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.

Wie von Drachsler und Greller in [DG16] erläutert ist eine perfekte Anonymisierung schwierig, selbst wenn entsprechende Checklisten und Frameworks verwendet werden. Gerade zum Zeitpunkt der Erfassung der Daten sind diese fast immer auf eine Person zu beziehen. Allein die beim Konsumieren eines Web-Inhaltes eingesetzten Mechanismen (Cookies, Browser-Fingerprints, IP-Adressen) reichen dafür aus. Zwar kann später dafür gesorgt werden, dass dieser Personenbezug entfernt wird, aber bei einem Einsatz im schulischen Kontext soll der Personenbezug oft explizit beibehalten werden, etwa wenn die Learning-Analytics-Daten Grundlage für Unterstützung des Lehrenden sind. Die bei der Auslieferung anfallenden personenbezogenen Daten können alternativ durch ein Hosting der Inhalte und Tools beim Schul-Cloud-Betreiber geschützt werden. Dadurch

[6] Fokusgruppe Datenschutz des Digital-Gipfels [Fo17]

kann vermieden werden, dass personenbezogene Daten bei den Inhalte- und Tool-Anbietern anfallen. Learning-Analytics-Daten können in diesem Falle direkt innerhalb der Schul-Cloud erfasst und verarbeitet werden. Für Open-Source-Tools und -Inhalte (OER) ist dieser Ansatz durchaus praktikabel. Für kommerzielle Anbieter wie Schulbuchverlage, bei denen die Auslieferungsplattformen Teil des Geschäftsmodells und als solche besonders schützenswert sind, oder auch für innovativere OER-Initiativen, die komplexere Auslieferungsumgebungen benötigen, ist eine solcher Ansatz nicht praktikabel. Demnach wird auch für solche Inhalte eine Lösung nötig, welche im folgenden Kapitel diskutiert wird.

3 Integration von externen Lerntools

Lerntools müssen zur Entfaltung ihres Potenzials (Adaptivität, Benutzerkomfort) den Nutzer wiedererkennen. Um einen Kompromiss zwischen Anonymität und direktem Personenbezug zu schließen, sollte die Nutzerkennung nur in pseudonymisierter Form an die Anbieter der Inhalte gelangen. Dazu wird ein vertrauenswürdiger Mittler zwischen Nutzer und Anbieter nötig. Eine Schul-Cloud kann diese Rolle einnehmen und die Identität des Nutzers schützen. Für Anbieter, die entweder in ihrem Inhalt oder bei der Rückmeldung von Ergebnissen, Nutzernamen verwenden, entstehen dadurch neue Bedürfnisse, die mit der sicheren Rückübersetzung der Pseudonyme zusammenhängen. Pseudonymisierte Learning-Analytics-Ergebnisse müssen wieder dem richtigen Nutzer zugeordnet werden. Wenn ein Lehrer zum Beispiel innerhalb der Lernsoftware einem Schüler eine Aufgabe zuweisen möchte, ist ihm verborgen, welcher Nutzer sich hinter einem Pseudonym verbirgt.

3.1 Authentifizierung und Pseudonymisierung

Beim erstmaligen Abruf des Lerntools wird dem Nutzer das Tool per URL entweder in einem eigenen Fenster oder in einem Iframe angezeigt. In beiden Fällen wird im Browser eine Webseite abgerufen, die in einer anderen Domäne liegt. Deshalb muss sich der Cloud-Nutzer beim Anbieter authentifizieren. Zum einen kann der Nutzer so die personalisierten Inhalte erhalten und zum anderen der Anbieter den Zugriff auf seine Inhalte kontrollieren. In Moment der Authentifizierung entscheidet sich, mit welcher Zeichenfolge der Nutzer referenziert wird. Hierfür eindeutige Zeichenketten wie die E-Mail-Adresse oder die Telefonnummer zu verwenden, würde die Identität des Nutzers offenlegen. Daher wird in diesem Moment eine Pseudoidentität geschaffen. Es wird nach dem UUID-Standard[7] eine zufällige, global eindeutige Zeichenfolge, das *Pseudonym* generiert und in der Schul-Cloud-Domäne mit dem Nutzer verknüpft. Durch das Pseudonym sinkt die Schutzwürdigkeit der Daten auf Anbieterseite, da diese ohne die Zuordnungstabelle nicht mehr unmittelbar auf reale Personen bezogen werden können.

[7] https://tools.ietf.org/html/rfc4122

Das Pseudonym ist angebotsspezifisch. Damit wird erschwert, dass durch den Zusammenschluss von Nutzungsprofilen verschiedener Tools ein umfangreiches Profil eines Nutzers geschaffen wird. Dazu müssten einzelne Nutzer durch eine tiefergehende Analyse in verschiedenen Angeboten identifiziert werden. Es wird durch eine eindeutige Kennung eines Nutzers die ursprüngliche Adaptivität innerhalb des einzelnen Inhalts weiterhin gewährleistet. Im Rahmen der Authentifizierung werden ebenfalls weitere Schnittstellen-Parameter zwischen Schul-Cloud und Anbieter ausgetauscht wie die URL von Endpunkten für xAPI oder Rostering. Zur Authentifizierung können unter anderem LTI und OAuth2 genutzt werden. Bei Nutzung von LTI nach [IMS12] wird der einzelne Nutzer mit seinem Pseudonym durch den user_id-Parameter referenziert. Bei Freigabe der OpenID via OAuth2 wird ebenfalls das Pseudonym statt einer realen Identität verwendet.

3.2 Rostering

Der Begriff *Roster* beschreibt ursprünglich die Auflistung von Mitgliedern eines Sport-Teams. Im Lerntool-Kontext werden darunter Metadaten über die Rollen und Assoziationen der Nutzer verstanden. Beim Rostering wird übertragen, welcher Lehrer für welchen Schüler zuständig ist oder welcher Klasse ein Schüler angehört. [IMS17] beschreibt mit OneRoster 1.1 einen Standard, der zum Austausch von diesen Informationen zwischen dem Studenten-Informationssystem und dem Lerntool dient. Das Tool sollte die Rostering-Informationen dazu nutzen, dass ein Lehrer nur die Analysen zu seinen eigenen Schülern sehen kann. Rostering funktioniert technisch mit Pseudonymen statt Klarnamen auf dieselbe Weise. Problematisch wird es jedoch, wenn die vermeintlichen Namen im externen Tool anzeigt werden. Damit Nutzernamen im Tool verwendbar sind, muss eine De-Pseudonymisierung stattfinden (siehe Abschnitt 3.4).

3.3 xAPI-basierte Learning Analytics und LernCockpit

Die Experience API (xAPI) ist ein Standard zur Erfassung von Lernprozessen, der in [xAPI13] spezifiziert wurde. An die Schnittstelle können Daten von allen Geräten gesendet werden. Beim Auftreten eines Lernereignisses wie „John hat Aufgabe 3 korrekt gelöst" kann ein Statement der Form Subjekt (John) - Verb (lösen) - Objekt (Aufgabe 3) abgespeichert werden. Die Statements sind formal nicht weiter beschränkt. Für die einzelnen Komponenten existieren jedoch Ideen für Schemata. So hat die [XAPI Community] eine kurierte Sammlung von möglichem Vokabular verfasst. Die Statements werden in einem Learning Record Store (LRS) gespeichert, der die xAPI-Spezifikation unterstützt. Dazu eignet sich die Open-Source-Lösung LearningLocker[8], welche von Haus aus Diagramme für die Analyse der Statements anbietet.

Bezüglich des Datenschutzes ist das Abspeichern in einem LRS, der sich in der Schul-Cloud-Domäne befindet, unproblematisch. Beim Einfügen der Daten wird das Pseudo-

[8] https://learninglocker.net

nym zum echten Nutzer und das gesendete Statement dem Anbieter zugeordnet. Außerdem kann noch eine Zuordnung zum Kurs geschehen, in dem der Inhalt eingesetzt wird. Datenschutzrechtlich wird das Auslesen aus dem LRS komplizierter. Es bietet einen Mehrwert, wenn Anbieter ein interdisziplinäres Profil eines Nutzers erhielten. Dazu müssten sie auf mehr Statements zugreifen als die selbst generierten. Dies ist jedoch widersprüchlich zum angebotsspezifischen Pseudonym, weshalb hier ein Kompromiss eingegangen werden muss. In jedem Fall muss für den Nutzer transparent sein, welche Daten ein Anbieter erhält.

Auch allein über den LRS ist eine Tool-Anpassung an den Nutzer möglich. So kann er im Extremfall ganz auf anbieterseitige Speicherung von Nutzungsprofilen verzichten, sofern alle relevanten Nutzungsdaten im LRS gespeichert und nur anhand dieser Daten personalisiert wird. Dies wäre im Sinne der Datensparsamkeit wünschenswert. Konzeptionell enthält der LRS die relevanten Informationen für die Personalisierung.

Das *LernCockpit* ist die Analyse-Oberfläche für Lehrer. Die Statements im LRS können hier ohne Einschränkungen auf bestimmte Anbieter ausgewertet werden. Ohne bildungswissenschaftlichen Hintergrund kann bereits ein Aktivitätenlog einen Mehrwert für den Lehrer darstellen. So kann er anhand der Aktivität abschätzen, welche Schüler langsamer vorankommen und Hilfe benötigen. Bisher problematisch ist die mangelnde Kompatibilität der xAPI-Daten der verschiedenen Anbieter und die mangelnde Verknüpfung mit Kompetenzen. Dazu sind die einzelnen Inhalte oft sehr umfangreich und an komplette Bücher angelehnt, sodass ein Mapping von Kompetenzen oder ähnlichen Meta-Daten aufwendig ist. Dadurch wird die angebotsübergreifende Auswertung zunächst oberflächlich bleiben. Einen wirklichen Mehrwert bietet es, wenn sich Anbieter auf eine Standardisierung der übertragenden Metadaten, bspw. in Bezug auf Kompetenzen einigen. De-Pseudonymisierung von anbieterspezifischen Learning Analytics

Es gibt Anbieter, die dem Lehrer inhaltsspezifische und fortgeschrittene Auswertungen der Lernleistung zur Verfügung stellen. Dies passiert als Teil des Geschäftsmodells innerhalb der Anbieter-Domäne. Aufgrund der Pseudonymisierung sind alle Auswertungen, die sich auf einzelne Nutzer beziehen, für den Lehrer dort aber unbenutzbar. Damit der Lehrer weiter gezielt auf die Stärken und Schwächen einzelner Schüler eingehen kann, muss dieser Bezug wiederhergestellt werden.

Den allgemeinen Workflow für die De-Pseudonymisierung veranschaulicht Abbildung 1. Der Lehrer erhält dort Feedback sowohl vom Lerntool (3.) als auch von der Schul-Cloud (5.). Das Lerntool-Feedback wird über den Zwischenschritt (4.) erst beim Lehrer de-pseudonymisiert. Das Feedback von der Schul-Cloud wird bereits beim Eintreffen vom Lerntool de-pseudonymisiert und im LRS mit Klarnamen gespeichert.

Die Pseudonyme müssen also spätestens bei der Anzeige auf dem Endgerät des Lehrers wieder zurückübersetzt, im Folgenden *de-pseudonymisiert*, werden. Dies darf aufgrund des Datenschutzes nicht in der Domäne des Anbieters geschehen. Damit bleiben lediglich der Server der Schul-Cloud und der Browser des Lehrers als mögliche Stellen. Die erste Variante entspricht einem Proxy. Die Inhalte werden dabei anstatt vom Anbieter aus der Schul-Cloud abgerufen. Diese stellt die Anfrage an den Anbieter und ersetzt in

der Antwort alle Pseudonyme, deren Nutzernamen der aktuell eingeloggte Nutzer abrufen darf. Die Autorisierung ist hier wichtig, damit kein Dritter über diesen Weg alle Pseudonyme abrufen kann. Beispiel: Anstatt den Lehrer auf die URL *anbieter.de/results* zu leiten, ruft er *schul-cloud.org/anbieter/results* auf. Dies sorgt jedoch für eine deutlich erhöhte Netzwerk-Last auf den Servern der Schul-Cloud. Zusätzlich müssen die Inhalte so umgerüstet werden, dass alle dynamisch nachgeladenen Inhalte ebenfalls über die Proxy-URL abgerufen werden. Gerade bei Apps, die auch offline funktionieren sollen, kann die Notwendigkeit des Proxy-Abrufs problematisch sein.

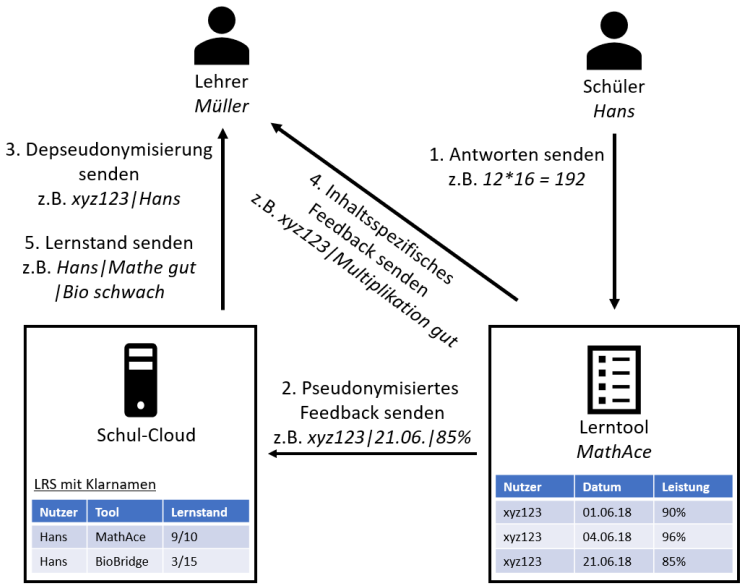

Abb. 1: Ablauf der Feedback-Auslieferung über die Schul-Cloud

3.4 Browser-basierte De-Pseudonymisierung

Um den Nachteilen der Proxy-Lösung zu entgehen, kann die De-Pseudonymisierung auch vom Browser des Endnutzers initiiert werden. Dabei gibt es verschiedene Herangehensweisen:

Skript Bei dieser Variante integriert der Anbieter ein Skript in sein Tool. Über die Web-Messaging-API wird die Liste von autorisierten Pseudonymen an das Frame gesendet, indem das Tool geöffnet wird. Das integrierte Skript empfängt die Liste und ersetzt entweder automatisch alle Pseudonyme oder stellt eine Funktion bereit, die von der Anwendung aufgerufen werden kann. In diesem Fall landen die Klarnamen nicht auf dem Server des Anbieters, jedoch in dessen Domäne. Die Client-Anwendung kann die Klarnamen auslesen und dem Anbieter senden. Der Anbieter muss sich vertraglich verpflichten, dies zu unterlassen.

Iframe Hier wird anstelle des Pseudonyms ein kleines Iframe angezeigt, worin eine spezielle URL der Schul-Cloud abgerufen wird, die das Pseudonym enthält. Da die Iframe-Seite in der Schul-Cloud-Domäne liegt, kann sie die für den eingeloggten Nutzer autorisierten Pseudonyme anzeigen. Aufgrund der same-origin policy kann der Anbieter technisch keine Namen aus dem Iframe lesen [SNM17]. Die same-origin policy kann von technisch versierten Nutzern aufgeschaltet werden. Dann kann der Anbieter aber nur die Klarnamen im Rechtebereich des aktuellen Nutzers auslesen. Datenklau einer Großzahl von nichts-ahnenden Nutzern ist auf diese Weise schwer möglich. Er kann jedoch auch keinen Einfluss auf die Darstellung nehmen, wodurch das Layouting problematisch wird. Eine Lösung ist, ein anbieterspezifisches CSS einzubinden.

SVG Die SVG-Lösung ist ähnlich zur Iframe-Lösung, nur dass SVG-Grafiken problemlos skaliert werden können. Sie sind zudem einfach zu generieren und in ihnen kann grafisch gekennzeichnet werden, dass es sich um einen Inhalt aus der Schul-Cloud handelt (durch ein stempelartiges Symbol).

4 Das datenschutzrechtliche Konstrukt

Datenschutzrechtlich besteht das Konstrukt aus drei Elementen. Das erste Element besteht in der Datenschutzerklärung. Dort ist unter Absatz IV (Weitergabe von Daten an Inhalte-Anbieter) beschrieben, dass und warum beim Einsatz von Drittanbieter-Software Pseudonyme verwendet werden. Außerdem wird auf die Auftragsdatenverarbeitung hingewiesen und die nach DS-GVO bestehenden Rechte für den Nutzer auch bei den Drittanbietern. Darüber hinaus findet sich im *Anhang 2, Verzeichnis aller Empfänger der personenbezogenen Daten* eine Liste von „Inhalte-Anbieter[n], die aufgrund von Kooperationsverträgen pseudonymisierte nutzungsbezogene Daten erhalten". Dort sind alle Anbieter mit Adresse aufgeführt.Drittens gibt es entsprechende vertragliche Regelungen zwischen den einzelnen Anbietern und der Schul-Cloud. Erwähnenswert ist noch, dass je nach Alter eine Einverständniserklärung der Erziehungsberechtigten, den Erziehungsberechtigten und dem Schüler oder nur dem Schüler abgegeben werden muss.

4.1 Löschung von Daten

Je nach Bundesland kann es gesetzliche Löschfristen geben. Darüber hinaus sieht auch die DS-GVO in Artikel 17 vor, dass ein Nutzer jederzeit die Löschung seiner personenbezogenen Daten einfordern kann. Dies erfordert, dass auch die bei den Inhalteanbietern abgelegten mit dem Pseudonym verknüpften Daten gelöscht werden müssen. Dafür müssen alle Anbieter ein (vorzugsweise) elektronisch automatisierten Workflow implementieren, der die Löschung durchführt. Einfacher ist es hingegen, lediglich das angebotsspezifische Pseudonym aus der Mapping-Tabelle zu entfernen. Dies muss nur in der Schul-Cloud erfolgen, nicht aber auf Anbieterseite. Dafür muss jedoch ausgeschlossen sein, dass die xAPI-Statements personenbezogene Daten in den Verb- und Objektinformationen enthalten. Dadurch sind die erfassten Daten auf Anbieterseite nicht länger de-

pseudonymisierbar und fallen dann als anonymisierte Daten nicht mehr unter die DS-GVO.

5 Zusammenfassung und Ausblick

Die Vermeidung von personenbezogenen Daten ist insbesondere für anspruchsvolle interaktive Inhalte nicht praktikabel. Eine Wiedererkennung von Nutzern, wie sie auch für personenbezogene Learning Analytics Funktionen notwendig ist, lässt sich mit angebotsspezifischen Pseudonymen realisieren. Rechtlich gesehen, handelt es sich immer noch um personenbezogene Daten, jedoch sind sie anbieterseitig nicht mehr ohne weiteres auf reale Identitäten zu beziehen. Deshalb sinkt das Schutzniveau der Daten, sodass eine indirekte Einverständniserklärung, welche als Teil der Einverständniserklärung mit der einbettenden Plattform abgeschlossen wird, ausreichend sein kann. Während einfache eventbasierte Learning-Analytics-Funktionen angebotsübergreifend auf Basis pseudonymisierter xAPI-Events erfolgen kann, erfordern fortgeschrittene angebotsspezifische Learning Analytics eine Auswertung auf Seite des Anbieters. Diese kann unter Verwendung der Pseudonyme erfolgen, wobei eine De-pseudonymisierung zur Laufzeit im Browser (bspw. des Lehrers) erfolgt und somit bei entsprechender Implementierung (Iframe oder Proxy) ein Zugriff auf die de-pseudonymiserten Daten durch den Anbieter ausgeschlossen werden kann. Problematisch bleiben vom Nutzer erzeugte personenbezogene Daten. Erlaubt bspw. ein Lerninhalt das Anlegen von Kommentaren oder Notizen, kann dies dazu führen, dass diese Daten auch in den dazugehörigen xAPI-Events auftauchen. Sofern nicht schon die Erfassung unterbunden werden kann, sollten diese Daten zumindest in den Learning Analytics Daten gefiltert werden.

Parallel zu der Einführung der hier bereits im Prototyp implementieren Ansätze gilt es zudem solche Ansätze weiter zu verfolgen, personenbezogene Inhalte auf Seite des Anbieters vermeiden. So ist denkbar, dass Anbieter Algorithmen oder Laufzeitumgebungen anbieten, die an den in der Schul-Cloud liegenden Learning Record Store angebunden werden. Hierzu bedarf es allerdings eines Paradigmenwechsels bei den Anbietern. Auch Verschlüsselung für vom Nutzer in den Lernlösungen erfasste Daten kann in diesem Zuge angegangen werden. Gemeinsam mit den Inhalteanbietern sollte eine Standardisierung und Erweiterung der zu übermittelnden xAPI-Daten angestrebt werden, wobei bis dato Schulbuchverlage hierzulande nicht durch Kollaboration hervorstechen. Noch sind die vorgestellten Konzepte nicht vollständig in Produktion ausgerollt, auch da die Abstimmung mit den Facharbeitskreisen der Landesdatenschützer und den zuständigen Landesdatenschützern noch nicht abgeschlossen ist. Es wird sich daher zeigen, ob ggf. noch Anpassungen vorzunehmen sind, bevor die geschilderten Lösungen zum flächendeckenden Einsatz kommen können.

6 Literaturverzeichnis

[DG16] Drachsler, H.; Greller, W.: Privacy and Analytics: It's a DELICATE. Issue a Checklist for Trusted Learning Analytics. In: Proceedings of the Sixth International Conference on Learning Analytics & Knowledge. LAK '16, ACM, Edinburgh, United Kingdom, S. 89–98, 2016, ISBN: 978-1-4503-4190-5, URL: http://doi.acm.org/10.1145/2883851.2883893.

[Fo17] Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2017, 2017, URL: https://www.gdd.de/downloads/whitepaper-zur-pseudonymisierung, Stand: 01.06. 2018.

[IMS12] IMS Global Learning Consortium, 2012, URL: https://www.imsglobal.org/specs/ltiv1p1/implementation-guide, Stand: 19.06.2018.

[IMS17] IMS Global Learning Consortium, 2017, URL: https://www.imsglobal.org/oneroster-v11-final-csv-tables, Stand: 20. 06. 2018.

[Me17] Meinel, C.; Renz, J.; Grella, C.; Karn, N.; Hagedorn, C.: Die Cloud für Schulen in Deutschland: Konzept und Pilotierung der Schul-Cloud. Universitätsverlag Potsdam, 2017.

[SNM17] Schwenk, J.; Niemietz, M.; Mainka, C.: Same-Origin Policy: Evaluation in Modern Browsers. In: 26th USENIX Security Symposium (USENIX Security 17). USENIX Association, Vancouver, BC, S. 713–727, 2017, ISBN: 978-1-931971-40-9, URL: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/schwenk.

[XAPI Community] XAPI Community, URL: http://xapi.vocab.pub, Stand: 20.06.2018.

[xAPI13] Experience API Working Group, 2013, URL: https://github.com/adlnet/xAPI-Spec/blob/master/xAPI-About.md, Stand: 20.06.2018.