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

# Facing the General Data Privacy Regulation: What data is being collected about me and how can I get access?

**Abstract:** With the General Data Privacy Regulation (GDPR) coming into force, users get new and advanced privileges in dealing with their personal data. Especially in virtual learning environments, where manifold data is aggregated and processed, the transparency about which data is gathered, and saved is lost quickly. When the number of applications increases, it gets even more confusing for the users to keep track of their data. In addition, at worst case it entails several manual steps by the service providers to exercise the data subject rights. This article presents a self-information dashboard, by which the users achieve an overview about their personal data. The implementation of the use cases is based on the GDPR fundamental data subject rights and is automated as far possible. Therefore, users can exercise most of their rights without manual intervention of service providers. The article closes with a discussion about current limitations and future challenges.

# Der EU-Datenschutz-Grundverordnung begegnen: Welche Daten sind über mich erhoben und wie komme ich da ran?

Alexander Kiy[1], Kristin Sass und Ulrike Lucke

**Abstract:** In Folge der Datenschutzgrundverordnung (DSGVO) erhalten die Nutzenden neue und erweiterte Rechte im Umgang mit ihren Daten. In Lernumgebungen, wo verschiedenste personenbezogene Daten angebundener Anwendungen aggregiert und für die Nutzenden aufbereitet werden, geht die Transparenz schnell verloren, welche Daten wo und wie erhoben und gespeichert werden. Steigt die Anzahl an Anwendungen wird es für einen Nutzenden schnell unübersichtlich, und die Wahrnehmung der Rechte durch die Betroffenen ist mit erheblichen manuellen Aufwänden seitens der Systembetreuer verbunden. In diesem Beitrag wird eine Lösung in Form eines Self Information Dashboard vorgestellt, mit der die Nutzenden Auskunft über ihre eigenen Daten erhalten können. Die Umsetzung der konzipierten Anwendungsfälle orientiert sich an der DSGVO und erfolgt automatisiert, so dass manuelle Arbeitsschritte für die Systembetreuer entfallen und die Nutzenden ihre Rechte weitestgehend eigenständig wahrnehmen können. Der Beitrag schließt mit einer kritischen Auseinandersetzung mit aktuellen Limitationen und zukünftigen Herausforderungen.

**Keywords:** GDPR, DSGVO, PLE, Self Service, Learning Analytics

[1] Universität Potsdam, Institut für Informatik & Computational Science, August-Bebel-Str. 89, 14482 Potsdam, vorname.nachname@uni-potsdam.de

# 1 Einleitung

Mit der Einführung der Europäischen Datenschutzgrundverordnung (EU-DSGVO) am 25. Mai 2016 und deren Inkrafttreten am 25. Mai 2018 müssen alle Diensteanbieter – d. h. auch Forschungseinrichtungen, Rechenzentren und Projekte – geeignete technische und organisatorische Maßnahmen beim Umgang mit personenbezogenen Daten ergreifen, die es nach Artikel 24 DSGVO[2] zu erfüllen gilt. Auch wenn ein Großteil der dort formulierten Regularien im Vergleich zum bisherigen deutschen Datenschutzgesetz nicht neu sind, stellt die erstmalige Erwähnung der sogenannten „Rechte der Betroffenen" (Art. 12 – Art. 21 DSGVO) eine Neuerung dar. Hierzu gehören u. a. das Recht auf Auskunft über die Nutzung der eigenen Daten (Art. 15), das Recht auf Widerspruch zur Nutzung der Daten (Art. 21) und das Recht auf Löschung (Art. 17) sowie das Recht auf Aushändigung der Daten in einem strukturierten, gängigen und maschinenlesbaren Format (Art. 20).

Die Sicherstellung der vorhandenen Rechte – unter Abwägung der Verhältnismäßigkeit (vgl. Art. 32) und der noch unklaren Ausdifferenzierung von Einzelfällen und Verhältnismäßigkeiten für den Betrieb (vgl. Löschpflicht in Datensicherungen) [DR17] – stellt Akteure, die mit personenbezogenen Daten umgehen, vor neue Herausforderungen. Die organisatorische und technische Implementierung der Rechte umfasst dabei im schlimmsten Fall eine Vielzahl manueller Handgriffe seitens der Systembetreibenden, der Verfahrensverantwortlichen und fachlich involvierter Personen. Mit einer steigenden Anzahl an Softwaresystemen und der Implementierung wechselseitiger systemübergreifender Prozesse, unter Nutzung personenbezogener Daten, wird dieser Sachverhalt noch verschärft. Insbesondere im Bereich von Virtuellen Umgebungen, egal ob nun für Forschung, Lehre oder Verwaltung genutzt, wird das Problem der Datenaggregation über unterschiedliche Quellsysteme immanent. Mit einer zunehmenden Kopplung von Systemen und der Vereinigung in einem Portal treten die Quellsysteme und Prozesse nicht mehr als eigenständige Systeme auf. Die Aggregation und Orchestrierung personenbezogener Daten aus unterschiedlichen Systemen [Ki18] und die Vereinigung unter einer einheitlichen Oberfläche wie bspw. in Form einer Persönlichen Lernumgebung (PLE) stellen zwar für den Nutzenden einen Mehrwert seitens der Bedienung aber nicht notwendigerweise hinsichtlich des Datenschutzes dar. Den Nutzenden, ist häufig nicht mehr bewusst aus welchen Systemen Daten verarbeitet werden (vgl. Abschnitt 2). Auch im Bereich von Learning Analytics ergeben sich Herausforderungen im Umgang mit der DSGVO, beispielsweise bezüglich einer datenschutzkonformen Implementierung oder der Verfügbarkeit von Daten [HC16; Za17]. Die Learning Analytics Community hat die Notwendigkeit eines proaktiven Umgangs mit Daten und der Einbeziehung der relevanten Akteure nicht erst seit der DSGVO erkannt [PS15; DG16]. So gilt es dem Nutzenden u. a. transparent darzustellen welche Daten gesammelt werden, zu welchem Zweck und mit wem diese geteilt werden (auch unter welchen Bedingungen) [PS15]. Mit dem Ziel die Transparenz für die Nutzenden zu erhöhen und Auskunft über die verschiedenen Prozesse und Systeme sowie ihre personenbezogenen Daten zu ermöglichen, wird die Einführung einer Self-

[2] http://data.europa.eu/eli/reg/2016/679/oj

Service Komponente – nutzbar auch als Teil einer Persönlichen Lernumgebung – vorgeschlagen, welche die grundlegenden Rechte der Nutzenden abbildet. Hierzu wird zunächst die DSGVO analysiert. Daraus werden Anwendungsfälle abgeleitet. Darauf aufbauend wird ein modularer Aufbau des Self Information Dashboard vorgestellt, welches eine Anbindung beliebiger anderer Datenquellen (Service Provider / Dienste) ermöglicht. Im Anschluss wird die auf Webservices / APIs basierende Implementierung vorgestellt, bevor die aktuellen Limitierungen und Verbesserungen im Hinblick auf Learning Analytics und DSGVO diskutiert werden.

## 2 Rechte der Betroffenen seitens der Datenschutzgrundverordnung

Der zu Grunde liegende Anwendungsbereich ergibt sich aus der ganz oder teilweise automatisierten sowie nicht-automatisierten Verarbeitung und Speicherung personenbezogener Daten in Dateisystemen gemäß Art. 2 DSGVO. Hochschulen als Landeseinrichtung unterliegen dem jeweiligen Landesdatenschutzgesetz. Im vorliegenden Fall bedeutet das, dass das Brandenburgischen Datenschutzgesetz (BrbgDSG[3]) beziehungsweise das Gesetz zur Anpassung des Allgemeinem Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/80[4] anzuwenden sind. Die konkrete Ausprägung ist für jedes Bundesland individuell zu prüfen und kann Ergänzungen oder weitere Einschränkungen beinhalten.

Bei personenbezogenen Daten handelt es sich nach Art. 4 I DSGVO zunächst um „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.“

Unter der Verarbeitung versteht man nach Art. 4 II DSGVO „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.“

Dabei stehen den Betroffenen die in Artikel 14 bis Artikel 21 formulierten Rechte zu.

[3] https://bravors.brandenburg.de/gesetze/bbgdsg
[4] https://www.landesrecht.brandenburg.de/dislservice/public/gvbldetail.jsp?id=7633

**Recht auf Auskunft:** Betroffene sollen nach Art. 15 DSGVO die Möglichkeit haben, problemlos und in einem angemessenen Abstand eine Auskunft zu ihren erhobenen personenbezogenen Daten zu erhalten. Diese Auskunft muss auch die Folgen der Verarbeitung aufzeigen, sowie auf welche Art und Weise die Daten verarbeitet werden. Weiterhin muss den betroffenen Personen ein Fernzugang mit direktem Zugang zu ihren personenbezogenen Daten ermöglicht werden.

**Recht auf Löschung (Recht auf „Vergessenwerden"):** Der Artikel 17 der EU-Datenschutz-Grundverordnung behandelt das Löschrecht der Betroffenen. Das Recht auf Löschung kann dabei nicht nur durch einen formlosen Antrag geltend gemacht werden [Dr17]. Die Löschung kann begründet sein bspw. in Folge des Erlöschens des Zwecks der Verarbeitung oder durch den Widerruf der Verarbeitung der personenbezogenen Daten durch den Betroffenen. Automatisierte Löschroutinen bilden dabei bisher die absolute Ausnahme [Dr17].

**Recht auf Datenübertragbarkeit:** In Artikel 20 der DSGVO wird Bezug auf die Übertragung personenbezogener Daten genommen. Gemeint sind im diesem Fall Daten, deren Nutzen für einen vergleichbaren Dienst geeignet sind. Den Betroffenen muss auch die Möglichkeit zur Verfügung gestellt werden ihre eigenen Daten selbstständig herunterzuladen [Be18]. Die Daten müssen dabei in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format zur Verfügung gestellt werden. Die verantwortlichen Stellen sind verpflichtet interoperable Formate zu entwickeln, um die Datenübertragung zu erleichtern [Di18]. Daten, die aus den bereitgestellten Daten generiert wurden oder aus öffentlichen Quellen bezogen wurden, sind von dieser Pflicht der Bereitstellung ausgenommen. Das Auskunftsrecht über diese Daten besteht aber weiterhin, und auf das Recht darauf muss hingewiesen werden [Be18].

Ergänzend werden in der DSGVO die folgenden Rechte erwähnt, für die im Rahmen dieser Arbeit zunächst keine Lösung entwickelt werden. Hierzu gehören die Informationspflicht (Art. 14 DSGVO), das Recht auf Berichtigung (Art. 16 DSGVO), das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO), die Mitteilungspflicht (Art. 19 DSGVO) und das Widerspruchsrecht (Art. 21 DSGVO). Der Informationspflicht kann dabei u. a. in Form einer aktuellen Allgemeinen Geschäftsbedingung (AGB) nachgekommen werden. Der Anspruch bezüglich des Rechts auf Widerspruch und auf Einschränkung der Verarbeitung ist meist im Einzelfall zu prüfen, so dass eine automatisierte Lösung nicht sinnvoll erscheint.

## 3 Konzeption eines Self Information Dashboards

Die prototypische Implementierung einer Oberfläche zur Wahrnehmung der eigenen Rechte im Rahmen der DSGVO umfasst somit eine Reduktion auf das Recht auf Auskunft (vgl. Anwendungsfall „Daten anzeigen"), das Recht auf Datenübertragbarkeit (vgl. „Daten herunterladen") und das Recht auf Löschung (vgl. „Daten löschen"), welche in Form der

entsprechenden Anwendungsfälle umgesetzt werden. Das Recht auf Auskunft umfasst dabei die Zurverfügungstellung genauerer Informationen zur Verarbeitung oder beispielsweise zu den Empfängern der Daten. Diese und andere Informationen können auch dem Verfahrensverzeichnis entnommen werden. Es würde somit genügen dem Nutzenden Zugang zum Verfahrensverzeichnis des jeweiligen Dienstes zu gewähren, sowie einen Fernzugang zu den gespeicherten personenbezogenen Daten zu ermöglichen. Der Anwendungsfall „Daten herunterladen“ soll so implementiert werden, dass die vorhandenen Daten soweit möglich in einem gängigen Datenformat des Dienstes exportierbar sind. Für den Anwendungsfall „Daten löschen“ gilt nach wie vor, dass entweder eine automatisierte beziehungsweise eine vollständige und rückstandslose Löschung nur im Ausnahmefall für einen Großteil der Anwendungen implementiert ist. Doch bevor die Anwendungsfälle gemäß DSGVO für die einzelnen Dienste und Prozesse angeboten werden können, gilt es für den Betroffenen einen Überblick darüber zu erhalten, in welchen Systemen im Rahmen des Hochschullebens jemals eine Anmeldung erfolgte und somit ein Account mit personenbezogenen Daten erstellt und im Rahmen einer möglichen Nutzung zugehörige Daten angefallen sind.

Doch wo sind überhaupt Daten über mich gespeichert? Um diese Frage zu beantworten gilt es im schlimmsten Fall in den Datenbanken aller Dienste nach dem entsprechenden Nutzenden zu suchen, um eine Aussage darüber treffen zu können in welchen Diensten ein Nutzender im Laufe seines Account-Lifecycles aktiv wurde. Statt individuelle Datenbank-Queries für alle Dienste schreiben zu müssen, wäre es von Vorteil wenn bereits nutzbare Webservices oder APIs nutzbar wären. Im Idealfall sind die Dienste und Prozesse bereits an eine Authentifizierungs- und Autorisierungs-Infrastruktur des Deutschen Forschungsnetzes (DFN-AAI) angeschlossen. Unter der Nutzung des Shibboleth Identity Providers mit der bereits eingebauten datenschutzkonformen uApprove[5]-Erweiterung wird in einer zugehörigen Datenbank abgelegt, welche personenbezogenen Daten an welchen Dienst übergeben wurden. Somit entfällt die Implementierung gegen eine Vielzahl an Datenbanken unter Nutzung der Datenbank des Shibboleth Identity Providers.

[5] https://www.switch.ch/aai/support/tools/uapprove/

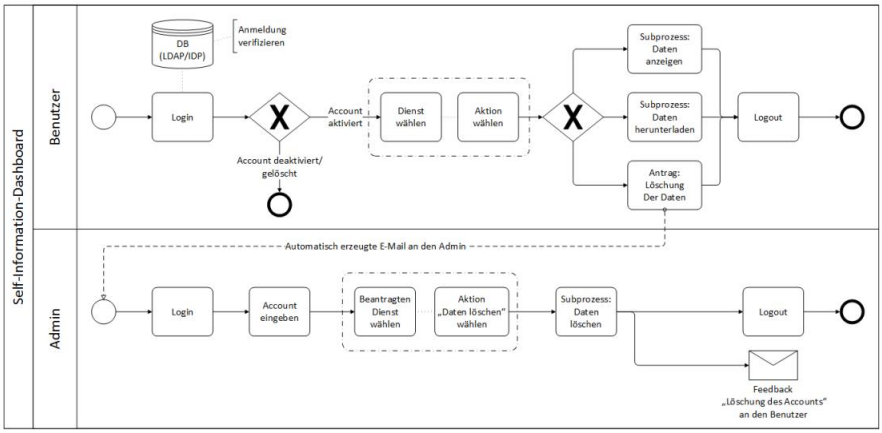


Abb 1. – Funktionsumfang des Self Information Dashboard mit den Anwendungsfällen „Daten anzeigen", „Daten herunterladen" und „Daten löschen"

Das vorangegangene Schaubild (Abb. 1) fasst die drei Anwendungsfälle des Self Information Dashboard für einen Betroffenen und einen Administrator exemplarisch zusammen. Sobald der Account des Betroffenen deaktiviert wurde (in der Regel 180 Tage nach Ausscheiden aus der Hochschule), ist es ihm nicht mehr möglich sich im Portal anzumelden. Die Einsicht, ein Datenexport und das Löschen der Daten kann dann nur noch durch einen Administrator durchgeführt werden. Das Konzept sieht es vor, dass die Betroffenen für die Löschung der Daten aus einem Dienst bisher lediglich einen Antrag stellen können. Nach vorheriger Einzelfallprüfung unter Berücksichtigung der einzubeziehenden Personen (Datenschutzbeauftragter, Verfahrensverantwortlicher, Kommissionen etc.) kann ein Administrator den Löschvorgang anschließend initiieren.

# 4 Implementierung des Self Information Dashboards

## 4.1 Modulare Architektur zur Erweiterung von Diensten

Für die prototypische Implementierung wurden drei E-Learning-Werkzeuge ausgewählt, die bereits von einer Vielzahl an Nutzenden verwendet werden und somit bei der Wahrnehmung der jeweiligen Rechte durch die Betroffenen einen maximalen Mehrwert generieren würden. Hierzu gehört die Lernplattform Moodle[6], der Speicherdienst owncloud respektive nextcloud[7] und der kollaborative Editor Etherpad Lite[8]. In jedem dieser

[6] https://moodle.de/
[7] https://nextcloud.com/
[8] http://etherpad.org/

Dienste werden unterschiedlich viele sowie mehr oder weniger sensible personenbezogene Daten vorgehalten. Für Moodle sind das u. a. Kursmaterial, eigene Dateien, Foren- und Diskussionsbeiträge, versendete Mitteilungen, besuchte Kurse oder Bewertungen von Aufgaben oder Teilleistungen. Beim Speicherdienst nextcloud geht es vornehmlich um die persönlichen Dateien und Freigabe- sowie Teilinformationen und bei Etherpad Lite um die Autorenschaft und den Inhalt kollaborativer Pads. Für einen modularen Aufbau des Dashboards wurden die einzelnen angebundenen Dienste als Provider umgesetzt, die jeweils als Interface drei Methoden (show, download und delete) für die jeweiligen Anwendungsfälle implementieren. Soweit vorhanden wurden für die Implementierung Webservices / APIs der Dienste genutzt, um robuster gegenüber Versionssprüngen zu sein. Für die Erweiterung des Self Information Dashboards um weitere Provider sind lediglich die drei genannten Methoden zu implementieren. Der Prototyp wurde unter Verwendung des PHP-basierten Mikro-Frameworks SLIM[9] implementiert. Die Webservices der Provider werden dabei mit einfachen cURL-Anfragen angesprochen. Die Nutzendenansicht des resultierenden Prototyps ist in Abb. 2 ersichtlich. Für die hinterlegten Provider wird die Existenz eines Accounts überprüft, und anschließend werden Funktionen für die Realisierung der drei Anwendungsfälle angeboten. Für den Administrator besteht zudem die Funktion nach Nutzenden zu suchen und für diese nachträglich – sofern der Account bereits deaktiviert wurde – die Betroffenenrechte in Anspruch zu nehmen.

### 4.2 Moodle-Provider

Die umfangreichste Implementierung weist Moodle auf, da hier zum einen die rückstandlose Löschung von Haus aus nicht vorhanden ist und sich die DSGVO-konforme Anpassung der Implementierung zur Zeit der Umsetzung noch auf dem Weg befand. Für den Anwendungsfall „Daten anzeigen“ existieren bereits eine Vielzahl an Webservices[10], die den Zugriff auf die unterschiedlichen personenbezogenen Daten des Betroffenen ermöglichen und bereits zum Ausdruck bringen, dass viele Daten über die Nutzungsdauer erhoben werden. Für einen ganzheitlichen Auszug müssten alle Webservice-Requests kaskadierend hintereinandergeschaltet werden.

[9] https://www.slimframework.com/
[10] https://docs.moodle.org/dev/Web_service_API_functions

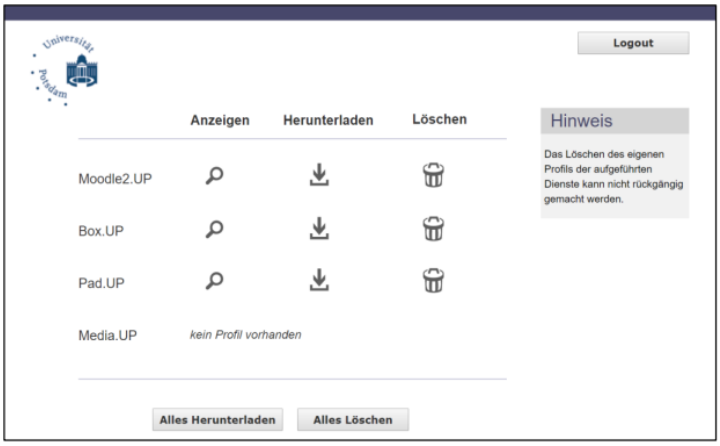


Abb. 2 – Benutzeroberfläche des Self Information Dashboard aus Sicht des Betroffenen mit den drei Anwendungsfällen für drei exemplarische Dienste der Universität Potsdam

Für den Anwendungsfall „Daten herunterladen“ existiert bisher kein Webservice. Daher wurde auf das Plugin *block_material_download*[11] zum Herunterladen aller Materialien in einem eingeschriebenen Kurs und das Plugin *block_my_external_privatefiles*[12] zum Herunterladen der persönlichen Dateien genutzt. Da die Plugins keine Webservices anbieten, wurden diese um Webservicefunktionen erweitert. Dies ermöglicht es auch über alle eingeschriebenen Kurse zu iterieren und ein gesamtes ZIP-Archiv zu erstellen. Zur Umsetzung des Anwendungsfalles „Daten löschen“ hätte zwar der vorhandene Webservice *core_user_delete_users* genutzt werden können, der jedoch nur den Account deaktiviert und dabei den Nutzernamen wie folgt ersetzt:

```
username=E-Mail-Adresse.10-stellige Ziffernfolge
```

Dies hätte weder zu einer Löschung noch zu einer Anonymisierung bzw. Pseudonymisierung geführt. In Folge dessen musste ebenfalls eine Erweiterung zur Umsetzung herangezogen werden. Mit Hilfe des Plugins *local_eledia_makeanonymous*[13] kann zumindest eine Pseudonymisierung des Accounts erreicht werden.

### 4.3 ownCloud-Provider

Zu den hinterlegten Daten in ownCloud gehören neben den Profilinformationen, vorhandene Gruppen, geteilte Ordner und Dateien (sogenannte Shares). Die Implementierung des Anwendungsfalls „Daten anzeigen“ kann unter zu Hilfenahme der *User-Provisioning*

[11] https://github.com/TUM-MZ/moodle-block_material-download
[12] https://github.com/cperves/moodle-block-my_external_privatefiles
[13] https://github.com/eledia/local_eledia_makeanonymous

*API*[14] und der OCS Share API[15] erfolgen. Für das „Daten herunterladen“ existiert keine automatisierte Lösung. Zwar können mit Hilfe des Desktop-Clients bzw. einem manuellen Download alle Daten bezogen werden, doch für ein Angebot über ein Webinterface bedarf es einer anderen Lösung. Hierfür bietet sich die Erweiterung des Plugins *oc_files_mv*[16] an, welches alle Dateien in ein ZIP verpackt und zum Herunterladen anbietet. Das Löschen erfolgt über die *User-Provisioning API*.

### 4.4 Etherpad-Provider

Für die Anwendungsfälle „Daten anzeigen“ und „Daten herunterladen“ existieren entsprechende Webservices, die über die Etherpad Lite API zugreifbar sind. Jeder Autor ist dabei über die *AuthorID* einer Menge an Pads, mit *padID* gekennzeichnet, zugeordnet. Für das Löschen sieht der Sachverhalt erneut komplizierter aus. Eine vollständige Löschung des Nutzers ist nicht möglich, da jeder Textbeitrag eines Autors mit ihm verknüpft ist und somit aus allen Pads entfernt werden müsste. Es scheint somit lediglich praktikabel das Auftauchen des Accountnamens in Bezug zur *AuthorID* zu anonymisieren. Hierfür wurde bis zu einer Implementierung einer geeigneten API eine SQL-Query für die Datenbank von Etherpad Lite geschrieben.

## 5 Diskussion & Ausblick

Nach wie vor sind viele Applikationen nicht datenschutzkonform implementiert, so dass eine reibungslose Umsetzung der Rechte der Betroffenen gemäß der DSGVO nur schwer bzw. mit erheblichen Mehraufwand zu realisieren sind. Das vorgestellte Self Information Dashboard stellt hingegen eine Möglichkeit dar, unter Nutzung von APIs die grundlegenden Rechte der Betroffenen umzusetzen und somit aus Sicht für der Betreibenden auf ökonomische Art und Weise Teile der DSGVO sicherzustellen. Als herausfordernd stellt sich dabei die unterschiedliche Implementierung der APIs heraus (zum Beispiel uneinheitliche Authentifizierung, Funktionsumfang, Datenformat etc.). In der aktuellen Implementierung fehlen für den Anwendungsfall „Daten anzeigen“ noch die Auflistung der Form der Daten, des Speicherorts, des Verwendungszwecks und des Empfängers. Hier bietet sich eine Verknüpfung bzw. Nachnutzung der Informationen des Verfahrensverzeichnisses an. Zur Vereinfachung der Datenpflege erscheint das langfristige Anlegen eines Informationsbestandsregisters (engl. Information Asset Register) als sinnvoll. Diese Informationen könnten in das Self Information Dashboard eingebunden werden.

Noch unklar ist wie mit dem Sachverhalt umgegangen wird, wenn ein Betroffener bspw. seine Daten löschen möchte; die Nutzung des Dienstes jedoch eine essentielle Voraus-

[14] https://docs.nextcloud.com/server/13/admin_manual/configuration_user/user_provisioning_api.html
[15] https://docs.nextcloud.com/server/13/developer_manual/core/ocs-share-api.html
[16] https://github.com/eotryx/oc_files_mv

setzung für die Nutzung weiterführender Funktionen innerhalb einer Persönlichen Lernumgebung darstellt. Zur langfristigen Nutzung personenbezogener Daten bspw. im Kontext von Learning Analytics bietet sich an Stelle des konsequenten Löschens vielmehr eine Pseudonymisierung der Daten an, so dass die Datenbestände für Algorithmen zur Generierung von Empfehlungen, Anpassungen oder nachträglichen statistischen Erhebungen noch zur Verfügung stehen. Hier gilt es noch einmal grundlegend über das Verhältnis von Datenschutz und der DSGVO nachzudenken und ggf. im Design von Learning Analytics Frameworks und integrierter Umgebungen zu berücksichtigen [Za17]. Die vorgestellte Lösung könnte so um „partial self-management"-Funktionen erweitert werden, die es erlauben global Datenschutzeinstellungen zu setzen, die dann für alle Systeme gelten [PS15]. Auch wenn die DSGVO die Verarbeitung personenbezogener Daten für im öffentlich Interesse liegende Archivzwecke oder wissenschaftliche und historische Forschungszwecke privilegiert, soll es dem Betroffenen prinzipiell ermöglicht werden eine Einwilligung für die einzelnen Forschungsprojekte zu geben (vgl. Erwägungsgründe (33) [Di18]). Hier gilt es tragfähige Lösungen für Hochschulen zu entwickeln, die auch vom Einzelvorhaben abstrahieren um so eine datenschutzkonforme Nutzung von Daten zu ermöglichen.

Das Inkrafttreten der DSGVO stellt einen Anlass dar noch einmal grundlegend über den bisherigen Umgang mit Nutzendendaten insbesondere der Deprovisionierung von Nutzendenaccounts und einer datenschutzkonformen Implementierung von Applikationen nachzudenken. Besondere Bedeutung wird in Zukunft dem Entwurfsparadigma *Privacy by Design* [GTD11] zukommen, welches es bei der Implementierung Persönlicher Lernumgebungen zu berücksichtigen gilt.

Mit der Erweiterung von uApprove im Rahmen der DFN-AAI ist ein erster Schritt getan die Transparenz der Übertragung personenbezogener Daten deutlich zu erhöhen. Aktuelle Arbeiten in Richtung der *Consent-Informed Attribute Release*-Erweiterung lassen vergleichbare Arbeiten erahnen. Nach wie vor stellt die Kopplung der implementierten Prozesse und des Identity Managements eine Herausforderung dar. Nach Löschung eines Accounts müssten im Bestfall soweit wie möglich vollautomatisiert die nachgelagerten Lösch-/Pseudonymisierungs-Routinen, die Rahmen des Self Information Dashboards implementiert wurden, angestoßen werden (natürlich unter Berücksichtigung der geltenden Verfahren, Aufbewahrungsfirsten uvm.). Es ist auch denkbar, dass wie im Rahmen dieser Arbeit skizzierten Informationen, sich eines Tages in einem Self-Service-Portal der Hochschulen oder in einem Learning Analytics Dashboard wiederfinden werden, in dem die Nutzenden bestimmen können in welchem Umfang die erhobenen Daten zur weiteren Nutzung – auch nach dem Ausscheiden aus der Hochschule – für weitere Analysen und Erhebungen zur Verfügung stehen können.

Literaturverzeichnis

[Be16] Becker, R.: Art. 20 – EU-DSGVO – Recht auf Datenübertragbarkeit. Online unter: https://www.datenschutz-grundverordnung.eu/grundverordnung/art-20-ds-gvo/

[DG16] Drachsler, H.; Greller, W.: Privacy and analytics: it‘s a DELICATE issue a checklist for trusted learning analytics. In: Proc. of the 6th Int. Conf. On Learning Analytics & Knowledge (LAK 16), S. 89-98, 2016, doi: 10.1145/2883851.2883893.

[Di18] Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: Datenschutz-Grundverordnung. Info 6. 5 Auflage, Bonn, 2018.

[Dr17] Dralle, T. M.: Recht auf Löschung: Der Radiergummi der DS-GVO. In: BvD-News Ausgabe 3/2017. S. 46-49.

[GTD11] Gürses, F. S.; Troncoso, C.; Díaz, C.: Engineering Privacy by Design. In: Computers, Privacy & Data Protection, 2011.

[HC16] Hoel, T.; Chen, W.: Implications of the European Data Protection Regulations for Learning Analytics Design. In: The International Workshop on Learning Analytics and Educational Data Mining (LAEDM 2016) in conjunction with the International Conference on Collaboration Technologies (CollabTech 2016), Kanazawa, Japan - September 14-16, 2016.

[Ki18] Kiy, A: Digitale Medien & Hochschul-Cloud: Eine vielversprechende Verbindung. e-learning & education (eleed), Iss. 12. (urn:nbn:de:0009-5-46594), 2018.

[PS15] Prinsloo, P.; Slade, S.: Student privacy self-management: implications for learning analytics. In: Proc. of the 5th Int. Conf. on Learning Analytics and Knowledge (LAK), S 83-92, 2015, doi: 10.1145/2723576.2723585.

[Za17] Zarsky, T.: Incompatible: The GDPR in the Age of Big Data. Seton Hall Law Review, Vol. 47, No. 4(2), 2017. Online unter: https://ssrn.com/abstract=3022646