Hochschule Karlsruhe
Technik und Wirtschaft
UNIVERSITY OF APPLIED SCIENCES

Seminararbeit

Technologiegestütztes Lernen

Datenschutz und Learning Analytics

Authors:
Niklas Kreutzarek
Moritz Ulte
Claudio Busse
Betreuer:
Dipl.-Inf. Alexander Streicher
Dipl.-Inf. Dipl.-Ing.-Päd. Martin Mandausch

28. Juni 2019

Inhaltsverzeichnis

1 Inhalt

Für die automatische Analyse des Lernfortschritts eines Nutzers werden Verfahren aus dem Bereich Learning-Analytics eingesetzt, also die Analyse von Daten wie Nutzerinteraktionen, Lernprofilen, usw. Die Datenerfassung erfolgt dabei zielgerichtet, um beispielsweise die Lernumgebung automatisch an die Bedürfnisse des Nutzers zu adaptieren. Fraglich ist, inwieweit die automatische Datenerfassung mit geltenden Datenschutzbestimmungen konform gehalten werden können. Sind für eine Adaption personenbezogene Daten notwendig? Wie können diese automatisch anonymisiert werden? Was sind technische Lösungen dafür? Wie ist der aktuelle Stand der Forschung und Technik bei der anonymisierenden Datenerfassung und Benutzerprofilerstellung? Welche positiven und negativen Beispiele sind bekannt? Der konzeptionelle Teil der Arbeit zeigt anhand eines Beispiels auf, wie Learning Analytics und Datenschutz funktionieren kann, unter Einbeziehung automatisch anonymisierender Verfahren. Das Anwendungsbeispiel sind adaptive digitale Lernspiele für die Bildauswertung

2 Einleitung

In dieser Arbeit geht es, um Learning-Analytics mit Bezug auf den Datenschutz. Zuerst werden Grundlagen geklärt, daraufhin wird der aktuelle Stand der Technik und Forschung vorgestellt und zuletzt wird anhand eines Anwendungsbeispiels aufgezeigt, wie mithilfe der zuvor vorgestellten Grundlagen, Learning-Analytics und Datenschutz funktionieren kann.

2.1 Motivation

> "Everybody's talking about Big Data and Learning Analytics, but if you don't solve privacy first it is going to be killed before it has really started."(Larry Johnson, CEO of the New Media Consortium(NMC).

Learning Analytics hat zum Ziel, dass Lernen individuell an die Fähigkeiten und den Wissensstand der Lernenden anzupassen. Dafür werden eine Vielzahl an Daten, über den Lernenden gesammelt und ausgewertet. Auf Grundlage der Auswertungen können Rückschlüsse hinsichtlich vorhandener Defizite des Lernenden gezogen werden. Daraufhin können Gegenmaßnahmen eingeleitet werden, wie z. B. verschärft den Lernfokus auf Bereiche zu richten, in denen mehr Übung notwendig ist, um somit den Lernenden besser bei seinem Lernprozess zu unterstützen.

2.2 Zielsetzung

Im Rahmen dieses Dokuments soll eine genauere Einsicht in die aktuelle Datenschutz-Grundverordnung, im Folgenden nur DSGVO genannt und deren Auswirkungen auf die Speicherung und Nutzung gegeben werden. Dazu wird zuerst erklärt was das DSGVO beinhaltet, auf welche Daten und Situationen es sich bezieht. Im Anschluss werden Herausforderungen die sich durch das DSGVO im Bereich Learning-Analytics und Big-Data genauer erläutert und es wird versucht Ansätze und Lösungsvorschläge zu geben, um diese zu bewältigen.

3 Grundlagen

In diesem Kapitel werden die Grundlagen des DSGVO sowie nötigen Begrifflichkeiten erläutert. Dazu wird zuerst auf den Datenschutz allgemein und anschließend auf das DSGVO im genaueren eingegangen. Dazu zählt auch was Datenschutz und die DSGVO für Learning-Analytics und Big-Data bedeutet.

3.1 Datenschutz

Im Internet oder bei der Nutzung von Software geben Nutzer oft eine Vielzahl von Informationen preis, die von einem Unternehmen gespeichert, verarbeitet und ausgewertet werden könnten. Dabei ist die Informationsmenge über die Jahre stetig gestiegen und auch ihre Auswertung und Nutzung wurde zunehmend komplexer. Auch ist das Bewusstsein von Nutzern über die Preisgabe ihrer persönlichen Daten nicht immer ausgeprägt, sie geben also oft Informationen preis, in der Annahme die Daten seien sicher.
Werden viele Daten gesammelt, sei es von Unternehmen oder auch vom Staat, so taucht immer wieder ein Schlagwort auf: “Der gläserne Mensch”
Mit diesem Ausdruck wird die Sorge umschrieben, dass durch wissentlich oder unwissentlich preisgegebene Daten nahezu alles über einen Menschen in Erfahrung gebracht werden kann und die Privatsphäre verschwindet und der Betroffene keine Möglichkeit hat dies zu unterbinden. Zuletzt war dies bei der Debatte um die Vorratsdatenspeicherung präsent.

Die offensichtlichsten Daten sind hierbei zum Beispiel:

- Vor- und Nachnamen
- Adresse
- Alter und/oder Geburtsdatum
- Bankdaten

Einem Unternehmen stehen oft jedoch auch Daten zur Verfügung, von denen ein Nutzer oft nicht weiß, dass er sie einem Unternehmen übermittelt. Dazu gehören unter anderem:

- Ip-Adresse
- Browse-Verhalten über Cookies und Tracker
- Aufrufhäufigkeit einer Website
- Aufenthaltsort bei Nutzung eines mobilen Gerätes

Solche Daten werden allgemein als personenbezogene Daten bezeichnet. In Deutschland gelten jene Daten als personenbezogen, die einer identifizierten oder identifizierbaren, also einer bestimmten natürlichen Person zugeordnet werden können. Diese Daten können somit die betroffene Person identifizieren oder identifizierbar machen. Weiterhin werden bestimmte personenbezogene Daten verschärft geschützt. Zu diesen Daten zählen unter anderem:

- Ethnische Herkunft
- Politische Meinungen
- Religiöse Überzeugungen und Angehörigkeiten
- Gewerkschaftszugehörigkeit
- Gesundheit und Sexualität

Wird im weiteren nur von Daten gesprochen, so handelt es sich dabei immer personenbezogene Daten.

Mittels solcher gesammelten Daten, kann ein Unternehmen viel über seine Nutzer herausfinden. Dies kann dazu genutzt werden personalisierte Angebote zu erstellen oder aber auch an den Kunden angepasste Werbung anzuzeigen. Jedoch könnten diese Daten auch an dritte verkauft werden, welche die Daten für andere Zwecke nutzen ohne, dass ein Kunde oder Nutzer davon Kenntnis hat. Wird von der Verarbeitung von Daten gesprochen, so fällt darunter jegliche Art von Vorgang bei dem personenbezogene Daten involviert sind. Es stellen sich beim somit Datenschutz für einen Nutzer einige von Fragen:

- Wie sicher sind die Daten gespeichert
- Wer hat zugriff auf die Daten
- Was für Daten hat ein Unternehmen

Datenschutz ist auch aus einem anderem Grund wichtig, viele Daten bedeuten für jene Unternehmen die sie Besitzen ein gewissen Maß an Macht und natürlich Geld. Wie bereits angesprochen können Unternehmen solche Daten nutzen um Werbung zu personalisieren oder anonyme Daten an andere Unternehmen verkaufen. So verdiente Google durch seine Informationen über Nutzer Ende 2016 etwa 79 Milliarden Dollar durch angepasste Werbung und deren Einnahmen.
Ein anderes Beispiel wie über die Sammlung von Daten Geld verdient werden kann ist die Schufa. Eine Anfrage an dieses Institut kostet und ist nur möglich wenn personenbezogene Daten, wie die Bonität eines Betroffenen, vorhanden sind.
Grade von Staatlichen Stellen ist ein inzwischen beliebtes Argument um viele Daten sammeln zu können die Terrorvermeidung. So wird versucht Telefondaten, Chat-Verläufe und andere Daten zu speichern um eventuell auf sie zugreifen zu können falls es nötig wird.
Durch den Datenschutz soll ein Nutzer vor missbräuchlicher Verarbeitung seiner Daten geschützt werden und sein Recht auf informationelle Selbstbestimmung soll gewährleisten werden. Ebenso dient es als Wahrung seiner Privatsphäre und soll dem Nutzer/Kunden ermöglichen zu entscheiden, wem er wann welche seiner persönlichen Daten zugänglich macht. Wichtig ist hierbei vor allem das Recht auf informationelle Selbstbestimmung, da es unter das in **Art. 1 Abs. 1 lit. a GG** bestimmte allgemeine Persönlichkeitsrecht fällt. Nach diesem Recht hat jeder Bürger und somit auch Nutzer einer Website oder Services, das Recht über die Preisgabe und Verwendung seiner Daten selbst zu entscheiden. Somit ist der allgemeine Datenschutz ein Schutz des Kunden bzw. Nutzers vor missbräuchlicher Nutzung seiner Daten und bedeutet, dass die Daten eines Kunden oder Nutzers vertraulich behandelt werden. Dieser Datenschutz bezieht sich jedoch nicht nur auf das Internet sondern auf alle Bereiche in denen Daten eines Kunden oder Nutzers gespeichert werden. Ebenso sollen dem übermäßigen Sammeln von Daten enge Grenzen gesetzt werden.
[1, 2]
Die rechtliche Grundlage für den Datenschutz in Deutschland stellt das **Bundesdatenschutzgesetz(BDSG)** dar, welches im Jahre 2003 in Kraft gesetzt wurde. Es soll die Daten der Bundesbürger vor unbefugten Zugriffen und Missbrauch schützen. Genauer gibt es Einrichtungen, welche Daten von einer Person überlassen bekommen haben, vor diese Daten effektiv zu schützen und nur dann zu erheben und zu sammeln, wenn die Person dem effektiv auch zugestimmt hat. Dazu gehört auch die Möglichkeit die Daten zur Kontrolle jederzeit einsehen zu können. Weiterhin beschränkt das BDSG welche Daten erhoben werden dürfen, wann dies geschehen darf und zu welchem Zweck und legt auch fest, welche Sicherheitsvorkehrungen die Einrichtungen und Unternehmen treffen müssen um die Daten sicher zu hinterlegen.
Da dieses Gesetz recht umfangreich ist und nicht direkt Thema dieser Ausarbeitung ist wird daher auf den online verfügbaren Gesetzestext verwiesen, welcher auch die fälligen Bußgelder bei Verstößen beinhaltet. [3]

3.1.1 Datenschutz in Unternehmen

Bisher wurde der Datenschutz nur allgemein betrachtet, weswegen an dieser Stelle kurz auf den Datenschutz innerhalb eines Unternehmens und dessen Auswirkungen auf ein solches eingegangen werden soll.
Das BDSG regelt nicht nur den Datenschutz für öffentliche Stellen sondern auch für nicht öffentliche Unternehmen und öffentlich-rechtliche Wettbewerbsunternehmen. Für solche Unternehmen ist das BDSG verbindlich sobald sie personenbezogene Daten nutzen, erheben oder verarbeiten. Dabei betrifft es vor allem jene Daten, welche automatisiert erhoben werden, oder aus automatisierten Verfahren innerhalb des Unternehmens stammen. Das BDSG begrenzt außerdem die Nutzung personenbezogener Daten auf(§1 Abs. 1 lit. a BDSG):

- Rechtsgeschäftliche Vorgänge oder rechts-geschäftsähnliche Schuldverhältnisse, für die derlei Daten notwendig sind
- Ein vorliegendes berechtigtes Interesse der Stelle, soweit dieses dem schutzwürdigen Interesses des Betroffenen nicht entgegensteht
- Daten, die allgemein zugänglich sind

Weiterhin ist für den Datenschutz, der Datenerhebung und deren Verarbeitung eine Zweckgebundenheit zwingend erforderlich. Dadurch soll verhindert werden, dass Unternehmen Daten auf Vorrat sammeln.
Die wichtigsten Punkte für Unternehmen sind hierbei:

- Der Zugriff und ein möglicher Datenmissbrauch muss mit allen zur Verfügung stehenden Mitteln verhindert werden
- Die Nutzung, Erhebung und Verarbeitung zu Werbezwecken, Adresshandel oder Marketing ist nur zulässig, sofern der Betroffene dieser Zweckbindung zustimmt
- Es bedarf einer Einwilligung des Betroffenen bei der Erhebung und Verarbeitung einer Daten
- Alle Unternehmen sind verpflichtet einen Datenschutzbeauftragten zu ernennen.
- Unternehmen dürfen einen erfolgreichen Vertragsabschluss nicht in Abhängigkeit der Einwilligung des Betroffenen stellen, somit gilt das Kopplungsverbot
- Anonymisierte Daten müssen getrennt von Daten gehalten werden, welche eine Identifizierung einer Person möglich machen
- Ein Unternehmen unterliegt der Auskunftspflicht gegenüber Betroffenen, deren Daten sie erheben, verarbeiten oder nutzen.

- Verjährte oder falsche Daten müssen nicht öffentliche Stellen löschen, berichtigen oder zugangssicher speichern
- Alle Mitarbeiter eines Unternehmens müssen auf das Datengeheimnis nach §5 BDSG verpflichtet werden, sofern sie mit personenbezogenen Daten arbeiten

Abließend ist zu sagen, das der Datenschutz in einem Unternehmen nicht nur für den Kunden wichtig ist, sondern auch für die eigenen Mitarbeiter. Bei Missachtung können hohe Bußgelder drohen, außerdem stärkt ein striktes einhalten der Vorschriften das Vertrauen eines Kunden oder der Mitarbeiter zu einem Unternehmen. [3, 4]

3.2 DSGVO

Die Datenschutzgrundverordnung, im weiteren nur DSGVO genannt, trat am 25.5.2018 in der gesamten Europäischen Union in kraft und sorgt für eine einheitliche Regelung zum Schutz von personenbezogenen Daten. Es ersetzt somit das BDSG als geltendes Recht. Das DSGVO geht dabei nach dem Prinzip **Verbot mit Erlaubnisvorbehalt** vor. Dies besagt, dass personenbezogene Daten grundsätzlich nicht Verarbeitet werden dürfen, bis eine ausdrückliche Erlaubnis vorliegt. Es ist dabei irrelevant ob es sich um die manuelle Verarbeitung oder automatisierte Verarbeitung von Daten handelt.
Diese nötige Erlaubnis kann über zwei Wege erteilt werden:

- Gesetzliche Regelung
- Einwilligung des Betroffenen

[5]
Das DSGVO bietet hierbei jedoch auch Ausnahmen in der Sachlichen Anwendung, welche in **Art. 2 lit. a DSGVO** zu finden sind. Darunter fallen unter anderem folgende Tätigkeiten oder Verarbeitungsprozesse:

- Tätigkeiten die nicht in den Anwendungsbereich des Unionsrechts fallen
- Wenn die Verarbeitung ausschließlich durch natürliche Personen ausgeführt wird und zur Ausübung persönlicher oder familiärer Tätigkeiten dient
- Prozesse von zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder Strafvollstreckung, sowie des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit

[6]
Der genaue Räumliche Anwendungsbereich des DSGVO ist genau in **Art. 3 lit. a DSGVO** festgehalten, allgemein kann jedoch gesagt werden, das es Anwendung findet, sobald personenbezogene Daten eines Betroffenen, welcher sich innerhalb der Union befindet, verarbeitet werden. Ebenso wird es angewendet wenn sich die Verarbeitende Stelle innerhalb

der Union befindet.
Da das DSGVO recht umfangreich ist und die genaue Auslegung durch einen Datenschutzbeauftragten unter Hilfenahme eines Juristen erfolgen sollte, wird weiterhin nur ein grober Überblick über das DSGVO und die Grundsätze der Verarbeitung von personenbezogener Daten gegeben.
Das DSGVO sagt über die Verarbeitung von personenbezogenen Daten, dass sie auf rechtmäßige Weiße, nach Treu und Glauben in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen. Weiterhin müssen diese Daten für einen festgelegten, eindeutigen und legitimen Zweck erhoben werden und dürfen nicht in einer mit diesem Zweck unvereinbaren Weise weiterverarbeitet werden. Eine Ausnahme ist hierbei die Archivierung von Daten für wissenschaftliche oder historische Forschungszwecke, sowie für statistische Zwecke. Auch müssen die Daten auf eine für den Zweck angemessene und minimale Menge beschränkt werden und sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Ebenso müssen die Daten in einer Form gespeichert werden, welche die Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für die Zwecke, für die sie erhoben und verarbeitet werden, erforderlich ist. Das heißt, dass personenbezogene Daten nur dann länger gespeichert werden dürfen, genaueres dazu in **Art. 5 lit. a DSGVO**. Als letzten wichtigen Punkt ist hierbei auch die angemessene Sicherheit aufgeführt, was bedeutet, das die erhobenen Daten vor unbefugter oder unrechtmäßiger Verarbeitung geschützt werden müssen, was geeignete technische und organisatorische Maßnahmen einschließt.
Auch die Rechtmäßigkeit der Verarbeitung von personenbezogener Daten wird im DSGVO geregelt. Dazu muss mindestens einer der Bedingungen in **Art. 6 lit. a DSGVO** erfüllt sein. Beispielhaft seien hier folgende aufgeführt:

- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben
- Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt
- Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen
- Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen

[6]
Als Bedingungen für eine Einwilligung gelten laut DSGVO folgende im Auszug von **Art. 7 lit. a DSGVO** genannten Punkte:

- Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat

- Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.

[6]
Wie durch diese Auszüge zu erkennen ist, regelt das DSGVO relativ genau wie mit personenbezogenen Daten umzugehen ist. Die Anwendung ist für die allgemeinen Fälle dabei ebenfalls vorgegeben, bei speziellen Anwendungsgebieten ist es jedoch ratsam einen Juristen zu konsultieren um sich Rechtlich absichern zu können.
Auf die weiteren genauen Bestimmungen, Bedingungen und Inhalte des DSGVO kann im Rahmen dieser Arbeit nicht eingegangen werden, da diese, wie bereits vorhergehend erläutert, einerseits sehr umfangreich sind, andererseits unter Zuhilfenahme eines Juristen und Datenschutzbeauftragten durchgegangen werden sollten.[5, 6]

Auf die weiteren genauen Bestimmungen, Bedingungen und Inhalte des DSGVO kann im Rahmen dieser Arbeit nicht eingegangen werden, da diese, wie bereits vorhergehend erläutert, einerseits sehr umfangreich sind, andererseits unter Zuhilfenahme eines Juristen und Datenschutzbeauftragten durchgegangen werden sollten. Darunter fallen zum Beispiel diverse im DSGVO enthaltenen Öffnungsklauseln welche im BDSG-neu beschrieben sind. Dieses BDSG-neu ist eine Erweiterung des DSGVO auf nationaler Ebene, dennoch gilt zuerst die DSGVO unmittelbar.[5, 6]

Kurz sei an dieser Stelle noch erläutert, was ein **Datenschutzbeauftragter** ist und welche Aufgaben ihm zufallen. Ein Datenschutzbeauftragter ist direkt der Geschäftsleitung unterstellt und kontrolliert sowie evaluiert die Prozesse unter datenschutzrechtlichen Gesichtspunkten und berät Unternehmen und Behörden in Datenschutzfragen. Er sorgt somit dafür, dass die datenschutzrechtlichen Bestimmungen hinsichtlich personenbezogener Daten eingehalten werden und ist zwingend notwendig und muss regelmäßig konsultiert werden. Ändern sich Geschäftsprozesse, muss dieser umgehend informiert werden um die geänderten Prozesse zu überprüfen, weiterhin ist er dafür zuständig Angestellte hinsichtlich des Datenschutzes regelmäßig zu schulen.[7]

3.3 Allgemeine Herausforderungen im Bezug auf das DSGVO

Wird das DSGVO in einem Unternehmen angewendet, so kommt es zu oft zu einer Vielzahl von Herausforderungen die gemeistert werden müssen. In diesem Abschnitt soll auf ein paar der Häufigsten eingegangen werden.

3.3.1 Zeitraum der Datenspeicherung

Ein wichtiges Recht welches durch die DSGVO gestärkt werden soll ist das **Recht auf Vergessen**. Das DSGVO gibt hierbei an, wann und unter welchen Umständen personenbezogene Daten zu löschen sind. Somit müssen diese Daten gelöscht werden sobald**Art. 17 Abs. 1 lit. a DSGVO**:

- Die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind
- Die betroffene Person ihre Einwilligung widerruft und es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt
- Die betroffene Person Widerspruch gegen die Verarbeitung einlegt und keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen
- Die personenbezogenen Daten unrechtmäßig verarbeitet wurden
- Die Löschung der personenbezogenen Daten zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich ist
- Die personenbezogenen Daten eines Kindes wurden in Bezug auf angebotene Dienste der Informationsgesellschaft, d. h. Internetangebote, wie Medien, Webshops oder Online-Spiele, erhoben.

[2]
Problematisch ist hierbei jedoch, dass das DSGVO den Begriff “Löschen”nicht genau definiert. Einzig ist dabei nur nötig, dass keine Möglichkeit mehr besteht, die personenbezogenen Daten ohne unverhältnismäßigen Aufwand zu erhalten oder zu rekonstruieren. Somit gibt es die Möglichkeit der physikalischen Löschung oder Zerstörung des Datenträgers und/oder die Verknüpfungen oder Codierungen zu löschen. Bei wiederbeschreibbaren Datenträgern muss ggf. eine spezielle Löschsoftware verwendet werden, welche z.B den Datenträger mehrfach mit zufälligen Daten überschreibt und somit eine Rekonstruktion erschwert/unmöglich macht.
Nicht ausreichend ist es hingegen den Datenträger im Müll zu entsorgen oder nur rein organisatorische Maßnahmen zu ergreifen.
Wichtig ist ebenfalls, dass die Daten unverzüglich, in der minimal nötigen Zeit, spätestens

jedoch innerhalb eines Monats, zu löschen sind sobald dies durch oben Genannte Bedingungen nötig sein sollte.
Das DSGVO sieht jedoch auch bei der Löschungspflicht Ausnahmen vor:

- Wenn die Daten für die Verarbeitung weiterhin erforderlich sind
- Die Daten für die Ausübung des Rechts auf freie Meinungsäußerung und Information nötig sind
- Sie zur Erfüllung einer Rechtspflicht oder öffentlicher Aufgaben nötig sind
- Wenn die Daten weiterhin genutzt werden für Gründe des öffentlichen Interesses im Bereich der öffentlichen Gesundheit
- Wenn ein öffentliches Interesse, wie Archivzwecke, Forschungszwecke oder statistische Zwecke vorliegen
- Falls die Daten für eine Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen nötig sind

Interessant ist hierbei dass der besprochene Punkt der Löschung von Verknüpfungen und Codierungen welche durch eine vollständige Anonymisierung erreicht werden kann.

3.3.2 Weitergabe von Daten an dritte

Die Weitergabe von personenbezogenen Daten, stellt einen massiven Eingriff in die Rechte der betroffenen Person dar. Daher ist vorab von Unternehmen sowie Privatpersonen zu klären ob die Weitergabe nach **Art. 6 lit. a DSGVO** rechtens ist, siehe dazu auch 3.2. Diese Vorgaben und Bedingungen sind zwingend einzuhalten, da ansonsten hohe Bußgelder drohen. Trifft keine dieser Bedingungen zu so ist die Weitergabe grundsätzlich verboten.

3.3.3 Wann ist ein Datenschutzbeauftragter nötig

Ein Datenschutzbeauftragter ist dann zwingend nötig, wenn es sich um eine öffentliche Einrichtung handelt und es muss sich in diesem Fall um einen behördlichen Datenschutzbeauftragten handeln. Bei nichtöffentlichen Stellen und Unternehmen ist ein solcher notwendig, wenn zehn oder mehr Personen dauerhaft mit der automatisierten Datenverarbeitung beschäftigt sind. In diesem Falle gilt die Pflicht einen Datenschutzbeauftragen zu bestellen, das heißt es kann sich auch um einen externen Beauftragten handeln. Wird die Datenverarbeitung hingegen nicht automatisiert also manuell durchgeführt, so ist es erst ab einer Personenstärke von zwanzig nötig einen Beauftragten zu bestellen. Zu beachten ist bei der Nutzung einer externen Kraft, dass diese oft für mehrere Unternehmen tätig sind und im schlimmsten falle nicht rechtzeitig reagieren können.

3.3.4 Anwendungsbereiche des Datenschutzes

Der Datenschutz findet Anwendung sobald personenbezogene Daten verarbeitet oder erhoben werden. Dabei ist es unerheblich wie diese Daten konkret verarbeitet werden. Somit besteht kein Unterschied zwischen der Verarbeitung von personenbezogenen Daten auf einem Blog, einer Shop-Website, einer Umfrage-Website oder in einem Lernspiel. Einzige Unterschiede sind die Technischen und organisatorischen Herausforderungen für die Umsetzung des DSGVO die sich durch die tatsächliche Verarbeitung und Nutzung der Daten ergeben.

3.4 Intelligente Lernumgebung

> „Everything will learn. These innovations are beginning to emerge enabled by cloud computing, big data analytics and learning technologies all coming together.“ - IBM

Eine Intelligente Lernumgebung passt sich den individuellen Bedürfnissen der Lernenden an.
Durch die Sammlung und Auswertung von Daten eines Lernenden und der Daten über die erbrachten Leistungen wird die Lernmethodik und der Inhalt so angepasst, dass der Lernprozess möglichst passend für den Lernenden geschneidert ist.

3.5 Intelligentes Tutorsystem

Ein intelligentes Tutorsystem (ITS) ist ein Computersystem, das darauf abzielt, den Lernenden sofortige und maßgeschneiderte Anweisungen oder Rückmeldungen zu geben. Das Ziel solcher Tutorsysteme ist ein sinnvolles und effektives Lernen zu ermöglichen. Ein Beispiel für so ein System wäre ILIAS, ein Forum in dem es durch verschiedene Plugins ermöglicht wird eine Rückmeldung zum Lernverlauf zu geben.

3.6 Digitale Lernspiele (Educational Serious Games)

Lernen mit Spaß ist der Grundsatz von Serious Games. Der Spaß am lernen fördert die Aufnahmefähigkeit des Lernstoffs. Das Wissen wird durch interaktive Methoden, die wie ein Spiel sind übermittelt, diese Strategie kann in jeder Bildungsstufe angewandt werden. Insbesonders digitale Lernspiele ermöglichen auch durch Fehler, die sonst einen Schaden verursachen würden, in der digitalen Welt durchzuführen. Das ”Learning by doing”wird hiermit gefördert. Ein gutes Beispiel für so ein digitales Lernspiel wären Flugsimulator Spiele.

4 Stand der Forschung und Technik

Im Bereich des Datenschutzes gibt es kaum bis keine Forschung, das die Rahmenbedingungen und Vorgaben Gesetzlich sind und somit feststehen. Diese Vorgaben sind einzuhalten, wie dies technisch und fachlich umgesetzt wird, wird im DSGVO auf der fachlichen Ebene beschrieben. Die technische Umsetzung ist dabei meist trivial oder aber siedelt sich eher im Bereich der Datensicherheit an, welche nicht Teil dieser Arbeit ist. Dennoch soll in den folgenden Kapiteln ein kurzer Überblick über die gängigsten und grundlegendsten Optionen für die anfängliche Sicherstellung der Einhaltung des DSGVO gegeben werden.

4.1 Datenschutz/DSGVO & E-Learning \Learning Analytics

Da wie bereits in den vorhergehenden Kapiteln der Datenschutz über das DSGVO allgemein ausgelegt ist und sich ausschließlich mit dem Verarbeiten von personenbezogenen Daten bezieht, gibt es diesbezüglich keine Forschung. Das DSGVO ist eine Gesetzesvorlage die einzuhalten ist, da ansonsten Bußgelder und Sanktionen drohen. Somit ist es irrelevant in welchem Kontext solche Daten verarbeitet werden, sei es über eine Umfrage oder das maschinelle Auswerten von Ergebnissen und Daten innerhalb eines Adaptiven Lernspieles. Sobald personenbezogene Daten, siehe Kapitel 3.1, involviert, erhoben oder auf irgend eine weise verarbeitet werden, greift das DSGVO und ist einzuhalten. Problematisch ist hierbei vor allem, ob durch genutzte Algorithmen nicht personenbezogene Daten doch einer bestimmten und korrekten Person zugeordnet werden könnten. Dies ist jedoch einer der Fälle, bei denen ein Datenschutzbeauftragter hinzugezogen werden sollte und übersteigt die Möglichkeiten innerhalb dieser Arbeit bei weitem.
Somit sollte als eine Grundregel gelten, dass genutzte Algorithmen überprüft werden und die Menge der verarbeiteten Daten auf ein Minimum reduziert wird.
Weiterhin ist es sinnvoll zu prüfen in wie weit personenbezogene Daten für eine Auswertung überhaupt nötig sind:

- Wird der Vollständige Name benötigt?
- Werden weiter Daten wie Alter, Geschlecht, Adresse etc. benötigt ?
- Kann von Beginn an eine Pseudonymisierung oder gar Anonymisierung genutzt werden ?

Da ein Lernspiel in der Regel mehrfach vom gleichen Nutzer aufgerufen und genutzt wird, ist eine Art der Identifikation nötig. Dies kann jedoch wie vom DSGVO vorgesehen über ein Pseudonym erfolgen, was ein erster Schritt zum Datenschutz des Betroffenen ist. Weitere personenbezogene Angaben dürfen hierbei, erst gespeichert werden, wenn der Betroffene dem zustimmt. Dies ist hierbei für alle Bereiche die das DSGVO tangiert gleich.

4.2 Anonymisierungsmethoden

Unter Anonymisierung versteht man nach § 3 Abs. 6 BDSG: „Das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.“

Das bedeutet, dass für Daten, welche anonymisiert vorliegen, die Grundsätze des Datenschutzes nicht gelten. Der Einsatz von Anonymisierung bildet somit eine Gesetzeskonforme Möglichkeit, mit sensiblen Daten umzugehen.

Im Folgenden wird ein kleines Beispiel aufgeführt, wie ein Datensatz, mithilfe einer einfachen Methode anonymisiert werden kann. Im Anschluss wird aufgezeigt, warum es weitere Methoden bedarf, um die Daten besser zu schützen.

Die Erste unten abgebildete Tabelle zeigt einen Datensatz, in dem Vorname, Nachname, Geschlecht, Adresse, PLZ, Geburtsdatum und Lieblingsfarbe gespeichert sind. Zur Anonymisierung müssen die personenbezogenen Daten identifiziert werden und daraufhin aus dem Datensatz entfernt werden. In diesem Fall, wären das der Vorname, der Nachname und die Adresse, da eine Person dadurch eindeutig identifiziert werden kann.

Vorname	Nachname	Geschlecht	Adresse	PLZ	Geburtsdatum	Lieblingsfarbe
Max	Musermann	M	Musterweg 12	76139	12.12.2012	Rot

Entfernt man die Daten aus dem Datensatz, so entsteht eine neue Tabelle. Der neue Datensatz ist nun anonymisiert.

Geschlecht	PLZ	Geburtsdatum	Lieblingsfarbe
M	76139	12.12.2012	Rot

Sweeny zeigt jedoch in einer Studie [**?**], dass in den USA, 87% aller Menschen eindeutig über ihre Postleitzahl, ihr Geburtsdatum und ihr Geschlecht identifiziert werden können. Die Ergebnisse aus der Studie verdeutlichen, dass das Weglassen von z. B. Namen und Adresse nicht ausreicht, um eine Zuordnung zu einer natürlichen Person zu verhindern.

Eine einfach Möglichkeit dies zu verhindern, wäre das Löschen aller Attribute, welche auf irgendeine Weise, Rückschlüsse auf die natürliche Person geben könnten. Das führt jedoch dazu, dass die Qualität des Datensatzes erheblich abnimmt und eine sinnvolle Auswertung

verhindert.

Zur Unterstützung der Anonymisierung personenbezogener Daten gibt es Modelle, welche bei der oben beschriebenen Problematik versuchen Abhilfe zu schaffen. [**?**]

K-Anonymität

Die K-Anonymität verhindert die Reidentifizierung einer Person in einem Datenbestand durch Anonymisierung dieser in einer Gruppe von anderen Personen des Datenbestandes.

4.3 Pseudonymisierung

Eine weitere Art des Schutzes der zugänglich gemachten Daten eines Nutzers stellt die sogenannte Pseudonymisierung dar. Im Gegensatz zur vollständigen Anonymisierung, welche im vorgehenden Kapitel erläutert wurde, werden hierbei personenbezogene oder persönliche Daten durch das Ersetzen von Kennzeichen oder Pseudonymen verändert. Genauer sind dies solche Daten und Merkmale, welche zur Identifikation einer Person genutzt werden können, also Identifikationsmerkmale. Dies soll eine Identifikation und Bestimmung des Betroffenen ausschließen oder zumindest deutlich erschweren. Jedoch ist es durch die Zusammenführung der Daten weiterhin möglich auf die Person zu schließen. Wichtig ist hierbei das die Zuordnung der Pseudonyme zu den tatsächlichen Daten separat und gut gesichert gespeichert wird, sodass der Aufwand diese Daten zu erlangen erheblich vergrößert wird. Was in diesem Kontext unter “erheblichßu verstehen ist, würde den Rahmen dieser Arbeit übersteigen, da dies eher in die Zuständigkeit eines Juristen bzw. Datenschutzbeauftragen fällt und im Einzelfall geklärt werden muss. Rechtlich fallen pseudonymisierte Daten weiterhin unter den Datenschutz und geltende Gesetze diesbezüglich. [8, 9]
Anbei sei noch ein Beispiel für eine Pseudonymisierung gegeben:

Vor der Pseudonymisierung:

ID	Vorname	Nachname	Bank
0001	Peter	Meyer	Taunusbank

Nach der Pseudonymisierung

ID	Bank
0001	Taunusbank

ID	Vorname	Nachname
0001	Peter	Meyer

5 Szenario: Learning Analytics für ein adaptives Bildauswertung-Lernspiel

SAR-Tutor ist eine vom Frauenhofer Insitut entwickelte Lernsoftware für die Radarbildauswertung. Grundlegende Prinzipien der Radartechnik und insbesondere des synthetischen Apertur Radar (SAR) werden als interaktiver Kurs mit Bilderkennungsaufgaben sowie Wissensfragen beigebracht. Die Ausbildung zur Radarbildauswertung wird in vielen Bereichen wie Küsten- und Gewässerschutz, Umweltschutz, Aufklärung und Überwachung benötigt.

5.1 Szenario 1: Benutzername und Passwort

In unserem ersten Szenario gehen wir vom momentanen Stand des Spiels aus. Das Spiel ist nicht adaptiv und speichert nur die Registrierungsdaten des Nutzers. Es werden keine Zugriffsdaten auf die Website gespeichert.

Damit das Szenario 1 Datenschutzkonform ist, muss als erster Schritt zwingend bei der Registrierung auf der Website eine Datenschutzerklärung akzeptiert werden. In dieser Datenschutzerklärung muss darauf hingewiesen werden, dass die Registrierungsdaten gespeichert werden. Dies erfolgt z.B. durch folgenden Absatz in der Datenschutzerklärung:

> Registrierung auf dieser Website
>
> Zur Nutzung bestimmter Funktionen können Sie sich auf unserer Website registrieren. Die übermittelten Daten dienen ausschließlich zum Zwecke der Nutzung des jeweiligen Angebotes oder Dienstes. Bei der Registrierung abgefragte Pflichtangaben sind vollständig anzugeben. Andernfalls werden wir die Registrierung ablehnen.
>
> Im Falle wichtiger Änderungen, etwa aus technischen Gründen, informieren wir Sie per E-Mail. Die E-Mail wird an die Adresse versendet, die bei der Registrierung angegeben wurde.
>
> Die Verarbeitung der bei der Registrierung eingegebenen Daten erfolgt auf Grundlage Ihrer Einwilligung (Art. 6 Abs. 1 lit. a DSGVO). Ein Widerruf Ihrer bereits erteilten Einwilligung ist jederzeit möglich. Für den Widerruf genügt eine formlose Mitteilung per E-Mail. Die Rechtmäßigkeit der bereits erfolgten Datenverarbeitung bleibt vom Widerruf unberührt.
>
> Wir speichern die bei der Registrierung erfassten Daten während des Zeitraums, den Sie auf unserer Website registriert sind. Ihren Daten werden gelöscht, sollten Sie Ihre Registrierung aufheben. Gesetzliche Aufbewahrungsfristen bleiben unberührt.

Die Registrierungsdaten (Kontoname und Passwort) müssen daraufhin so gespeichert werden, dass der Zugriff deutlich erschwert ist. Um eine weitere Abstraktionsstufe einzufügen, könnten die Daten Pseudonymisiert werden.

Die Pseudonymisierung der Datensätze in der Datenbank könnte wie folgt aussehen:

ID	Benutzername
0001	MaxMust99

ID	Verschlüsseltes Passwort
0001	0x88192A8F32492

5.2 Szenario 2: Benutzername, Passwort, Alter, Geschlecht Bildungsgrad, Lernverhalten

In diesem Szenario gehen wir davon aus, dass der SAR-Tutor adaptiv ist. Um den Lernverlauf für den Lernenenden am besten zu gestalten benötigt das Spiel verschiedene Daten.

Wie im Szenario 1 wird eine Registrierung mit Benutzername und Passwort benötigt. Der SAR-Tutor benötigt aber auch noch Daten zur adaptivität. Um eine Einstufung vor dem Spielen zu erstellen benötigen wir in unserem Fall das Alter, das Geschlecht und den Bildungsgrad des Lernenden. Diese Daten sollen dann auch bei der Registrierung abgefragt werden. Im weiteren Spielverlauf kann das Lernverhalten des Lernenden basierend auf das festgestellte Lernmuster (Prozent der korrekten Antworten, Zeit zum Antworten) weiterhin angepasst werden. Diese Daten werden auch gespeichert.

Analog zum Szenario 1 muss bei der Registrierung (vor dem Speichern von Daten) die Datenschutzerklärung akzeptiert werden. In diesem Fall wird die Datenschutzerklärung noch um die Daten ergänzt, die wir für die Adaptivität benötigen.

Die Daten könnten dann wieder pseudonymisiert in der Datenbank gespeichert werden:

ID	Benutzername
0001	MaxMust99

ID	Verschlüsseltes Passwort
0001	0x88192A8F32492

ID	Alter	Geschlecht	Bildungsgrad	Lernverhalten
0001	18	M	Abitur	4

6 Fazit & Ausblick

Datenschutz, das DSGVO, deren Umsetzung und Einhaltung dieser Bestimmungen sind ein umfangreiches und komplexes Thema. Es gibt viele Bereiche und Punkte, wie die Dokumentation, Weitergabe der Daten an Dritte, Art der Speicherung und Löschung welche beachtet werden müssen und bei denen Unternehmen oft juristischen Rat einholen sollten. Das DSGVO ist so ausgelegt, dass es allgemein gültig ist, also nicht nur für Software, sondern für alle Arten der Verarbeitung von personenbezogenen Daten. Personenbezogene Daten dürfen somit nur Zweckgebungen nach Ausdrücklicher Erlaubnis des Betroffenen gespeichert und verarbeitet werden. Ein Notlösung welche Rechtlich dennoch abgesichert werden muss, stellt die vollständig Anonyme Speicherung von Daten dar. Die genaue Umsetzung in einem Unternehmen hängt zudem von den verarbeiteten Daten und der Art der Verarbeitung ab, weshalb in dieser Arbeit darauf nur sehr beschränkt anhand von kleinen Beispielen eingegangen werden konnte. Somit wird eher ein allgemeiner Überblick über den Datenschutz mit einigen Hinweisen und Herausforderungen die sich im Bereich Learning Analytics ergeben können.
Dennoch ist der Datenschutz ein anhaltendes und wichtiges Thema und bei korrekter Umsetzung schützt es ein Unternehmen nicht nur vor rechtlichen Konsequenzen, es stärkt auch das Vertrauen der Kunden/Nutzer in ein Unternehmen.

Literatur

[1] Wikipedia. Datenschutz, 2019. https://de.wikipedia.org/wiki/Datenschutz, Aufruf-Datum: 10.06.2019.

[2] datenschutz.org. Datenschutz im Internetzeitalter: Privatsphäre & globale Vernetzung im Konflikt, 2019. https://www.datenschutz.org/, Aufruf-Datum: 21.06.2019.

[3] Bundesamt für Justiz. Bundesdatenschutzgesetz, 2019. https://www.gesetze-im-internet.de/bdsg_2018/, Aufruf-Datum: 21.06.2019.

[4] datenschutz.org. Datenschutz im Unternehmen: Was müssen nicht öffentliche Stellen beachten?, 2019. https://www.datenschutz.org/unternehmen/, Aufruf-Datum: 21.06.2019.

[5] datenschutz.org. DSGVO – Änderungen für Verbraucher und Unternehmen, 2018. https://www.datenschutz.org/dsgvo/, Aufruf-Datum: 31.05.2019.

[6] Datenschutz-grundverordnung. https://dsgvo-gesetz.de/,Aufruf-Datum: 11.05.2019.

[7] datenschutz.org. Datenschutzbeauftragter: Unabhängiges Kontrollorgan im Bereich Datenschutz, 2018. https://www.datenschutz.org/dsgvo/, Aufruf-Datum: 31.05.2019.

[8] Melissa Thesing. Unterschied zwischen Anonymisierung, Pseudonymisierung und Verschlüsselung, 2017. https://www.datenschutz-notizen.de/unterschied-zwischen-anonymisierung-pseudony-misierung-und-verschluesselung-291698 Aufruf-Datum: 11.04.2019.

[9] Dr. Datenschutz. Pseudonymisierung – was ist das eigentlich?, 2018. https://www.datenschutzbeauftragter-info.de/pseudonymisierung-was-ist-das-eigentlich/, Aufruf-Datum: 18.04.2019.