Hartmut Aden und Rainer Rumpel

Hochschul-Datenschutz in Zeiten der Digitalisierung

Einleitung

Unter Digitalisierung – auch digitale Transformation genannt – versteht man die Veränderung von Prozessen, Verfahren und Abläufen aufgrund des Einsatzes digitaler Technologien. Digitalisierung im engeren Sinne meint eine solche Veränderung aufgrund des Einsatzes von Computern. Diese Entwicklung begann in den 1950er Jahren und hat durch die Erfindung des Mikrocomputers in den 1980er Jahren einen Schub bekommen. Die „digitale Revolution" begann nach Auffassung vieler Autoren Anfang der 1990er Jahre mit der Verbreitung des Internets in Form des World Wide Web bei Forschungseinrichtungen, Unternehmen und Privatpersonen. Der Begriff „Digitalität" wird vornehmlich in den Geisteswissenschaften verwendet. Es geht hier um Bedingungen, unter denen der Mensch in einer digitalen Kultur lebt.

Dieser Beitrag untersucht – unter Berücksichtigung aktueller Entwicklungen – die Auswirkungen der Digitalisierung auf den Schutz der personenbezogenen Daten von Studierenden, Lehrenden und anderen Hochschulangehörigen. Dabei wird die These vertreten, dass diese Auswirkungen nicht völlig neu sind, sondern es sich um eine Weiterentwicklung jener Herausforderungen handelt, die mit der zunehmenden Nutzung von Informationstechnik in Hochschulen seit mehreren Jahrzehnten verbunden sind. Dies gilt umso mehr in Deutschland, wo das Bundesverfassungsgericht bereits im Jahr 1983 – als neue Variante des Allgemeinen Persönlichkeitsrechts aus der Menschenwürde (Art 1 Abs. 1 GG) und der Allgemeinen Handlungsfreiheit (Art. 2 Abs. 1 GG) abgeleitet[1] – in seiner Entscheidung zu der seinerzeit geplanten Volkszählung die *informationelle Selbstbestimmung* als Grundrecht etabliert hatte. Die Ausformulierung eines Datenschutz-Grundrechts in Art. 8 der EU-Grundrechtecharta und die EU-Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO)[2], die im Mai 2018 in Kraft getreten ist, können als konsequente Weiterentwicklungen dieses Grundrechts im Zeitalter der Digitalisierung betrachtet werden.

---

1 BVerfGE 65, 1.

2 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr […], Amtsblatt EU L 119 vom 4.5.2016, S. 1.

Die intensivierte Nutzung von Informationstechnik in Lehre, Forschung und Hochschulverwaltung, die zunehmende Vernetzung von Informationen und neuere Entwicklungen wie Cloud-Dienste und -Speicher erfordern neuartige Lösungen, bei denen Recht und Technik sowie Datensicherheit und Datenschutz eng miteinander verknüpft sind. Das *Privacy-by-Design*-Vorgehen, wie es auch die EU-Datenschutz-Grundverordnung vorsieht, ist dabei ein sinnvoller Trend.

1. Intensivere Nutzung von Informationstechnik in Hochschulen im Zuge fortschreitender Digitalisierung

Die Nutzung von Anlagen zur automatischen Verarbeitung von Daten hat eine lange Tradition an deutschen Hochschulen bzw. Universitäten. Der Bauingenieur Konrad Zuse (1910–1995) studierte an der TH Berlin (heute TU Berlin) und entwickelte die erste programmgesteuerte Rechenmaschine der Welt. Zuse wurde kein akademischer Mitarbeiter, sondern gründete ein Unternehmen. 1958 wurde mit der Z22 erstmals ein Zuse-Computer von der TU Berlin beauftragt und dort in erster Linie für technische Berechnungen in Betrieb genommen.[3] Ende der 1960er Jahre begannen die ersten Universitäten mit der Katalogisierung ihrer Monografien mithilfe von Computern.[4] In den 1970er Jahren hielt die Computertechnik auch in Fachhochschulen Einzug. Es wurden kleine Rechenzentren eingerichtet, die überwiegend technische Fachbereiche versorgten.[5] Hochschulinformationssysteme (EDV-Systeme zur Hochschulverwaltung) gibt es seit 1969.[6] Von der Zulassung über die Studierenden- und Prüfungsverwaltung bis hin zur Finanz- und Sachmittelverwaltung, Kosten- und Leistungsrechnung sowie zur Personal- und Stellenverwaltung bieten diese Systeme heutzutage IT-Unterstützung. Bis Ende der 1980er Jahre war an den Hochschulen der sogenannte zentrale Rechnerbetrieb mit Großrechnern (Mainframe) oder leistungsstarken Minicomputern für Fachbereiche vorherrschend.

3 *Rürup,* 1979, S. 398.

4 *Schnalke,* 2014, S. 144.

5 Siehe z. B. https://www.haw-hamburg.de/ti-mp/institute/ti-mpicamm/rechenzentrum/geschichte.html (aufgerufen am 25.3.2019).

6 *Auferkorte,* 2005, S. 53.

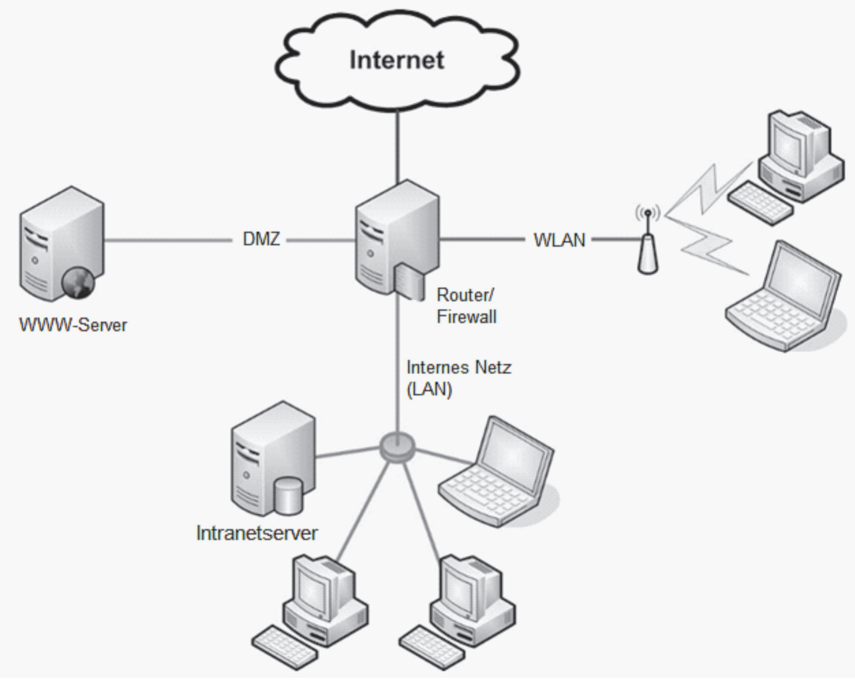
Abbildung 1: DEC-Minicomputer PDP-12, in den 1970er Jahren eingesetzt an diversen Universitäten

In den 1990er-Jahren schritt mit dem verstärkten Einsatz von Mikroprozessor-Personal-Computern (PC) die Dezentralisierung der automatischen Informationsverarbeitung voran. Einen weiteren Schub bekam die EDV an den Hochschulen durch die Nutzungsmöglichkeiten des weltweiten Internets, insbesondere des sogenannten World Wide Web (WWW) mit seinen Hypertexten. Nur wenige Jahre nach Erfindung des WWW wurde ein interaktiver Betrieb zwischen Webbrowser und Webserver möglich. Die Web-Anwendung war geboren. Datenbanken konnten am Endgerät ohne einen eigenständigen Datenbank-Client mittels Webbrowser über den Webserver angesteuert werden.

Zu Beginn des neuen Jahrhunderts entstand an den Hochschulen das „Ubiquitous Computing" („allgegenwärtiger Computereinsatz"): Fast alle Büro- und Laborarbeitsplätze an deutschen Hochschulen und die meisten Heimarbeitsplätze wurden mit vernetzten PCs ausgestattet. Studierende und Wissenschaftler nutzten zunehmend auch mobile Computer. Leistungsfähige leitungsgebundene und funkgestützte Netzwerke erlaubten den Austausch multimedialer Informationen. Softwaresysteme unterstützten immer mehr Prozesse in Forschung und Lehre sowie Fachverfahren von Bibliothek und Verwaltung. Es wurde begon-

nen, interne Daten- und Systemressourcen mit Internetressourcen zu einer IT-Landschaft zu integrieren.[7]

Abbildung 2: Typische Netzstruktur seit 1995



Zu den Standard-IT-Diensten für Lehrende und Studierende gehören heutzutage: Internetzugang, E-Mail, Bibliothekssoftware (z. B. OPAC), E-Learning-Plattformen (z. B. Moodle) und Informationsanwendungen für die Organisation des Hochschulbetriebs, die oft auf Intranetservern betrieben werden. Zunehmend stehen etliche Dienste an vielen Hochschulen auch als mobile Apps (Anwendungssoftware speziell für Mobilgeräte, z. B. Smartphones) zur Verfügung. Die Informationstechnik mit ihren Diensten ist der tägliche Begleiter von Studierenden, Lehrenden, Forschenden und Beschäftigten in der Verwaltung geworden.

7 *Moog,* 2005, S. 3 f.

2. Anforderungen des Datenschutzrechts an den Hochschul-Datenschutz

Rechtlich gesehen greift jede Erhebung und weitere Verarbeitung personenbezogener Daten durch eine staatliche Stelle, z. B. die Speicherung, die Nutzung oder die Übermittlung an Dritte, in das 1983 vom Bundesverfassungsgericht aus der Menschenwürde (Art. 1 Abs. 1 GG) und der Allgemeinen Handlungsfreiheit (Art. 2 Abs. 1 GG) abgeleitete Grundrecht auf informationelle Selbstbestimmung ein. Inzwischen gilt ein vergleichbarer Grundrechtsschutzstandard auch in der Europäischen Union, wo Art. 8 der EU-Grundrechtecharta die zentralen Anforderungen des Datenschutz-Grundrechts explizit ausführt:

> „(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
> (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
> (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht."

Die rechtlichen Grundanforderungen an den Hochschul-Datenschutz lassen sich unmittelbar aus diesen Formulierungen ableiten und werden durch die Anforderungen der DSGVO und des bundesdeutschen Hochschulrechts weiter konkretisiert. Ausgangspunkt ist der Anspruch aller Hochschulangehörigen und Dritter, deren Daten verarbeitet werden, auf Schutz ihrer personenbezogenen Daten. Hieraus folgt eine Pflicht der Hochschulen, Vorkehrungen für einen verantwortungsvollen Umgang mit personenbezogenen Daten zu treffen. Hochschulen dürfen personenbezogene Daten nur verarbeiten, wenn sie dafür eine gesetzliche Befugnis haben. Seit Mai 2018 ist für die Rechtmäßigkeit der Verarbeitung Art. 6 Abs. 1 lit. e DSGVO maßgeblich. Demnach ist eine Datenverarbeitung unter anderem dann rechtmäßig, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen (gemäß Bundesdatenschutzgesetz „verantwortliche Stelle") übertragen wurde. Wie in Deutschland bereits seit den 1980er Jahren üblich, wird diese Regelung weiterhin für den Zweck ordnungsgemäßer Anwendung durch spezialgesetzliche Regelungen konkretisiert, z. B. im Sozialgesetzbuch X und im Telekommunikationsgesetz. Solche spezialgesetzlichen Regelungen für die Hochschul-Datenverarbeitung sind in den Landesdatenschutzgesetzen, aber auch in den Hochschulgesetzen, speziel-

len Rechtsverordnungen für die Verarbeitung von Daten der Studierenden,[8] im Hochschulstatistikgesetz und in den Landesbeamtengesetzen für das verbeamtete Personal zu finden. Hochschulen und andere öffentliche Stellen erheben personenbezogene Daten fast ausschließlich auf Basis von gesetzlichen Befugnissen. In vielen Fällen werden Daten verarbeitet, weil dies zur Erfüllung von Hochschulaufgaben erforderlich ist. Nur ausnahmsweise können Hochschulen darüber hinaus Daten auf freiwilliger Basis erheben. Die Betroffenen müssen dann eine informierte Einwilligung für die Datennutzung zu konkret festgelegten Zwecken abgeben (Art. 7 DSGVO). In Berlin ist dies z. B. für die Verarbeitung von Alumnidaten erforderlich, weil es bislang an gesetzlichen Regelungen für die Kontaktpflege mit ehemaligen Studierenden fehlt. Wenn staatliche Hochschulen zur Erfüllung ihres Auftrags personenbezogene Daten verarbeiten, benötigen sie, damit dies zulässig ist, in der Regel keine Einwilligung, sondern sie handeln grundsätzlich auf gesetzlicher Basis.

Der Zweckbindungsgrundsatz ist auch für den Datenschutz in Hochschulen von zentraler Bedeutung. Personenbezogene Daten dürfen nur für zuvor festgelegte legitime Zwecke erhoben werden. Sollen sie später auch für andere Zwecke genutzt werden, so erfordert dies entweder eine spezifische Rechtsgrundlage oder eine informierte Einwilligung der Betroffenen. So wäre es z. B. unzulässig, Kontaktdaten der Studierenden, die für die Abwicklung des Studiums erhoben wurden, an Dritte weiterzugeben, die Werbung an die Studierenden verschicken möchten.

Auch die für den Datenschutz zentralen Individualrechte auf Zugang zu den eigenen Daten und Berichtigung fehlerhafter Daten, die in Art. 8 der EU-Grundrechtecharta garantiert sind, sind im Hochschulbereich zu implementieren. Hier gibt es Synergien mit dem Eigeninteresse der Hochschule an der Verwendung aktueller und korrekter Daten. Dieser Aspekt des Datenschutz-Grundrechts lässt sich am besten dadurch implementieren, dass die Studierenden lesenden Zugriff auf die sie betreffenden Daten erhalten.

3. Funktionen und Aufgaben von Hochschul-Datenschutzbeauftragten

Die Einhaltung von Datenschutzstandards wird nicht nur von den zuständigen staatlichen Datenschutzbeauftragten auf Landes- bzw. Bundesebene kontrolliert. Unternehmen sind gemäß Art. 37 Abs. 1 DSGVO zur Bestellung von Datenschutzbeauftragten verpflichtet, wenn sie in erheblichem Umfang personenbezogene Daten verarbeiten. Trotz der direkt wirkenden EU-Verordnung haben

8 In Berlin: Studierendendatenverordnung (StudDatVO) in der Fassung vom 25.2.2016, GVBl., S. 58.

die Mitgliedstaaten hier einen Gestaltungsspielraum. Gemäß Bundesdatenschutzgesetz (2018) haben Unternehmen Datenschutzbeauftragte zu bestellen, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, ihre Verarbeitungen der Datenschutzfolgeabschätzung unterliegen oder sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeiten.[9] Gemäß Art. 37 Abs. 1 lit. a DSGVO sind dagegen alle Behörden oder öffentlichen Stellen zur Benennung von Datenschutzbeauftragten verpflichtet, wenn sie personenbezogene Daten verarbeiten, also auch Hochschulen. Diese Form regulierter Selbstregulierung entlastet die staatliche Aufsicht und trägt zu einer effektiveren dezentralen Durchsetzung von Datenschutzstandards bei. Das für den Datenschutz erforderliche Fachwissen ist so auch in dezentralen Organisationseinheiten und eigenständigen öffentlich-rechtlichen Körperschaften wie Hochschulen verfügbar. Gemäß Art. 77 EU-DSGVO besteht für Betroffene das Recht auf Beschwerde bei der zuständigen Datenschutz-Aufsichtsbehörde, im Fall der HWR die Berliner Beauftragte für Datenschutz und Informationsfreiheit.

Hochschul-Datenschutzbeauftragte sind Teil eines Systems von Verantwortlichkeiten und Kontrollen – und damit ein *Accountability*-Forum.[10] In einem solchen *Accountability*-Forum haben Verantwortliche ihr Handeln gegenüber bestimmten Akteuren zu rechtfertigen. Verantwortliche für den Hochschul-Datenschutz sind die Hochschulmitarbeiter/-innen, die personenbezogene Daten verarbeiten, und ihre Vorgesetzten bis hin zur Leitungsebene.

Manche *Accountability*-Foren sind auf die Pflicht der Verantwortlichen beschränkt, Informationen und Rechtfertigungen bereitzustellen. Die Rechte von Datenschutzbeauftragten gegenüber Verantwortlichen gehen aber darüber hinaus, denn die Verantwortlichen sind auch zur Beantwortung von Nachfragen verpflichtet. Die Datenschutzbeauftragten können das Handeln der Verantwortlichen bewerten. Diese drei Elemente von *Accountability* gehören somit bei Hochschul-Datenschutzbeauftragten zum Standard. Noch weiter reichen *Accountability*-Foren, die auch Sanktionen aussprechen können. So eröffnet Art. 83 DSGVO den staatlichen Datenschutz-Aufsichtsbehörden die Möglichkeit, Bußgelder zu verhängen. Hochschul-Datenschutzbeauftragte und andere behördliche Datenschutzbeauftragte haben indes keine Sanktionsmöglichkeiten. Bei gravierenden Verstößen oder Meinungsverschiedenheit mit den Verantwortlichen über die einzuhaltenden Standards können sie den Datenschutzbeauftragten des zuständigen Bundeslands einschalten.

9 Zur Praxis: *Jaksch, von Daacke,* DuD 2018.

10 *Bovens* et al., 2014; *Raab*, 2012.

In Deutschland waren staatliche Stellen auch nach dem früheren Landes- bzw. Bundesrecht verpflichtet, eigene Datenschutzbeauftragte zu benennen. Aufgrund des Charakters der DSGVO als EU-Verordnung haben die Datenschutzgesetze des Bundes und der Länder nur noch konkretisierende Funktionen, so §§ 5 bis 7 BDSG 2018. Nach dem EU-einheitlichen Datenschutzrecht haben Datenschutzbeauftragte von Hochschulen und anderen öffentlichen Stellen vor allem beratende und kontrollierende Aufgaben (Art. 39 DSGVO). Bei größeren IT-Projekten wirken sie beratend an der Erstellung einer Datenschutz-Folgenabschätzung mit (Art. 35 DSGVO) mit. Eine frühzeitige fachliche Einbindung der Datenschutzbeauftragten in Entscheidungsprozesse über neue IT-Verfahren trägt zu einer datenschutzfreundlichen Technologieauswahl bei, soweit die Entscheidungsträger/-innen die Datenschutzbelange am Ende gebührend gewichten. So können insbesondere *Privacy-by-Design*-Konzepte verwirklicht werden, die hohe Datenschutzstandards durch technische Lösungen implementieren. Sie sind oft effektiver als Nutzungsregeln, deren Erfolg von der Beachtung durch die Beschäftigten oder die Studierenden abhängt.

Die unabhängige Stellung der Datenschutzbeauftragten ist für die Beratungs- und Kontrolltätigkeit essenziell. Sie reduziert das Risiko, dass niedrige Datenschutzstandards mit Rücksicht auf Vorgesetzte oder die Leitungsebene hingenommen werden. Die Europäisierung des Datenschutzrechts hat die Unabhängigkeit der Datenschutzaufsicht weiter gestärkt. Auf Bundesebene wurde die Datenschutzaufsicht daher im Jahr 2015 per Gesetz aus dem Innenministerium herausgelöst und ist jetzt als oberste Bundesbehörde unmittelbar dem Deutschen Bundestag zugeordnet.[11] Art. 38 DSGVO setzt hier jetzt die europaweit unmittelbar geltenden Standards.

Die Möglichkeiten und Grenzen dessen, was Hochschul-Datenschutzbeauftragte für die Gewährleistung hoher Datenschutzstandards leisten können, hängen von den verfügbaren Arbeitskapazitäten und von ihrer Positionierung in der Hochschulorganisation ab. Manche Hochschulen beschäftigen einen oder mehrere hauptamtliche Datenschutzbeauftragte. Dieses Modell hat den Vorteil, dass sich die Beauftragten ausschließlich diesen Aufgaben widmen können. Sie sind Teil der Hochschulverwaltung, aber bei der Erfüllung ihrer Aufgaben von der Leitungsebene unabhängig (Art. 38 DSGVO). Alternativ nehmen in anderen Hochschulen Professorinnen und Professoren die Aufgabe im Nebenamt wahr, so an der HWR Berlin. Dieses Modell hat den Vorteil, dass die Beauftragten nicht nur nach dem Datenschutzrecht, sondern auch aufgrund ihrer hochschulrechtlichen Stellung und der Wissenschaftsfreiheit unabhängig sind. Häufig wird die Aufgabe von Professorinnen und Professoren wahrgenommen, die auch in der Forschung auf dem Gebiet des Datenschutzes tätig sind. Das Mo-

11 Näheres zur Bedeutung der Unabhängigkeit des Datenschutzes: *Aden*, Vorgänge, 2015.

dell hat den Nachteil, dass der Hochschul-Datenschutz für die Beauftragten nur eine Aufgabe von vielen ist, was auch durch eine Anrechnung auf das Lehrdeputat nur teilweise kompensiert werden kann. Mit hauptamtlichen Unterstützungskräften kann dieses Modell jedoch an Effektivität gewinnen.

Im Mittelpunkt der Aufgaben von Hochschul-Datenschutzbeauftragten steht die Beratung der Entscheidungsgremien und der zuständigen Arbeitseinheiten (z. B. Fachbereiche, Personalabteilung) bei der Einführung neuer IT-Verfahren und bei der Klärung technischer und rechtlicher Datenschutzfragen. Fortbildungsveranstaltungen und Onlineschulungen für Führungskräfte und Sachbearbeiter/-innen können maßgeblich zu hohen Datenschutzstandards beitragen. Die Anpassung der Abläufe an die DSGVO hat erheblichen zusätzlichen Beratungsbedarf erzeugt. Viel Raum nimmt auch die Reaktion auf Fragen oder Beschwerden ein. Anzahl und Komplexität solcher Eingaben hängen stark von der (Vor-)Sensibilisierung der jeweiligen Hochschulangehörigen ab.

Schließlich zählen auch Kontrollen zu den Aufgaben des Hochschul-Datenschutzes. Nach heutigen Standards sind dabei insbesondere Arbeitsbereiche mit erhöhten Risiken für die Rechte und Freiheiten von Betroffenen relevant, z. B. solche, die große Datenmengen oder besonders sensible Daten wie Informationen zu Noten, Krankheiten oder persönlichen Präferenzen verarbeiten. In welchem Umfang solche risikoorientierten präventiven Kontrollen durchgeführt werden können, hängt indes von der Ausstattung der behördlichen Datenschutzbeauftragten ab.

4. Technisch-organisatorische Sicherheitsanforderungen an die Verarbeitung von personenbezogenen Daten in Hochschulen und Privacy by Design

Mit der Intensivierung der Nutzung von Informationstechnik wuchs das Bewusstsein für die Notwendigkeit des Schutzes von personenbezogenen Daten in der Bundesrepublik Deutschland. 1977 wurde das „Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung“ verabschiedet. Schon in diesem ersten Gesetz wurden Anforderungen an technisch-organisatorische Maßnahmen zur Gewährleistung des Datenschutzes (§ 6, später § 9) formuliert (mit Konkretisierung in einer Anlage). Hochschulen unterliegen in der Regel Landesrecht. Berlin (West) hatte seit 1978 ein eigenes Landesdaten-

schutzgesetz. Heutzutage findet das Berliner Datenschutzgesetz[12] als Ergänzung zur EU-Datenschutz-Grundverordnung, kurz: DSGVO) Anwendung.

Technisch-organisatorische Maßnahmen

Die Notwendigkeit der Anwendung geeigneter technisch-organisatorischer Maßnahmen (auch „TOM" genannt) zur Gewährleistung des Schutzes personenbezogener Daten ist jetzt europaweit verankert. Artikel 32 Abs. 1 DSGVO fordert für die Sicherheit der Verarbeitung die Anwendung solcher Maßnahmen, „um ein dem Risiko angemessenes Schutzniveau zu gewährleisten". Und in Artikel 26 Abs. 1 BlnDSG heißt es zu spezifischen technischen und organisatorischen Maßnahmen zur Gewährleistung einer rechtmäßigen Verarbeitung unter anderem zusätzlich: Der Verantwortliche hat

> „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung Maßnahmen zu ergreifen, die gewährleisten, dass […] bei der Bereitstellung personenbezogener Daten eine Trennung der Daten nach den jeweils verfolgten Zwecken und betroffenen Personen möglich ist."

Das eigentlich Neue bei der Handhabung von technisch-organisatorischen Datenschutzmaßnahmen ist der risikobasierte Ansatz. In Artikel 32 Abs. 1 DSGVO wird gefordert, dass die Maßnahmen unter Berücksichtigung der „Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen" zu treffen sind. Um dieser Anforderung gerecht zu werden, ist es hilfreich, auf die sogenannte „Datenschutz-Folgenabschätzung" gemäß Artikel 35 DSGVO zurückzugreifen. Diese ist zwar nicht bei jeder Verarbeitungstätigkeit obligatorisch, erweist sich aber zur Definition geeigneter TOM als hilfreich. Mit diesem Ansatz kommt es also nicht zu einer statischen, sondern zu einer verfahrensspezifischen, risikoorientierten TOM-Liste.

Zwecks Einschätzung des Niveaus des mit der Datenverarbeitung verbundenen Risikos für die Rechte und Freiheiten der Betroffenen kann die Anwendung des in Tabelle 1 aufgeführten Schemas nützlich sein.

12 Langtitel: Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz – BlnDSG), an die DSGVO angepasste Fassung vom 13.6.2018, GVBl. 2018, S. 418.

Tabelle 1: Risikobewertungsschema

Niveau des Daten-verarbeitungsrisikos	Beschreibung
	Aufgrund der Datenverarbeitung kann der Betroffene in seiner gesellschaftlichen Stellung und seinen wirtschaftlichen Verhältnissen, insbesondere durch Rufschädigung, Diskriminierung, Identitätsdiebstahl oder -betrug, finanziellen Verlust, Verlust der Vertraulichkeit von personenbezogenen Daten und der unbefugten Aufhebung der Pseudonymisierung, …
gering	… nur geringfügig beeinträchtigt werden.
mäßig	… erheblich beeinträchtigt werden.
hoch	… nicht nur erheblich beeinträchtigt werden, sondern es kann auch eine Gefahr für die körperliche Unversehrtheit oder die persönliche Freiheit des Betroffenen gegeben sein.

Einige typische TOM-Gebiete sind:

- Zutrittskontrolle (Gebäude und Räume),
- Zugangskontrolle (IT-Systeme),
- Zugriffskontrolle (Daten),
- Weitergabekontrolle (Datentransfer),
- Verfügbarkeitskontrolle (IT-Systeme),
- Auftragskontrolle bei Auftragsverarbeitung und
- Pseudonymisierung.

Privacy by Design

Ein wichtiger Aspekt des Datenschutzes ist der Zeitpunkt der Einführung von TOM für eine Verarbeitungstätigkeit. Gemäß Artikel 25 DSGVO „trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen“. Es ist also zu beachten, dass die Festlegung geeigneter TOM bereits vor dem „Zeitpunkt der eigentlichen Verarbeitung“, also in der Planungsphase (Designphase) zu erfolgen hat.

Ann Cavoukian, seit 1997 Informationsfreiheits- und Datenschutzbeauftragte von Ontario (Kanada), hat den Begriff maßgeblich populär gemacht. In ihrem Buch[13] charakterisiert sie „Privacy by Design" wie folgt:

> „In brief, Privacy by Design refers to the philosophy and approach of embedding privacy into the design specifications of various technologies. […] This approach originally had technology as its primary area of application, but I have since expanded its scope to two other areas. In total, the three areas of application are: (1) technology; (2) business practices; and (3) physical design."

Eine Designspezifikation ist eine schriftliche Festlegung einer bestimmten Designidee. Sie dient üblicherweise der Erfüllung von Anforderungen (z. B. „Lernen soll ortsunabhängig möglich sein"). Die ursprüngliche Designspezifikation sollte immer dem Beginn der Implementierung der Lösung vorausgehen.[14] Cavoukian fordert die Einbettung von Datenschutzaspekten in die Designspezifikation für Verarbeitungstätigkeiten. Der oder die behördliche Datenschutzbeauftragte hat vornehmlich die Aufgabe, die Verfahren der Datenverarbeitung auf Rechtskonformität zu überprüfen, die Mitarbeiter/-innen zu schulen und zur Datensicherheit zu beraten. Der oder die Datenschutzbeauftragte einer Hochschule muss folglich über die Designspezifikation eines geplanten Verfahrens zur Verarbeitung von personenbezogenen Daten informiert werden, bevor die Implementierung beginnt, damit er oder sie aufgabengemäß agieren kann. Es ist dann möglich, bei Bedarf rechtzeitig eine Datenschutz-Folgenabschätzung durchzuführen, daraus angemessene TOM abzuleiten und diese in die Designspezifikation einfließen zu lassen.

5. Ausgewählte Anwendungsfälle und Problemfelder des Hochschul-Datenschutzes

Im Folgenden werden ausgewählte hochschulspezifische Anwendungsfälle und Problemfelder des Datenschutzes analysiert. Besonderer Aufmerksamkeit bedürfen insbesondere solche Anwendungsfälle, bei denen große Mengen personenbezogener Daten oder besonders sensible Daten verarbeitet werden, oder Fälle, in denen die Datenverarbeitung aus dem Verantwortungsbereich der Hochschule heraus auf Dritte verlagert wird.

13 *Cavoukian,* 2009, S. 3.

14 *Gilb,* 2005, S. 350 f.

Campus-Management

Ein Campus-Management-System realisiert ein IT-Verfahren, in dem insbesondere die benötigten Studierendendaten verwaltet sowie die Lehr- und Raumplanung organisiert werden. Die Studierendendatenverarbeitung beginnt in der Regel mit der heute überwiegend online eingehenden Bewerbung und der Immatrikulation nach erfolgreicher Bewerbung. Sie setzt sich fort mit der Einschreibung in Module, der Organisation von Prüfungen und Wiederholungsprüfungen und der Dokumentation der Modulnoten. Schließlich reicht sie bis zur Organisation der Abschlussprüfungen, zur Erstellung des Abschlusszeugnisses und letztlich zur Exmatrikulation sowie zur Archivierung der Daten, die später für eine Rekonstruktion des Abschlusszeugnisses benötigt werden könnten. Auch personenbezogene Daten der Lehrenden (z. B. im Rahmen der Unterrichts- und Raumplanung) und der mit der Studien- und Prüfungsorganisation befassten Verwaltungsmitarbeiter/-innen werden in einem solchen System notwendigerweise erfasst.

Im Interesse effizienter und standardisierter Abläufe und zur Vermeidung von ineffizienten bzw. komplizierten Datentransfers zwischen Systemen ist die Zusammenführung all dieser Funktionen in einem einzigen System sinnvoll und muss aus der Perspektive von Datenschutz und Datensicherheit begleitet werden. Allerdings enthält ein solches System dann notwendigerweise große Mengen teils sensibler Daten wie Noten, Angaben zu Fehlversuchen bei Prüfungen oder Informationen über gesundheitliche Beeinträchtigungen, die zu einer verlängerten Bearbeitungszeit bei Prüfungen berechtigen.

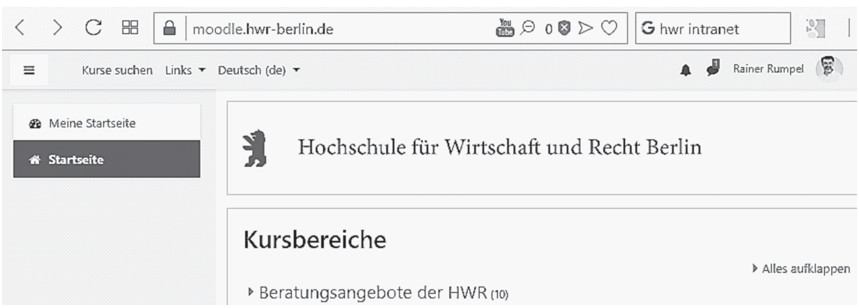
Aufgrund dessen sind technisch-organisatorische Maßnahmen nötig, die ein Campus-Management-System gegen „Datenpannen", Manipulation und unberechtigten Zugriff schützen. Eine essenzielle Datenschutzmaßnahme ist ein rollendifferenziertes Management der Zugriffsrechte, das sicherstellt, dass die zuständigen Lehrenden und Verwaltungsmitarbeiter/-innen schreibenden oder lesenden Zugriff nur auf diejenigen Daten erhalten, die für ihre spezielle Aufgabenerfüllung relevant sind *(Need-to-know-Prinzip)*. Die nötige Transparenz der Datenverarbeitung gegenüber den Betroffenen kann über einen Onlinezugang gewährleistet werden. Hierbei ist sicherzustellen, dass der Zugriff wirklich nur auf die eigenen Daten möglich ist und dass die für den Onlinezugriff nötige Netzanbindung möglichst keine Manipulations- oder unberechtigten Zugriffsmöglichkeiten für Dritte eröffnet.

E-Learning und Onlinetools für die Lehre

E-Learning soll das Lernen an der Hochschule unterstützen bzw. erleichtern. Es basiert auf IT-Systemen, die unter anderem personenbezogene Daten von Studierenden und Lehrenden verarbeiten. Im Mittelpunkt steht bei solchen Lernplattformen meist die Erstellung bzw. Verbreitung von Lernmaterialien. Elemente wie Foren und Wikis sind interaktive E-Learning-Komponenten. Systeme wie z. B. Moodle ermöglichen sogar elektronische Prüfungen. Es kann also sein, dass auch Leistungsergebnisse gespeichert werden. Die Leistungsbewertung sollte als Verarbeitungszweck nicht hinzugenommen werden. Dafür ist das von den Prüfungsämtern genutzte IT-System (z. B. das Campus-Management-System bzw. Hochschulinformationssystem) vorgesehen.

Für den Betrieb von E-Learning-Systemen werden als Benutzerstammdaten zumindest Nachname, Vorname und E-Mail-Adresse benötigt. Ansonsten sollten personenbezogene Daten der Nutzenden grundsätzlich nur erhoben werden, soweit dies zur Bereitstellung der Lernplattform und ihrer Funktionen erforderlich ist. Hier ist neben der DSGVO und dem Berliner Datenschutzgesetz die Studierendendatenverordnung Berlin maßgeblich.

Abbildung 3: Ansicht der Moodle-Plattform der HWR Berlin



Zum Schutz der Daten sollte auf jeden Fall darauf geachtet werden, dass der Anmeldevorgang auf der Lernplattform verschlüsselt abläuft (zu erkennen an dem Präfix *https*). Es ist nicht selbstverständlich, dass nach der Anmeldung am System auch alle nachfolgenden Transaktionen verschlüsselt ablaufen. Darauf ist zu achten bzw. dies ist zu berücksichtigen. In Abbildung 3 ist am Schloss in der Titelzeile erkennbar, dass beim Moodle-System der HWR Berlin mittlerweile auch der Datenverkehr nach Anmeldung verschlüsselt ist.

Weiterhin sollten angemessene Löschfristen festgelegt werden. Es ist beispielsweise unnötig, dass E-Learning-Accounts von Studierenden noch Jahre

nach der Exmatrikulation existieren bzw. aktiv sind. Stattdessen wäre ein Löschen wenige Monate nach Exmatrikulation angemessen. Ebenfalls ist es unnötig, Lernmaterialien auf Lernplattformen noch lange Zeit nach Abschluss der Lehrveranstaltung verfügbar zu halten. Eine Frist von drei bis vier Jahren ist vertretbar, damit die Informationen bis zum Studienabschluss der Studierenden bereitstehen.

Lernplattformen wie Moodle können so konfiguriert bzw. administriert werden, dass die Daten der Studierenden und Lehrenden ausschließlich auf hochschuleigenen Servern verarbeitet werden. Damit sind diese Daten von den allgemeinen Vorkehrungen der Hochschule für Datenschutz und Datensicherheit umfasst, z. B. für die Verhinderung des unerlaubten Zugriffs Dritter auf die Daten. Dieser Vorteil entfällt bei den meisten Onlinetools, die heute für die Lehre verfügbar sind. Projektmanagement, Lerntests, Abstimmungen und Kommunikationsplattformen sind niedrigschwellig und oft für die Benutzer kostenlos zugänglich. Viele dieser Angebote enthalten auch spielerische Elemente, die sich didaktisch gut in der Hochschullehre einsetzen lassen. Der Nutzung solcher Angebote sollte stets eine genaue Prüfung durch die Lehrenden vorausgehen, welche persönlichen Daten der Studierenden und Lehrenden die Anbieter erheben und für welche Zwecke sie diese verwenden. Sobald die in Lehrveranstaltungen genutzten Onlinetools personenbezogene Daten der Studierenden oder Lehrenden erheben, muss die Nutzung freiwillig sein. Die Hochschule verfügt über keine Rechtsgrundlage, aufgrund deren sie die Studierenden verpflichten könnte, ihre Daten solchen Anbietern zur Verfügung zu stellen. Studierenden, die ihre Daten dort nicht verwenden möchten, darf dadurch in Lehrveranstaltungen kein Nachteil entstehen.

Die Herausforderung besteht folglich darin, dass die Hochschule die Studierenden nicht nur mit den Einsatzmöglichkeiten solcher Onlineangebote vertraut macht, sondern auch mit ihren Risiken. Zu diesen Risiken zählt auch die Verwendung persönlicher Daten für Zwecke, mit denen die Betroffenen nicht einverstanden sind, z. B. für zielgenaue Onlinewerbung. Die Lehrkompetenz sollte – auch durch gezielte Fortbildungsangebote – so weiterentwickelt werden, dass Chancen und Risiken digitalisierter Lehre gleichermaßen bekannt sind und an den Studierenden vermittelt werden können.

Plagiatskontrolle

Nicht erst seit den Fällen, in denen Prominenten Doktortitel aufgrund von Plagiatsnachweisen aberkannt wurden, ist die Plagiatskontrolle für Hochschulen ein relevantes Thema. Im Zeitalter des Internets und leicht verfügbarer Onlinepublikationen steigt das Risiko, dass Studierende im Rahmen von Prüfungsarbeiten auf fremdes geistiges Eigentum zurückgreifen, ohne dies nach den wis-

senschaftlichen Regeln zu kennzeichnen. Plagiate können durch die vorsätzliche Übernahme fremder Leistungen entstehen, aber auch fahrlässig durch Sorgfaltsmängel beim wissenschaftlichen Arbeiten. So steigt das Plagiatsrisiko, wenn Arbeiten nicht auf der Basis eigener wissenschaftlichen Argumentation formuliert werden, sondern Studierende im Rahmen der Materialrecherche Textelemente Dritter zusammenkopieren. Daher ist es Aufgabe der Hochschule, Studierende vor den Folgen von Täuschungen über eigene Leistungen und Urheberrechtsverletzungen zu warnen und Plagiate aufzuspüren.

Plagiate, die durch das Kopieren von Texten aus Onlinepublikationen, die keine Zugangsbarriere haben, entstehen, lassen sich relativ leicht im Rahmen einer anlassbezogenen Überprüfung mit gängigen Internet-Suchmaschinen nachweisen. Darüber hinaus gibt es aber auch Plagiate, die durch die Übernahme von oder aus unveröffentlichten Arbeiten von Graduierten oder anderen Studierenden oder mittels Nutzung von zugangsbeschränkten Informationsdatenbanken entstehen. In diesen Fällen bedarf es eines Plagiatskontrollsystems.

Für das Aufspüren von Plagiaten haben einige Anbieter spezielle Kontrollsysteme entwickelt, die den Abgleich sowohl mit Onlinequellen als auch mit anderen, im zugehörigen Datenlager verfügbaren Arbeiten ermöglicht. Aus Datenschutzperspektive gibt es mehrere Aspekte der Herausforderung. Für die Hochschule handelt es sich um eine spezielle Variante von Auftragsverarbeitung (Auftragsdatenverarbeitung), wenn das System nicht im eigenen Netz mit eigenen Ressourcen betrieben wird (z. B. in einer internen Private Cloud). Die externe Plagiatskontrolle von Studierendenarbeiten generiert sensible Daten, da hohe Übereinstimmungswerte mit Drittquellen jedenfalls den Verdacht eines unrechtmäßigen Handelns erzeugen. Besonders problematisch ist der Umstand, dass führende Anbieter von Plagiatskontrollsystemen weltweit agieren und die Daten nicht in der Europäischen Union verarbeiten. Die Anbieter unterliegen mittlerweile auch den Regeln der DSGVO, wenn eine Niederlassung Dienstleistungen in der Europäischen Union erbringt. Die Datenverarbeitung muss dabei gemäß Artikel 3 DSGVO nicht in der EU stattfinden. Doch wird die Datenschutzkontrolle durch die Datenverarbeitung außerhalb der EU stark erschwert. Und Zugriffe, z. B. von Nachrichtendiensten der USA und anderer Drittstaaten, können trotz vertraglicher Regelungen nicht wirksam ausgeschlossen werden. Die Übermittlung von Inhalten, die Geschäfts- und Betriebsgeheimnisse enthalten oder die als Behörden-Verschlusssachen eingestuft sind – wie sie in HWR-Studiengängen vorkommen –, ist daher zu vermeiden.

Da eine Plagiatskontrolle, jedenfalls gelegentlich, heute erforderlich ist, um Täuschungen bei wissenschaftlichen Arbeiten wirksam zu verhindern, sind Veränderungen erforderlich. Zum einen müsste die Landesgesetzgebung den Hochschulen klare gesetzliche Regelungen für die Plagiatskontrollen bereitstellen. Zum anderen sollten die deutschen Hochschulen eine eigene, nichtkommerziel-

le Plattform für die Plagiatskontrolle aufbauen und die Verknüpfung mit gängigen E-Learning-Plattformen wie *Moodle* ermöglichen, um bei der Plagiatskontrolle mit möglichst wenig Studierendendaten auszukommen und diese in einem rechtlich und technisch sicheren Rahmen zu verarbeiten. Als Betreiber einer solchen Plattform käme das Deutsche Forschungsnetz in Frage.

Cloud-Dienste

Das Bundesamt für Sicherheit in der Informationstechnik hat folgende Definition für den Begriff „Cloud-Computing" festgelegt:

> „Cloud-Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud-Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software."[15]

Eine Kerntechnologie des Cloud-Computings ist die Virtualisierung von IT-Systemen. Cloud-Computing existiert hauptsächlich in den Formen „Private Cloud" und „Public Cloud". In einer Private Cloud wird die Cloud-Infrastruktur nur für eine Institution betrieben. Sie kann im Rechenzentrum der eigenen Organisation oder einer anderen Organisation stehen. Von einer Public Cloud wird gesprochen, wenn die Services von der Allgemeinheit oder einer großen Gruppe, wie beispielsweise einer ganzen Industriebranche, genutzt werden können und die Services von einem Anbieter zur Verfügung gestellt werden.

Ein Cloud-Dienst ist eine IT-Dienstleistung, die organisationsintern oder von einem IT-Dienstleister erbracht wird. Solange die Dienstleistung intern in einer Private Cloud erfolgt, entstehen keine besonderen datenschutzrechtlichen Herausforderungen. Wenn die Dienstleistung aber von einem externen Cloud-Dienst-Anbieter erbracht wird und personenbezogene Daten verarbeitet werden, so ist die Rechtmäßigkeit der Verarbeitung durch die verantwortliche Stelle (Cloud-Anwender) zu prüfen. Nimmt der Cloud-Anwender von einem Cloud-Anbieter einen Cloud-Dienst inklusive Übermittlung von personenbezogenen Daten in Anspruch, so wird dadurch ein Auftraggeber-Auftragnehmer-Verhältnis begründet, das datenschutzrechtlich *Auftragsverarbeitung* genannt wird und in der DSGVO geregelt ist.[16] Das Berliner Datenschutzgesetz führt dazu aus, dass die Verarbeitung auf der Grundlage eines Vertrags oder eines an-

15 BSI o. J.

16 Artikel 4, Artikel 28 DSGVO.

deren Rechtsinstruments zu erfolgen hat, der oder das den Gegenstand, die Dauer, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Rechte und Pflichten des Verantwortlichen festlegt.[17]

Da die Cloud und die darin stattfindende Datenverarbeitung nicht an geografische Grenzen gebunden sind, ist es wichtig zu wissen, wo die Cloud-Anbieter und Unteranbieter tätig werden. Die Datenschutz-Grundverordnung findet auch auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Europäischen Union befinden, Anwendung, wenn die Verarbeitung durch einen nicht in der Union niedergelassenen Auftragsverarbeiter im Rahmen der Tätigkeiten einer Niederlassung stattfindet.[18]

Weitere Anmerkungen zum Thema Cloud-Computing am Beispiel Software as a Service finden sich im nachfolgenden Abschnitt.

Externe Datenverarbeitung – Auftragsdatenverarbeitung

Die Datenverarbeitung durch die Hochschule auf eigenen Servern ist aus Sicht des Hochschul-Datenschutzes stets die beste Lösung. Sie stellt sicher, dass die Daten nach den hohen Standards öffentlicher Stellen gespeichert und gegen unbefugten Zugriff, Angriffe von außen oder Verluste wegen unsachgemäßer Handhabung geschützt werden. Technisch wäre es heute möglich, die gesamte Datenverarbeitung ausschließlich auf hochschuleigenen Servern durchzuführen.

Allerdings ist es auch für Hochschulen bei manchen Fachverfahren erforderlich bzw. sinnvoll, externe Stellen mit der Verarbeitung personenbezogener Daten für Hochschulzwecke zu beauftragen. Aus der Perspektive der Hochschule handelt es sich um Auftragsverarbeitung, deren Anforderungen jetzt EU-einheitlich in Art. 28 DSGVO geregelt sind. Aus Kostengründen könnte beispielsweise die Lohn- und Gehaltsabrechnung per Auftragsverarbeitung von einem Shared-Service-Center betrieben werden. Es handelt sich hier um eine Beauftragung mit einer fachlichen Dienstleistung, bei der die Datenverarbeitung im Vordergrund steht. Ein adäquates Datenschutzniveau lässt sich durch eigene Datenschutzvorkehrungen des Auftragsverarbeiters und die dort tätigen Datenschutzbeauftragten gewährleisten. Zudem haben auch die Datenschutzbeauftragten der Hochschulen Prüfungsrechte bei den Auftragsverarbeitern.

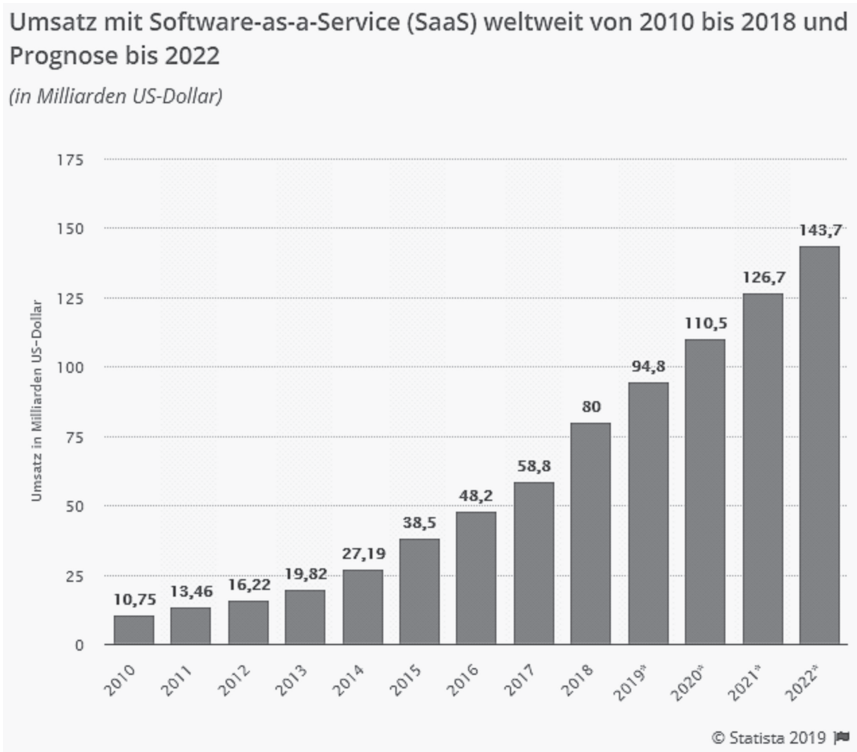
In weiteren Fällen wird erwogen, ob die Variante, dass Softwareanbieter ihre Dienste kostengünstig anbieten, indem sie die betroffenen Daten im Auftrag verarbeiten, attraktiv ist. Es handelt sich um Software as a Service, eine

17 § 48 Abs. 5 BlnDSG.

18 Artikel 3 Abs. 1 und 2 DSGVO.

Variante des Cloud-Computings. Das starke Marktwachstum ist in Abbildung 4 dargestellt.

Abbildung 4: Umsatz mit Software-as-a-Service (SaaS) weltweit von 2010 bis 2018 und Prognose bis 2022



Aus Datenschutzperspektive können Kostenargumente jedoch erhöhte Risiken nicht rechtfertigen, die etwa dadurch entstehen können, dass externe Dienstleister Daten für eine Vielzahl von Auftragnehmern verarbeiten oder dass sensible Daten via Internet zum Auftragnehmer transportiert werden. Es muss analysiert werden, ob es möglich ist, den Risiken mit angemessenen technisch-organisatorischen Maßnahmen zu begegnen.

In einigen Fällen basiert die Notwendigkeit einer Verarbeitung von personenbezogenen Daten bei externen Stellen auf hochschulpolitischen Entscheidungen, etwa im Fall der zentralisierten Studienplatzvergabe über das „dialog-

orientierte Serviceverfahren“, das die frühere Zentralstelle für die Vergabe von Studienplätzen abgelöst hat. Hier erteilt die Hochschule aber keinen expliziten Verarbeitungsauftrag, sondern für die Rechtfertigung der Verarbeitung besteht eine Rechtsgrundlage (z. B. Zulassungsverordnung).

Für die Hochschul-Datenschutzbeauftragten stellt die Auslagerung ganzer Datenbestände im Rahmen von Auftragsverarbeitung eine besondere Herausforderung dar. Denn die Prüfung des Umgangs mit den Datenbeständen ist dann am Hochschulstandort nur eingeschränkt möglich, da der Auftragsverarbeiter wesentliche Teile der Verarbeitung in seinen Räumlichkeiten oder bei Drittanbietern durchführt. Die Prüfung von Dokumenten des Auftragsverarbeiters ist eine nützliche Ergänzung. Eine Prüfung beim Auftragsverarbeiter vor Ort kann mit erheblichem Aufwand verbunden sein.

Auch wenn eine externe Datenverarbeitung manchmal Vorteile haben mag, sollte sie wegen der damit verbundenen Risiken nur im Rahmen des unbedingt Erforderlichen bleiben.

Datenschutz in der Forschung

Die Einhaltung von Datenschutzstandards ist an der HWR auch Gegenstand von Forschungsprojekten, etwa wenn im *Forschungsinstitut für Öffentliche und Private Sicherheit* (FÖPS Berlin) die Auswirkung neuer Sicherheitstechnologien auf den Datenschutz untersucht werden.[19]

Die Forschungstätigkeit selbst ist ebenfalls an Grundsätze des Datenschutzes gebunden. Grundrechtlich betrachtet muss hier die Konkordanz zwischen dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG/Art. 8 EU-Grundrechtecharta) und der Forschungsfreiheit (Art. 5 Abs. 3 GG) hergestellt werden. In der Praxis heißt dies, dass die Verwendung von personenbezogenen Daten für rechtlich und ethisch vertretbare Forschungszwecke grundsätzlich möglich ist, dass aber Vorkehrungen für den Schutz der personenbezogenen Daten getroffen werden müssen. In der Regel ist bei Forschungsvorhaben nicht die konkrete Person von Interesse, sondern ihre Meinungen, Einschätzungen oder Lebensumstände bilden zusammen mit den Daten anderer Personen die Datenbasis für die weitere Forschung. Die frühzeitige Anonymisierung von Forschungsdaten ist daher der Standard, der den Ausgleich zwischen Forschungsfreiheit und Datenschutz-Grundrecht gewährleistet.

Die zunehmende Digitalisierung kann im Spannungsverhältnis zwischen Datenschutz und Forschungsfreiheit zu neuen Herausforderungen führen. So wird die wirksame Anonymisierung von Forschungsdaten schwieriger, wenn

19 Überblick unter www.foeps-berlin.org.

Institutionen über Rechenkapazitäten verfügen, die es zumindest theoretisch ermöglichen, bei einer ausreichenden Menge an scheinbar anonymisierten Daten ein Persönlichkeitsprofil und damit eine Identifizierbarkeit abzuleiten.[20]

Neue Herausforderungen entstehen auch dort, wo Forschungsvorhaben große Mengen von Daten mit Personenbezug („Big Data") analysieren. Hier benötigt die Forschung neue Standards, die verhindern, dass Wissen über Menschen entsteht, das tief in deren Privatsphäre eindringt, etwa in der Gesundheitsforschung, bei der automatisierten Gesichtserkennung oder bei der Analyse von individuellen Bewegungsmustern.

Hochschul-Datenschutz muss hier darauf bedacht sein, die Interessen der Betroffenen zu schützen, ohne die Erfüllung der Forschungsaufgaben unnötig zu erschweren.

Literaturverzeichnis

Aden, H.: Datenschutzkontrolle auf Bundesebene – unabhängiger und effektiver? In: Vorgänge Nr. 210/211, 2015, S. 245–250.

Auferkorte-Michaelis, N.: Hochschule im Blick: Innerinstitutionelle Forschung zu Lehre und Studium an einer Universität, 2005.

Bovens, M. et al.: Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism, in: Accountability and European Governance, Oxford, 2014, S. 9–13.

BSI (Bundesamt für Sicherheit in der Informationstechnologie) o. J.: Cloud-Computing-Grundlagen, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.html (aufgerufen am 25.2.2019).

Cavoukian, A.: Privacy by Design – Take the Challenge, Toronto, 2009.

Gilb, T.: Competitive Engineering: A Handbook for Systems Engineering, Requirements Engineering, and Software Engineering, Oxford, 2005.

Jaksch, C., von Daacke, G: Datenschutzbeauftragter und Datenschutz-Organisation unter der DSGVO, DuD 2018, 758–763.

Moog, H.: IT-Dienste an Universitäten und Fachhochschulen, Hochschulplanung Band 178, Hannover, 2005.

Rürup, R. (Hrsg.): Wissenschaft und Gesellschaft – Beiträge zur Geschichte der Technischen Universität Berlin 1879–1979, Heidelberg, 1979.

Schnalke, M.: Die Anfänge der digitalen Revolution: Der Einzug der Computertechnik in das wissenschaftliche Bibliothekswesen am Beispiel der baden-württembergischen Universitätsbibliotheken Konstanz und Ulm, in: Perspektive Bibliothek Band 3, Nr. 1, Heidelberg, 2014.

Raab C.: The Meaning of „Accountability"' in the Information Privacy Context. In: Guagnin, D. et al. (Hrsg.), Managing Privacy Through Accountability. Basingstoke, 2012, S. 15–32.

Spindler, G.: Die neue EU-Datenschutz-Grundverordnung, in: Der Betrieb, Heft 16, 2016, S. 937–947.

20 *Spindler,* 2016, S. 938.