Bernhard C. Witt

Datenschutz an Hochschulen

Im stillen Gedenken an meine Eltern

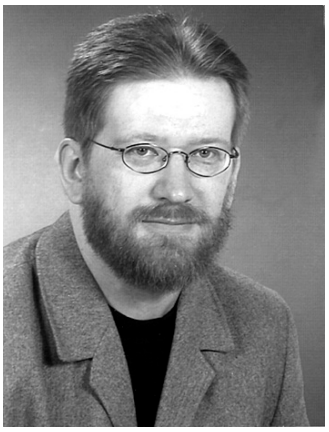
Datenschutz an Hochschulen

Ein Praxishandbuch für Deutschland am Beispiel der Universitäten Baden-Württembergs

von Bernhard C. Witt

Informatiker und Industriekaufmann,
Universität Ulm, Fakultät für Informatik

Leg Artis



Bernhard C. Witt, geboren 1967 in Pfullendorf (Baden), hat nach seiner Ausbildung zum Industriekaufmann das Studium der Informatik an der Universität Ulm aufgenommen. Sein inhaltlicher Schwerpunkt liegt dabei auf dem Gebiet „Informatik und Gesellschaft“ und darin wiederum beim Datenschutz. Er war jahrelang freiberuflich journalistisch tätig und ist seit 1998 im Bereich „Wissenschaftliches Arbeiten“ selbständig.
Seit 1996 ist er an der Fakultät für Informatik an der Universität Ulm für die Evaluation zuständig, beriet die Universität Ulm bei der Einführung ihrer Hochschulkostenrechnung und fungierte als Gutachter für den Akkreditierungsrat.

**Die Deutsche Bibliothek –
CIP-Einheitsaufnahme**

Witt, Bernhard C.
Datenschutz an Hochschulen
Ein Praxishandbuch für Deutschland am Beispiel der Universitäten Baden-Württembergs, Ulm,
LegArtis, 2004

ISBN 3-936494-36-3

Umschlagentwurf und Typografie:
ENORM Agentur für Visuelle Kommunikation, Köln

gesetzt aus der Janson;
gedruckt auf chlorfrei gebleichtem, holzfreiem Papier

ISBN 3-936494-36-3

www.legartis.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Einleitung

Dieser Arbeit liegt das Selbstverständnis der Informatik als Wissenschaft der Informationsverarbeitung zugrunde. Angesichts des seit geraumer Zeit angebrochenen „Zeitalters der Informationsgesellschaft“ ist es insbesondere für Informatiker wichtig, über die gesellschaftlichen Auswirkungen ihres Handelns zu reflektieren. Denn die Informatik entfaltet sich in der Praxis vorwiegend im Zusammenspiel mit anderen Disziplinen, den „Anwendungsgebieten“. Allgemein werden die Schnittstellen der Informatik mit diesen Gebieten „Angewandte Informatik“ genannt. Ein besonders sensibler, aber zugleich für die Informatik grundlegender Bereich aus der Angewandten Informatik ist der Umgang mit personenbezogenen Informationen.

Motivation und Eingrenzung des Themas

Bisher existiert keine Zusammenstellung, welche Datenschutz-Vorschriften unter welchen Umständen an Hochschulen zu beachten sind. Gleichwohl liegt hier jedoch ein spannendes Interessengeflecht vor, zumal gerade in Hochschulgremien des öfteren datenschutzrelevante Themen erörtert werden. Diese Arbeit soll daher einen Überblick verschaffen und Anregungen zu datenschutzkonformen Handlungen im Rahmen der Hochschulverwaltung und akademischen Selbstverwaltung geben.

Obwohl in Baden-Württemberg in vielen Belangen Fachhochschulen und Pädagogische Hochschulen den Universitäten gleichgestellt sind, wurden in dieser Arbeit speziell die Universitäten näher betrachtet – die Ergebnisse sind jedoch übertragbar. Dabei wurden bewusst Aspekte von Einrichtungen, die mit Universitäten in Verbindung stehen, wie etwa Studentenwerke oder An-Institute, außer Acht gelassen.

Es ist nicht Gegenstand dieser Arbeit, einen Abgleich zwischen gesetzlichen Vorschriften und der tatsächlichen Praxis an den Landesuniversitäten hinsichtlich der Einhaltung des Datenschutzes vorzunehmen. Dies ist vielmehr die Aufgabe von behördlichen Datenschutzbeauftragten sowie des Landesdatenschutzbeauftragten, welcher in seinen jährlichen Tätigkeitsberichten über etwaige Verstöße berichtet. Gleichfalls ist es nicht Thema dieser Arbeit, aufzuzählen, welche Konsequenzen jeweils aus etwaigen Verstößen resultieren würden.

Es ist auch nicht Aufgabe dieser Arbeit, darzustellen, an welchen Landesuniversitäten im Rahmen der Lehre und Forschung Themen aus dem Bereich des Datenschutzes vermittelt bzw. angegangen werden.

Die vorliegende Arbeit ist aus der Sicht der Informatik geschrieben und keine rechtswissenschaftliche Abhandlung. Sie ist in den Bereich der „Angewandten In-

formatik“ und dabei speziell in den Gebieten „Informatik und Gesellschaft“ und „Datenschutz“ einzuordnen.

Zum Verhältnis zwischen Informatik und Jura

In juristischen Fragen geht diese Arbeit überwiegend davon aus, dass die Gesetze, Verordnungen, Vereinbarungen und Urteile vorgegeben sind und sich im Einklang mit den verfassungsrechtlichen Grundsätzen befinden. In der Regel ist in der Jurisprudenz der Einzelfall entscheidend. Analogieschlüsse sind – im Gegensatz zu Informatik – eher untypisch. Erst im Zuge der Verfassungsauslegung gewinnen Analogien an Substanz.

Konnte also keine spezialrechtliche Vorschrift gefunden werden, wurden die Grundsatz-Urteile des Bundesverfassungsgerichts als maßgebliche Grundlage verwendet. Eine umfassende Herleitung von Rechtsgrundsätzen, ausgehend von der Menschenwürde, wäre eher Aufgabe der Rechtswissenschaften.

Ein Problem, das im Rahmen dieser Arbeit gelöst werden musste, ist jedoch die unterschiedliche Methodik der Zitierweise in den beteiligten Disziplinen:

- in der Informatik erfolgen üblicherweise gröbere Bezüge zu verwendeten Literaturquellen, auf deren Grundlagen ein Abschnitt fußt – eine detaillierte Quellenangabe (mit Angabe aller exakten Seitenverweise) ist daher eher unüblich
- in Jura sind detaillierte Einzelnachweise dagegen geradezu gefordert – und in dessen Folge erhöhen sich die Anzahl der Fußnoten

Ziel dieser Arbeit war, dass auf ihr auch rechtswissenschaftlich aufgebaut werden kann. Insofern wurde bei den zugrunde liegenden Quellen eine Reduktion auf das Grundlegende und besonders Aussagekräftige vorgenommen. Die Zitierweise der Literaturangaben entspricht dem aktuellen Standard in der Informatik.

Da sich gerade im Themenkomplex dieser Arbeit die Rechtsgrundlagen aktuell relativ häufig ändern, wurden hier Änderungen von Gesetzen und Verordnungen nur bis zum 1. Oktober 2002 berücksichtigt.

Struktur der Arbeit

Diese Arbeit gliedert sich in vier Hauptteile: Im ersten wird die Konzeption des Datenschutzrechts dargestellt, im zweiten das Verhältnis zwischen Datenschutzrecht und Wissenschaftsfreiheit untersucht und im dritten spezielle Aspekte beim datenschutzkonformen Umgang in einer baden-württembergischen Universität anhand der Bereiche Forschung, Lehre, Technik und Verwaltung dargestellt, soweit es sich um hochschul-spezifische Belange handelt; im vierten Teil wird der datenschutzkonforme Umgang schließlich in Form einer Richtlinie anhand von

Fallbeispielen aufbereitet, um den universitären Alltag hinsichtlich des Datenschutzes erleichtern zu können.

Adressat dieser Arbeit ist die Daten verarbeitende Stelle innerhalb einer Universität, also nicht die Personen, die von der Datenverarbeitung betroffen sind. Gleichwohl liefert diese Arbeit auch für die Betroffenen wichtige Hinweise, welcher Umgang mit ihren Daten zulässig ist.

Wird im vorliegenden Dokument von Personen nur in der männlichen Form gesprochen, so gilt dies auch für weibliche Personen.

Diese Veröffentlichung ist die verbesserte Version der Diplomarbeit über „Datenschutz im Hochschulwesen in Baden-Württemberg“ des Autors an der Universität Ulm.

Danksagungen

Schließlich soll nicht unerwähnt bleiben, dass eine solche Arbeit nur dann erfolgreich angefertigt werden kann, wenn sich der Autor der Unterstützung durch Andere sicher sein kann. In diesem Falle möchte ich deshalb folgenden Personen besonders danken:

- Heinrich R. Staack (Dezernat IV Finanzen der Universität Ulm) für die Anregung, mich mit diesem Thema näher zu befassen,
- Dr. Gisela Menger (Abteilung Rechnerstrukturen an der Fakultät für Informatik an der Universität Ulm) für das Überlassen einer Einführung in die Jurisprudenz, die mir beim Verständnis rechtswissenschaftlicher Ansätze sehr geholfen hat,
- Birgit Tümmers, Christiane Westhauser (beide Dezernat II Studium und Lehre der Universität Ulm) und Rainer Marxmeier (Dezernat III Personal und Recht der Universität Ulm) für die geduldige Beantwortung meiner Fragen zur Themeneingrenzung,
- Werner Schneider (ehemaliger Landesbeauftragter für den Datenschutz Baden-Württemberg) für die Bereitstellung zahlreicher Informationsmaterialien,
- Prof. Dr. Gerhard Kongehl (Professor für Datenschutz, Datensicherheit und Technikfolgenabschätzung an der Fachhochschule Ulm) für die Bereitschaft, als Zweitgutachter der dieser Veröffentlichung zugrunde liegenden Diplomarbeit zur Verfügung zu stehen, und die Vorschläge der zu behandelnden Themen,
- Prof. Dr. Michael Weber (Abteilung Medieninformatik an der Fakultät für Informatik an der Universität Ulm) für die

Bereitschaft, die dieser Veröffentlichung zugrunde liegenden Diplomarbeit auszugeben, als Erstgutachter zu fungieren und der fruchtbaren Zusammenarbeit bei der Festsetzung der Aufgabenstellung,

- Dr. Wolfram Gass (Honorarprofessor für Medienrecht an der Fakultät für Informatik an der Universität Ulm) für die Bereitstellung nützlicher Informationsmaterialien, hilfreicher Anregungen und vor allem die Durchsicht der Arbeit auf juristische Stimmigkeit,
- dem Betreuer der dieser Veröffentlichung zugrunde liegenden Diplomarbeit Martin Gumhold (Abteilung Medieninformatik an der Fakultät für Informatik an der Universität Ulm) für die organisatorische Unterstützung, viele nützliche Hinweise und wertvolles Feedback
- der Agentur ENORM für die zahlreichen Vorschläge zur Gestaltung der Veröffentlichung,
- Frau Gisela Steinfurth vom Verlag LegArtis für die Betreuung der Veröffentlichung durch den Verlag,
- Götz A. Maier, Rechtsanwälte Gass & Partner, für die fleißige Umsetzung der Gestaltungs- und Änderungswünsche in der Schlussphase der Veröffentlichung,
- und ganz besonders Rebecca für konstruktive Kritik, Geduld und Nervenstärke (vor allem in der Schlussphase dieser Arbeit), sowie für die kreative Beratung bei der Erstellung der Grafiken.

1. Konzeption des Datenschutzrechts

1.1 Hintergründe zur Etablierung des Datenschutzrechts in der Bundesrepublik und seine Funktion

1.1.1 Über die Anfänge des Datenschutzrechts

Mit dem Einzug der elektronischen Datenverarbeitung nahm zugleich die Sensibilisierung in Fragen des Umgangs mit personenbezogenen Daten zu: In der Bundesrepublik Deutschland ist das Datenschutzrecht ursprünglich im Wesentlichen durch die amerikanische Debatte um das „Recht auf Privatheit“ (privacy) sowie den Mikrozensus-Beschluss des Bundesverfassungsgerichts vom 16.07.1969 motiviert[1] – dies ist insbesondere maßgeblich bei der Verabschiedung des bundesweit ersten, hessischen Datenschutzgesetzes im Jahre 1970 gewesen. Im ausschlaggebenden Urteil des obersten Gerichtes heißt es[2]: „Mit der Menschenwürde wäre es nicht zu vereinbaren, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung“. Dies könnte sonst zu einem teilweisen bis zu einem weitgehend vollständigen Persönlichkeitsprofil von Betroffenen führen, das entlang einer zeitlichen Entwicklung (Langzeitprofil) oder als sektorenübergreifende Blitzaufnahme (Querschnittsprofil) systematisch zusammengefügt werden könnte[3].

Als wesentlicher Auslöser für die Debatte um das „Recht auf Privatheit“ kann in den USA die auf Kredit basierende Wirtschaft benannt werden[4], da die individuelle Kreditwürdigkeit zu den obersten sozialen Werten zählt, es in den 60er Jahren vermehrt zu Computerfehlern in diesem sensiblen Bereich gekommen und die Errichtung einer nationalen Datenbank zur Erfassung aller verfügbaren Informationen über die Bürgerinnen und Bürger geplant war. Allerdings sicherte in den USA erst 1974 der „Privacy Act“ den Betroffenen diverse Rechte in Datenschutz-Fragen zu und verbot eine Zweckentfremdung von Personendaten[5].

---

1 so [Brennecke2001], S. 6.

2 zitiert nach [Bergmann2002], S. 5 im Teil I, 2. Teil – das Originalzitat findet sich in BVerfGE 27, 1 [6].

3 so Thilo Weichert in [Kilian2002], S. 8, Rn 35 im Teil 13, Kapitel 130 über die "Verfassungsrechtlichen Grundlagen des Datenschutzes“.

4 nach [Tinnefeld1994], S. 14.

5 so [Tinnefeld1994], S. 16.

1.1.2 Datenschutzrecht als Abwehrrecht

Nach Ansicht des langjährigen Datenschutzbeauftragten Hessens, Spiros Simitis[6], ist der Datenschutz „immer und zugleich Gradmesser der Bereitschaft und Fähigkeit einer Gesellschaft, die Grundrechte der einzelnen zu respektieren und ihre Partizipationschancen zu garantieren."

Ein Grundrecht kann verschiedene Ausprägungen haben[7]. Es wird unterschieden zwischen einem:

- klassischen Freiheitsrecht (*status negativus*),
- Beteiligungsrecht (*status aktivus*) und
- Leistungsrecht (*status positivus*).

Die meisten Grundrechte sind in erster Linie als Individualrechte (und insofern auch garantierte Minderheitenrechte[8]) zur ersten Kategorie zu zählen und folglich als Abwehrrechte des Einzelnen gegenüber dem Staat und der öffentlichen Gewalt entstanden[9].

Insofern liegt die maßgebliche Ursache für das bundesrepublikanische Datenschutzrecht also in der Abwehr gegen staatliche Eingriffe in individuelle Interessen, während es im nicht-öffentlichen Bereich erst durch die EG-Datenschutzrichtlinie von 1995 ein aussagekräftigeres Korsett bekam: Ausgehend vom Widerstand gegen das Volkszählungsgesetz vom März 1982 befasste sich das Bundesverfassungsgericht (BVerfG) eingehender mit dem Datenschutz – nach eigener Darstellung sah es sich hierzu förmlich genötigt[10].

Das dabei zu lösende Problem war so wichtig, dass der übliche Instanzenweg umgangen wurde[11]. Zugleich wurde damit das Procedere zur Manifestation der herrschenden juristischen Meinung stark abgekürzt – mit dem ansonsten eher längerfristigen Instanzenweg soll dagegen der juristischen Fachdiskussion mehr Zeit zur Entfaltung eingeräumt werden[12].

Direkte Verfassungsbeschwerden werden vom Bundesverfassungsgericht nur akzeptiert[13], wenn der Beschwerdeführer durch diese Bestimmung selbst, gegenwär-

---

6 siehe [Simitis1998], S. 2473.
7 siehe [Kimminich1996a], S. 123
8 gemäß [Kimminich1996a], S. 125.
9 so [Bergmann2002], S. 4 im Teil I, Systematische Darstellung des Datenschutzrechts, Ziffer 2.3.2.
10 "Da (...) nur eine lückenhafte verfassungsgerichtliche Rechtsprechung bestand, nötigen die zahlreichen Verfassungsbeschwerden gegen das Volkszählungsgesetz 1983 das Bundesverfassungsgericht, die verfassungsrechtlichen Grundlagen des Datenschutzes umfassender zu prüfen." (BVerfGE 65, 1 [4])
11 siehe [Wesel1992], S. 52ff
12 siehe auch [Wesel1992], S. 28f.
13 gemäß BVerfGE 65, 1 [36ff].

tig und unmittelbar in seinen Grundrechten betroffen ist und das Gesetz bereits gegenwärtig zu später nicht mehr korrigierbaren Entscheidungen zwingt.

1.2 Auszüge aus dem Grundrechts-Urteil zum Informationellen Selbstbestimmungsrecht

1.2.1 Wesentliche Gründe für den Datenschutz

Das Bundesverfassungsgericht stellt in der Urteilsbegründung zum Volkszählungsgesetz fest[14], dass die „Möglichkeiten der modernen Datenverarbeitung (...) weithin nur noch für Fachleute durchschaubar (sind) und (...) beim Staatsbürger die Furcht vor einer unkontrollierbaren Persönlichkeitserfassung (...) auslösen (können)".

Dabei führte es weiter aus[15]: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. (...) Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. (...) Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus."

Als Prüfungsmaßstab für das informationelle Selbstbestimmungsrecht hat das Bundesverfassungsgericht im Volkszählungsurteil das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 GG, „Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt", in Verbindung mit Art. 1 Abs. 1 GG, „Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt") bestimmt[16]: „Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt. (...) Es umfasst (...) auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzel-

[14] zitiert aus BVerfGE 65, 1 [4].
[15] zitiert aus BVerfGE 65, 1 [43].
[16] zitiert aus BVerfGE 65, 1 [41f].

nen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden".

Seit dem Quellensteuerurteil[17] vom 27.06.1991 des Bundesverfassungsgerichts wird anstelle eines „Rechts auf informationelle Selbstbestimmung" auch von einem „Grundrecht auf Datenschutz" gesprochen.

1.2.2 Einschränkungen des Rechts auf informationelle Selbstbestimmung

Das Bundesverfassungsgericht bemisst dem informationellen Selbstbestimmungsrecht zwar einen hohen Stellenwert bei, doch hielt es im Volkszählungsurteil ausdrücklich fest[18], dass dieses Recht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet ist: „Der Einzelne (...) ist (...) eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. (...) Grundsätzlich muss daher der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen. Diese Beschränkungen bedürfen (...) einer (verfassungsmäßigen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben (...). Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. (...) Erst wenn Klarheit darüber besteht, zu welchem Zweck Angaben verlangt werden und welche Verknüpfungs- und Verwendungsmöglichkeiten bestehen, lässt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten."

Und das Gericht stellt schließlich klar[19]: „Ein Zwang zur Angabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind. (...) Auch werden sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken müssen. (...) Bei der Datenerhebung für statistische Zwecke kann eine enge und konkrete Zweckbindung der Daten nicht verlangt werden. (...) Ist die Vielfalt der Verwendungs- und Verknüpfungsmöglichkeiten damit bei der Statistik von der Natur der Sache her nicht im voraus bestimmbar, müssen der Informationserhebung und -verarbeitung innerhalb des Informationssystems zum Ausgleich entsprechende Schranken gegenüberstehen. (...) Zur Sicherung des Rechts auf informationelle Selbstbestimmung bedarf es ferner besonderer Vorkehrungen für Durchführung und Organisation der Datenerhebung und -verarbeitung, da die Informationen während der Phase der Erhebung – und zum Teil auch während der Speicherung – noch individualisierbar sind".

---

17 siehe [Bergmann2002], S. 4 im Teil I, Ziffer 2.3.1 bzw. BVerfGE 84, 239 [280].
18 zitiert aus BVerfGE 65, 1 [43ff].
19 zitiert aus BVerfGE 65, 1 [46ff].

1.3 Der Kern des Datenschutzrechts

1.3.1 Grundsätze des Datenschutzrechts

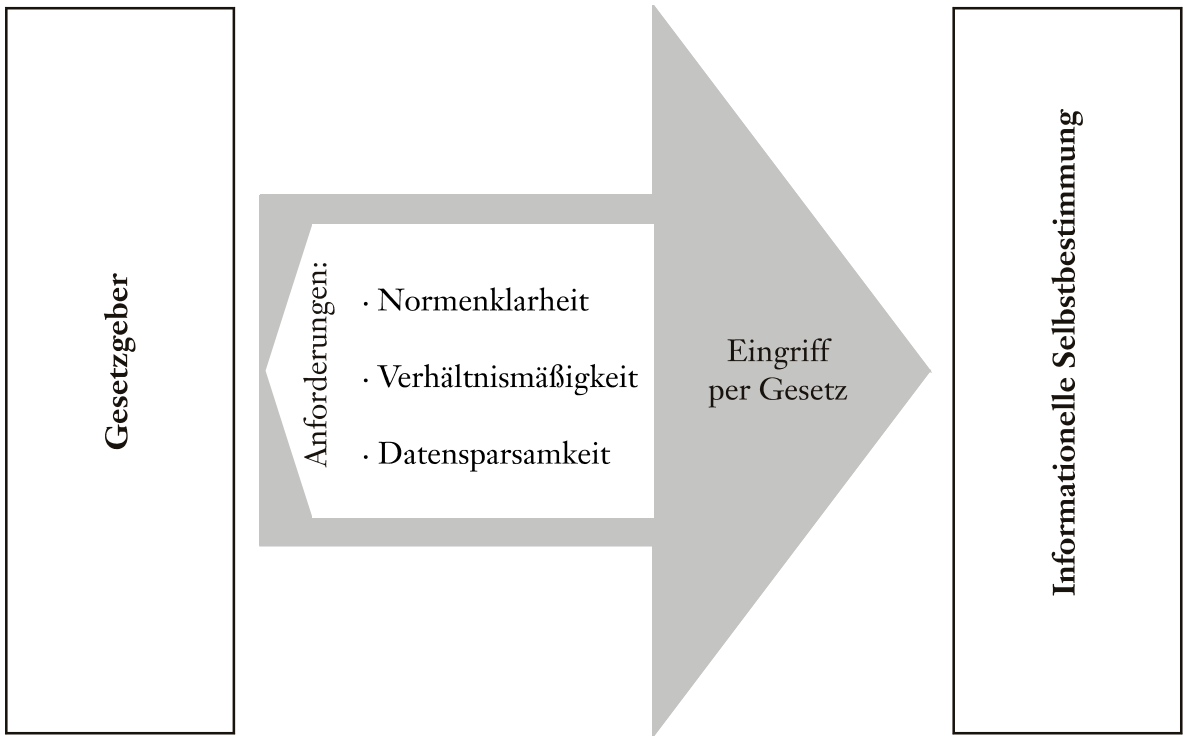
Jede Person darf also grundsätzlich selbst über die Preisgabe und Verwendung ihrer persönlichen Daten bestimmen. Dieses Grundrecht wird „informationelle Selbstbestimmung“ genannt. Hierin darf nur auf der Grundlage einer Rechtsvorschrift im überwiegenden Allgemeininteresse (und dies erfordert in jedem Falle eine verfassungskonforme gesetzliche Regelung) eingegriffen werden (so genannter „Gesetzesvorbehalt“[20]).

Die zugrunde liegende Rechtsvorschrift unterliegt schließlich folgenden Einschränkungen:

- der Verwendungszweck ist bereichsspezifisch und präzise zu bestimmen (Normenklarheitsprinzip)
- die Angaben personenbezogener Daten muss für den Zweck geeignet und erforderlich sein (Verhältnismäßigkeitsprinzip)
- es sind nur so viele Daten zu erheben, wie unbedingt benötigt werden (Grundsatz der Datensparsamkeit)

Dieser Kern ergibt sich unmittelbar aus dem Grundgesetz und ist daher stets zu beachten.

Abb. 1 Anforderungen an Eingriffe ins informationelle Selbstbestimmungsrecht



[20] siehe [Wesel1992], S. 254.

Anmerkung

In der Literatur wird anstelle des Verhältnismäßigkeitsprinzips z.T. die Bezeichnung „Übermaßverbot“ verwendet und dafür die Zweckbindung, Eignung und Erforderlichkeit jeweils zu eigenen Prinzipien erhoben. Die hier gewählte Aufteilung orientiert sich stärker am direkten Wortlaut des zugrunde liegenden BVerfG-Urteils. Aus der Normenklarheit ergibt sich auch der oftmals genannte Grundsatz der Transparenz, der Ausgangspunkt für die Kontrolle des Eingriffs (durch Datenschutzbeauftragte ausgehend von Betroffenenrechten) ist. Die meisten Darstellungen zu diesem Thema klammern bedauerlicherweise den Grundsatz der Datensparsamkeit in einer solchen Übersicht aus (die Datensparsamkeit wird dabei i.d.R. nur als besonderer Aspekt der Verhältnismäßigkeit – als Unterpunkt der Erforderlichkeit – aufgeführt), obwohl er spätestens nach der EG-Datenschutzrichtlinie erneut an Bedeutung gewonnen hat. Außerdem hat auf diesen Grundsatz schon das Bundesverfassungsgericht beim Volkszählungsurteil ausdrücklich hingewiesen, wie weiter oben bereits ausgeführt wurde.

1.3.2 Unterscheidung Datenschutz und Datensicherheit

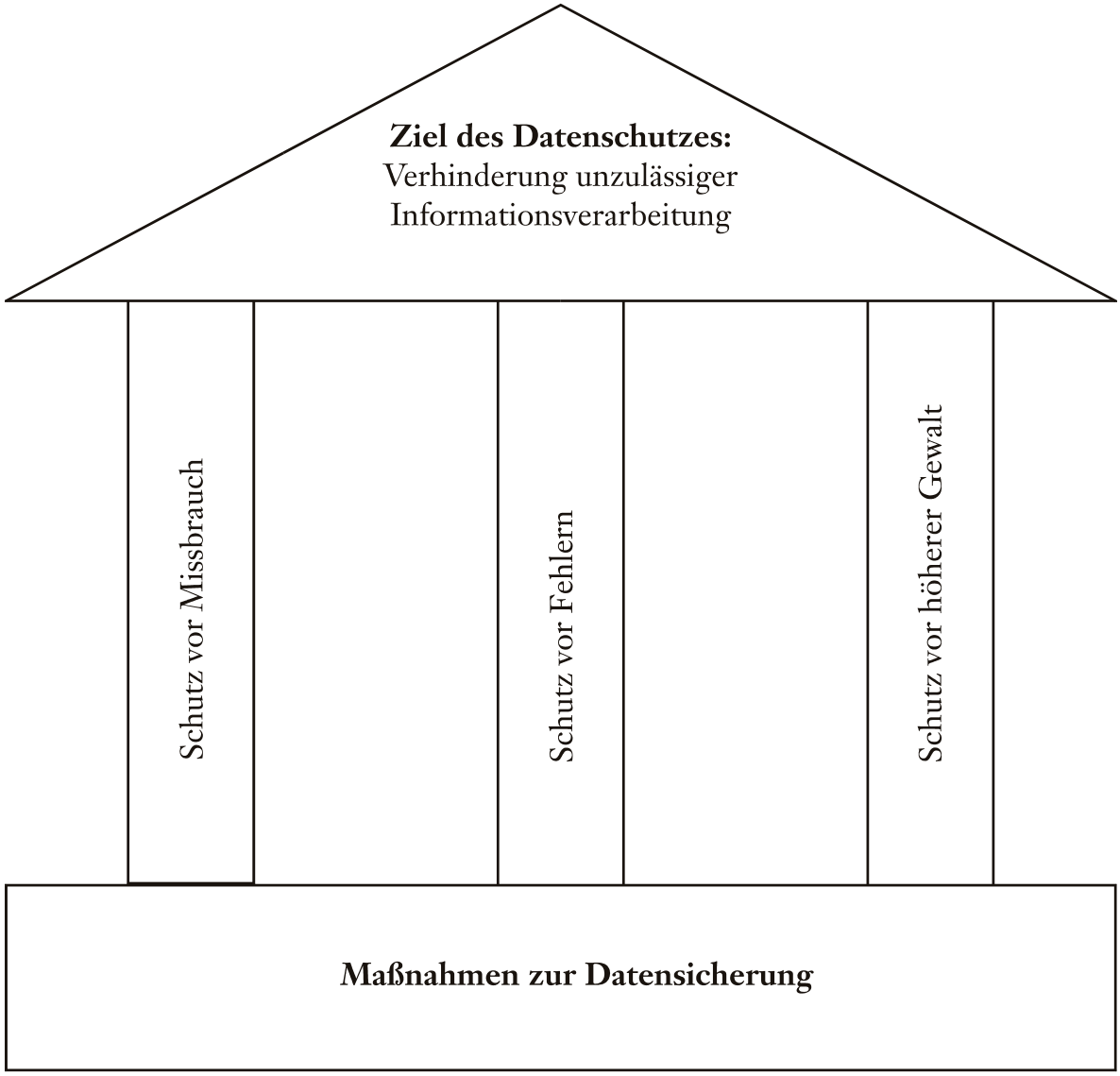
Der Begriff „Datenschutz“ wird häufig in vielerlei Nuancen und Bedeutungen verwendet. Diese Arbeit basiert auf den Definitionen von Bergmann, Möhrle und Herb[21]:

"Der Datenschutz hat das Ziel, jeden einzelnen Menschen vor den Gefahren beim Umgang mit personenbezogenen Daten zu schützen (...). Jeder Einzelne soll in der Regel selbst bestimmen, welche Daten er zur Verwendung preisgibt. (...) Datenschutz ist also die Menge aller Vorkehrungen zur Verhinderung unzulässiger Informationsverarbeitung“.

"Damit der Datenschutz als rechtliches Ziel erreicht werden kann, sind technische und organisatorische Maßnahmen erforderlich. Sie werden mit den Begriffen Datensicherung und Datensicherheit umschrieben. (...) Unter Datensicherung werden also alle Maßnahmen zur Erhaltung und Sicherung des gesamten DV-Systems und zum Schutz der Daten, Datenträger, DV-Anlagen und Programme vor Fehlern, Missbrauch und höherer Gewalt verstanden.“

[21] zitiert nach [Bergmann2002], S. 16f im Teil I, Ziffer 2.6.1 und 2.6.2.

Abb. 2 Verhältnis zwischen Datenschutz und Datensicherheit



1.4 Struktur des Datenschutzrechts

1.4.1 Aufgaben des Datenschutzes

Aufgabe des Datenschutzes ist der Schutz der personenbezogenen Daten vor Missbrauch durch Datenverarbeitung[22]. Quasi gleich lautende Formulierungen finden sich daher auch in allen Datenschutzgesetzen. Das Bundesverfassungsgericht hat hierzu festgehalten[23], dass das Recht auf informationelle Selbstbestimmung generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten schützt und nicht auf den jeweiligen Anwendungsbereich des Bun-

[22] siehe [Bergmann2002], S. 3 im Teil V, Überblick, Ziffer 1.1.

[23] zitiert nach [Bergmann2002], S. 1 im Teil V, Kommentar zu § 1 LDSG mit Verweis auf einen Beschluss des BVerfG vom 09.03.1988.

desdatenschutzgesetzes (BDSG), der Datenschutzgesetze der Länder oder datenschutzrelevanter gesetzlicher Sonderregelungen beschränkt ist.

1.4.2 Die Geltungsebenen im Datenschutzrecht

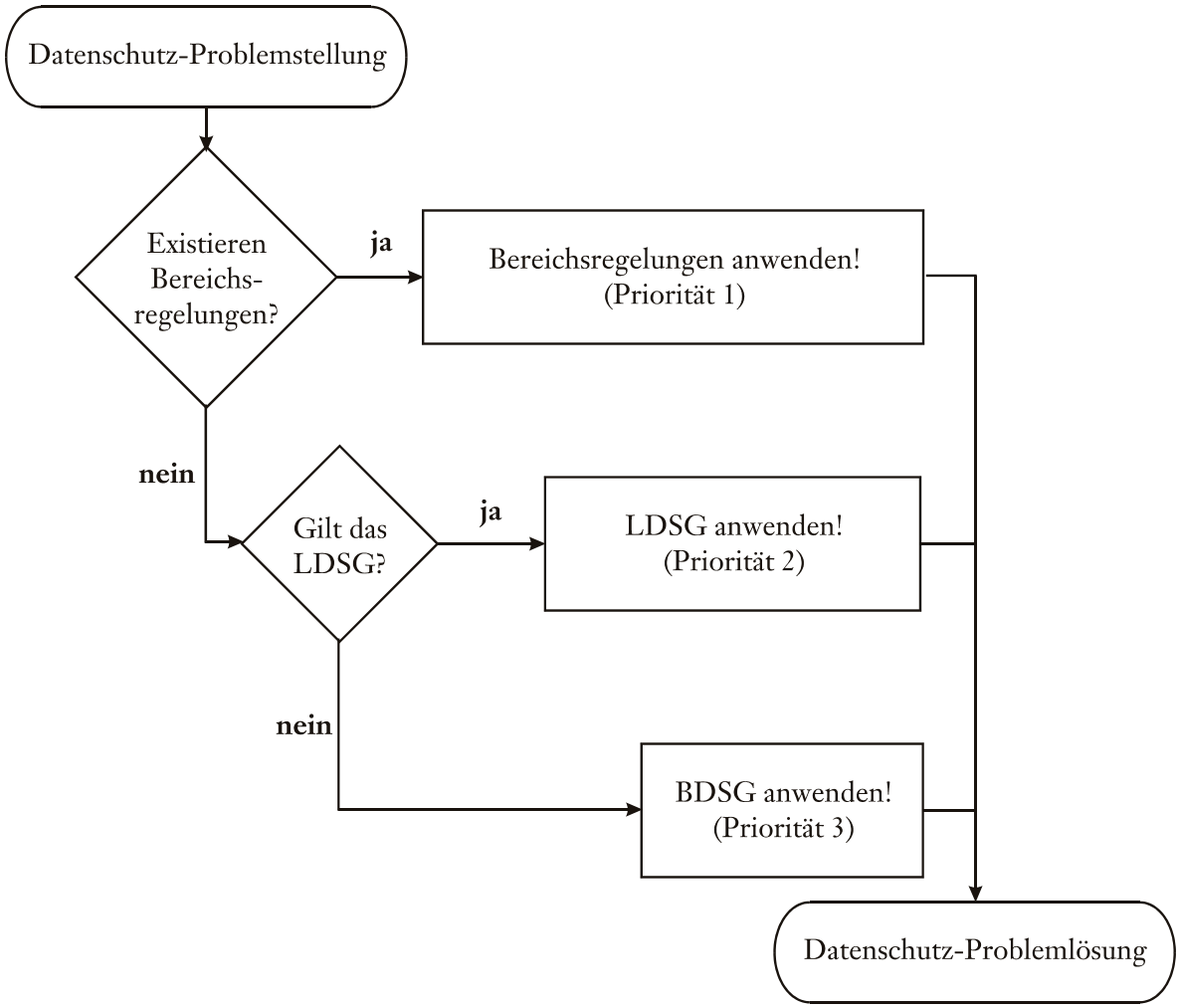
Das Datenschutzrecht hat sich nach Bergmann, Möhrle und Herb[24] „insbesondere im öffentlichen Bereich 'verselbständigt', d.h. vom BDSG abgekoppelt". Es könne sogar von einer „Aushöhlung des BDSG" gesprochen werden[25]. Alleine die Auflistung der wesentlichen bereichsspezifischen Regelungen umfasst daher gleich mehrere Seiten. Die Autoren folgern schließlich[26], dass „das BDSG in den Ländern grundsätzlich nicht mehr gilt".

Grundsätzlich ist das Datenschutzrecht anzuwenden, das am Sitz der personenbezogenen Daten verantwortlich verarbeitenden Stelle gilt (so genanntes „Sitzprinzip")[27]. Bei einem vorliegenden Fall ist anschließend stets zuerst zu prüfen, ob datenschutzrelevante Bereichsregelungen („lex specialis") existieren (im Falle der Hochschulen siehe hierzu insbesondere Kapitel 2.4), die vorrangig anzuwenden sind. Danach ist im Regelfall das Landesdatenschutzgesetz (LDSG) die anzuwendende Rechtsvorschrift und erst, wenn dieses Gesetz nicht greift, ist das Bundesdatenschutzgesetz (BDSG) maßgeblich.

---

[24] zitiert aus [Bergmann2002], S. 1 im Teil I, Ziffer 4.1.1.
[25] zitiert aus [Bergmann2002], S. 1 im Teil I, Ziffer 4.1.2.
[26] zitiert aus [Bergmann2002], S. 22 im Teil I, Ziffer 4.3.
[27] siehe [Blömer2002], S. 203.

Abb. 3 Schema zur Bestimmung des anzuwendenden Datenschutzrechts



1.4.3 Allgemein geltende Regelungen im Datenschutzrecht

Einige Regelungen finden sich fast wortidentisch in allen Datenschutzgesetzen, so dass hier von einem einheitlichen Recht gesprochen werden kann[28]. Zu nennen sind:

- die Bestimmung wichtiger Begriffe in den Datenschutzgesetzen (siehe hierzu insbesondere § 3 BDSG bzw. § 3 LDSG),
- die Zulässigkeit der Datenverarbeitung aufgrund einer Rechtsgrundlage oder der (freiwillig gegebenen) Einwilligung des Betroffenen (siehe hierzu insbesondere § 4 BDSG bzw. § 4 LDSG),
- die Wahrung des im Beschäftigungsverhältnis erworbenen Datengeheimnisses auch über das Beschäftigungsverhältnis

[28] siehe [Bergmann2002], S. 4ff im Teil V, Ziffer 1.2, 1.3 und 1.5 im Überblick, sowie in den Kommentierungen zu den jeweiligen Paragraphen.

hinaus (siehe hierzu insbesondere § 5 BDSG bzw. § 6 LDSG),
- die Rechte des Betroffenen auf Auskunft, Berichtigung, Löschung oder Sperrung (siehe hierzu insbesondere § 6 BDSG bzw. § 5 LDSG),
- der Grundsatz der Primärerhebung beim Betroffenen (siehe hierzu insbesondere § 13 BDSG bzw. § 13 LDSG),
- der Grundsatz der Zweckbindung der Daten (siehe hierzu insbesondere § 14 BDSG bzw. § 15 LDSG),
- der Grundsatz der Datensparsamkeit (siehe hierzu insbesondere § 3a BDSG bzw. § 9 Abs. 1 LDSG),
- die Kontrolle der Einhaltung datenschutzrelevanter Vorschriften durch einen unabhängigen Datenschutzbeauftragten (siehe hierzu insbesondere die §§ 4f und 4g BDSG bzw. § 10 LDSG).

Der Datenschutz ist irrelevant, wenn explizit keine personenbezogenen Daten verarbeitet werden. Personenbezogene Daten sind (gemäß ihrer Definition in § 3 Abs. 1 LDSG) Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Wenn eine Re-Identifikation nur mit unverhältnismäßigem Aufwand möglich ist (siehe auch § 3 Abs. 6 LDSG bzw. § 3 Abs. 6 BDSG)[29], sind die Daten (faktisch) anonymisiert und eine uneingeschränkte Verarbeitung zulässig[30].

Zum Volkszählungsgesetz 1987 hielt das Bundesverfassungsgericht in einem Kammerbeschluss fest[31]: „Von Verfassungs wegen ist lediglich eine faktische Anonymität der Daten geboten. Diese kann – in Anlehnung an § 16 Abs. 6 BStatG – allenfalls dann als gegeben angesehen werden, wenn Datenempfänger oder Dritte eine Angabe nur mit einem – im Verhältnis zum Wert der zu erlangenden Information nicht zu erwartenden – unverhältnismäßig großen Aufwand an Zeit, Kosten, Arbeitskraft und sonstigen Ressourcen (etwa das Risiko einer Bestrafung) einer Person zuordnen können".

---

[29] in [Bergmann2002], S. 21f im Teil III, Ziffer 18 im Kommentar zu § 3 BDSG, Rn 128ff.

[30] siehe hierzu exemplarisch H.-Erich Wichmann in [Hamm1999], S. 55.

[31] zitiert nach [Bizer1992], S. 153.

1.5 Wichtige Bestimmungen im Landesdatenschutzgesetz Baden-Württemberg

1.5.1 Anwendungsbereich und Verarbeitungsgrundsätze

Das Landesdatenschutzgesetz ist grundsätzlich auch auf Hochschulen anzuwenden[32], da diese als „sonstige öffentliche Stelle“ im Sinne von § 2 Abs. 1 LDSG anzusehen sind. Vorrang vor dem LDSG haben aber Gesetze (wie z.B. das Universitätsgesetz), Verordnungen und Satzungen, in denen entsprechende bereichsspezifische Regelungen (z.B. über die Zulässigkeit der Speicherung personenbezogener Daten) enthalten sind. Fehlen darin Regelungen (z.B. über Auskunftspflichten), so kommt wiederum das LDSG zum Zuge. Das bedeutet, dass jede Regelung, die vom LDSG abweichen soll, explizit aufgeführt sein muss.

Personenbezogene Daten dürfen nur verarbeitet werden, wenn der Betroffene eingewilligt hat oder eine Rechtsvorschrift dieses ausdrücklich erlaubt (§ 4 Abs. 1 LDSG). Zur Verarbeitung zählen das Erheben, Speichern, Verändern, Übermitteln, Nutzen, Sperren und Löschen der Daten (§ 3 Abs. 2 LDSG). Selbst gegen eine rechtmäßige Datenverarbeitung hat ein Betroffener ein Einwendungsrecht, das nur dann zurückgewiesen werden darf, wenn eine Abwägung ergeben hat, dass das öffentliche Interesse an der Verarbeitung überwiegt (§ 4 Abs. 6 LDSG).

Obgleich im LDSG die Datenverarbeitung eindeutig (und umfassend) definiert ist, wird in anderen Gesetzen z.T. wiederum in Erheben, Verarbeiten und Veröffentlichen unterschieden. Es wird daher davon ausgegangen, dass die Erhebung einerseits und die Veröffentlichung andererseits besonders schwere Eingriffe in das informationelle Selbstbestimmungsrecht der Betroffenen darstellen.

1.5.2 Die Rechte des Betroffenen

Niemand, sei er nun Betroffener oder Bediensteter, darf wegen der Geltendmachung seiner Rechte benachteiligt werden[33]. Etwaige Ansprüche werden stets gegen die „verantwortende Stelle“ im Sinne von § 3 Abs. 3 LDSG geltend gemacht, also gegenüber der Stelle, die personenbezogene Daten für sich selbst verarbeitet oder durch andere im Auftrag verarbeiten lässt, denn Auftragnehmer sind bei der Datenverarbeitung an die Weisungen der Auftraggeber gebunden[34].

Betroffene verfügen über:

- das Recht auf Auskunft über die zu seiner Person gespeicherten Daten (ausführlicher in § 21 LDSG), das nur bei der

---

[32] siehe hierzu die Ausführungen in [Bergmann2002], S. 2 und S. 5 des Kommentars zu § 2 LDSG.

[33] darauf verweist [Bergmann2002], S. 2, Ziffer 2.3 im Kommentar zu § 5 LDSG.

[34] siehe Thilo Weichert in [Kilian2002], S. 11, Rn 42 im Teil 13, Kapitel 131 über "Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes“.

Übermittlung an Sicherheitsbehörden, der Justiz und der Finanzverwaltung eingeschränkt ist – das Auskunftsrecht ist grundlegend für die Nutzbarkeit der anderen Rechte[35],
- das Recht auf Berichtigung, Löschung bzw. Sperrung unrichtiger oder unzulässiger bzw. nicht mehr erforderlicher Daten (ausführlicher in den §§ 22 bis 24 LDSG),
- das Recht auf Auskunft aus dem vom behördlichen Datenschutzbeauftragten zu führenden Verfahrensverzeichnis, in dem alle automatisierten Datenverarbeitungsverfahren aufzuführen sind – darin ist insbesondere die Grundlage für die Verarbeitung und die Zweckbestimmung zu benennen (detailliertere Angaben in § 11 LDSG),
- das Recht auf Einwendung bei begründet schutzwürdigen Interessen gegen eine Verarbeitung (§ 4 Abs. 6 LDSG),
- das Recht auf Schadensersatz bei schweren Verstößen gegen das LDSG, wobei die verantwortende Stelle nachzuweisen hat, ob der Schaden nicht von ihr zu vertreten ist (§ 25 LDSG),
- das Recht auf Anrufung des Landesdatenschutzbeauftragten (§ 27 LDSG).

Die verfahrensrechtlichen Schutzvorkehrungen (Aufklärungs-, Auskunfts- und Löschungsvorschriften) kommen in jedem Falle zum Zuge, da sie auf der Grundlage der geltenden Verfassungsauslegung zwingend zu gewähren sind[36]. Gleiches gilt für die Beteiligung unabhängiger Datenschutzbeauftragter[37], deren Aufgaben, soweit es sich um behördliche Datenschutzbeauftragte handelt, darin liegen, auf die Einhaltung der Datenschutzvorschriften hinzuwirken, für Datenschutzregelungen zu sensibilisieren und ein Verfahrensverzeichnis zu führen (§ 10 Abs. 4 LDSG). Ist kein behördlicher Datenschutzbeauftragter benannt, nimmt dessen Aufgaben der Landesdatenschutzbeauftragte wahr, wie sich u.a. aus den §§ 12, 28 und 32 Abs. 1 LDSG im Vergleich zu § 10 Abs. 4 LDSG ergibt.

1.5.3 Maßnahmen zur Datensicherheit

Grundsätzlich ist darauf zu achten, dass möglichst wenig personenbezogene Daten verarbeitet werden (§ 9 Abs. 1 LDSG). Im zugrunde liegenden Paragraphen werden die wesentlichen Maßnahmen zur Datensicherheit aufgeführt. Die verantwortliche Stelle hat (nach § 9 Abs. 3 LDSG) also dafür zu sorgen, dass:

---

35 und wird deshalb von Thilo Weichert in [Kilian2002], S. 2, Rn 5 im Teil 13, Kapitel 133 über "Betroffenenrechte" als "Magna Charta" des Rechts auf informationelle Selbstbestimmung bezeichnet.

36 siehe [Bergmann2002], S. 4, Ziffer 8.1 im Kommentar zu § 5 LDSG bzw. BVerfGE 65, 1 [46].

37 siehe ebenfalls BVerfGE 65, 1 [46].

- Unbefugte keinen Zutritt zu den DV-Anlagen erhalten,
- Daten nicht durch Unbefugte eingegeben, gelesen, verändert oder gelöscht werden dürfen,
- Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können,
- DV-Systeme nicht bei der Datenübertragung durch Unbefugte benutzt werden können,
- bei der Datenübertragung und dem Datenträgertransport nicht Unbefugte Daten lesen, kopieren, verändern oder löschen können,
- Zugriffsberechtigte nur auf die ihrer Berechtigung unterliegenden Daten zugreifen können,
- überprüft und festgestellt werden kann, an wen Daten übermittelt wurden,
- auch nachträglich überprüft und festgestellt werden kann, wer wann welche Daten eingegeben hat,
- personenbezogene Daten gegen zufällige Zerstörungen oder Verlust geschützt sind,
- die Datenverarbeitung im Auftrag ebenfalls entsprechend der Weisungen der verantwortlichen Stelle unter Beachtung der Datenschutzbestimmungen erfolgt,
- die Organisationsstruktur der Verwaltung den Datenschutzbestimmungen gerecht wird.

1.5.4 Besonderheiten bei der Datenerhebung

Bei der Prüfung, ob die Datenerhebung erforderlich ist, ist ein strenger Maßstab anzulegen[38]. Im Vordergrund steht dabei nicht, wie die Daten am einfachsten erhoben werden könnten, sondern wie möglichst wenig Daten erhoben werden können[39]: Demnach dürfen nur die Daten erhoben werden, die zur Erfüllung einer konkreten, aktuellen Aufgabe benötigt werden. Datensammlungen auf Vorrat (soweit sie nicht den Rechtsvorschriften der Statistik-Erstellung unterliegen) sind folglich verboten. Eine Erhebung ist nur für einen konkreten und aktuellen Zweck zulässig.

Vom Grundsatz der Primärerhebung beim Betroffenen kann nur abgewichen werden, wenn eine ausdrücklich erlaubte Ausnahme vorliegt oder Daten aus allgemein zugänglichen Quellen entnommen werden[40]. Hierzu zählen insbesondere:

- Adress- und Telefonbücher
- öffentliche Register

---

38 so [Bergmann2002], S. 3, Ziffer 4.3 zum Kommentar zu § 13 LDSG.
39 dies erfordert BVerfGE 65, 1 [46f].
40 so [Bergmann2002], S. 4, Ziffer 5.1 zum Kommentar zu § 13 LDSG.

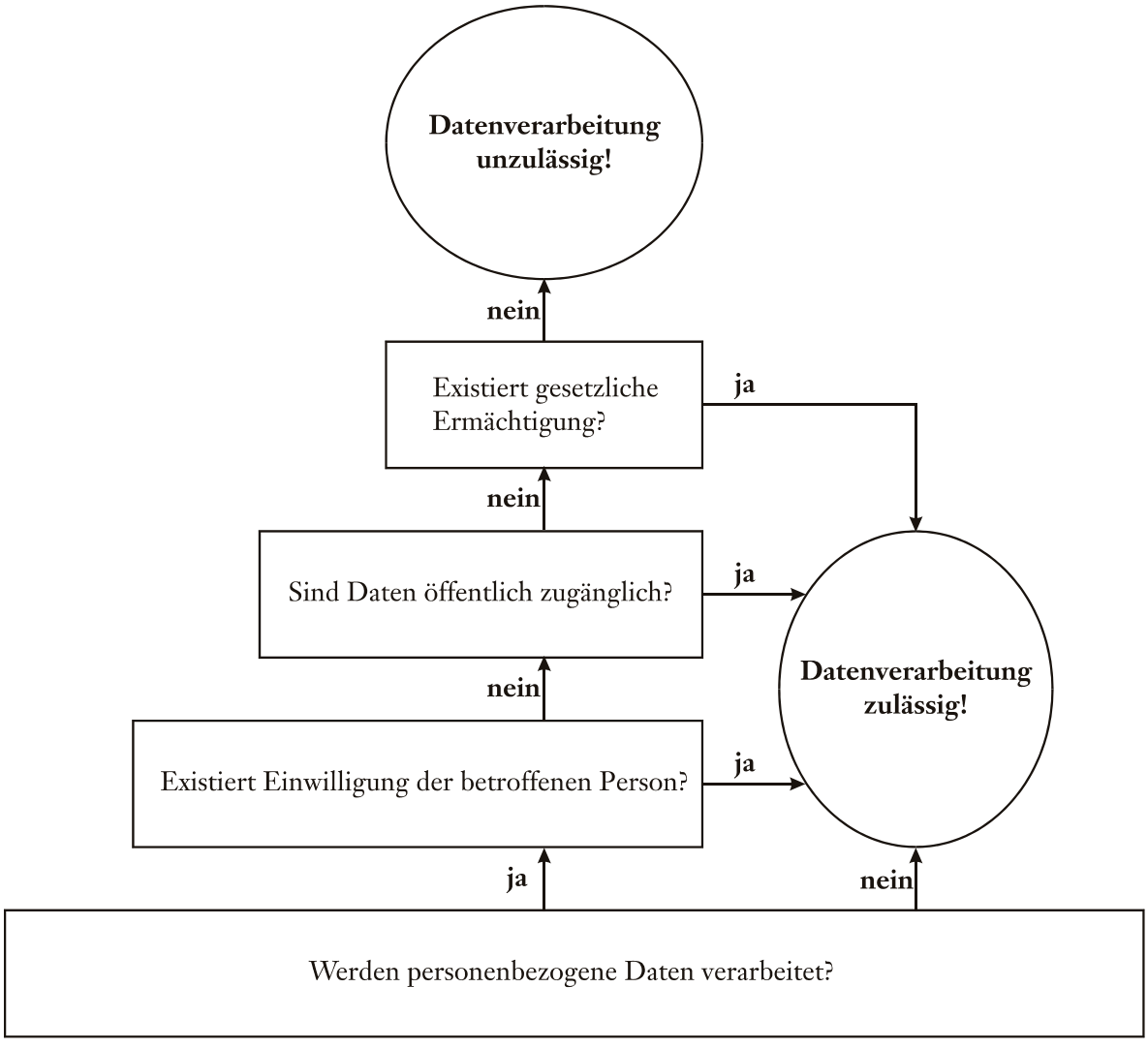
- Veröffentlichungen
- Internet

Jede erhebende Stelle hat daher zwingend zu prüfen, ob es möglich ist, die Daten vom Betroffenen selbst zu erhalten und ihm damit eine Mitwirkung an der Datenbeschaffung zu ermöglichen.

Eine Einwilligung des Betroffenen erfordert, dass der Betroffene (gemäß § 4 LDSG)

- über die beabsichtigte Datenverarbeitung, deren Zweck und etwaige Empfänger der Daten aufzuklären ist,
- über seine Rechte informiert wird (siehe Abschnitt 1.5.2) und insbesondere die Einwilligung verweigern oder widerrufen kann und
- seine Einwilligung zur Gültigkeit schriftlich erklären muss.

Abb. 4 Hierarchie für zulässige Datenverarbeitungen



2. Verhältnis zwischen Datenschutzrecht und Wissenschaftsfreiheit

2.1 Bedeutung und Umfang der Wissenschaftsfreiheit

2.1.1 Über die Anfänge der Wissenschaftsfreiheit

Wissenschaft kann, vereinfacht ausgedrückt, beschrieben werden als ein Suchen nach Wahrheit[41] mittels objektivierbarer und überprüfbarer Methoden[42]. Diese Aufgabe erfordert also insbesondere geistige Freiheit als notwendige Voraussetzung[43] und darf daher durch kein Dogma (religiöser wie weltlicher Natur) eingeschränkt werden.

Als wesentliches ideengeschichtliches Fundament für die Wissenschaftsfreiheit in der Bundesrepublik Deutschland kann neben der Universitätskonzeption Wilhelm von Humboldts[44] auch der gemeinsame Protest der sog. „Göttinger Sieben“ gegen eine vollzogene Verfassungsaufhebung[45] angesehen werden: Der Berliner Universität wurde die Wissenschaftsfreiheit bei ihrer Gründung (1809) gewährt[46] und nach den Unruhen des Vormärz schließlich (1850) verallgemeinert in die Preußische Verfassung integriert.

Der Staat blieb allerdings stets für organisatorische Fragen an den Universitäten zuständig, wie z.B. die Finanzausstattung[47] oder die Ernennung von Professoren, denen das Privileg der Wissenschaftsfreiheit in besonderer Weise anheim gestellt wurde. Den Hochschullehrern (das sind Professoren, wissenschaftliche Räte und Dozenten) ist aus Sicht des Bundesverfassungsgerichts[48] „die Pflege von Forschung und Lehre vornehmlich anvertraut“.

---

41 wobei ich in diesem Zusammenhang keine philosophische Diskussion über "Was ist Wahrheit?" anstoßen will, zumal es m.E. auch verschiedene Sichtweisen über Wahrheit geben kann.

42 in Anlehnung an die Definition über wissenschaftliche Tätigkeit in BVerfGE 35, 79 [113] und Gerd Roellecke in [Roellecke1996], S. 24 über die Motivation Humboldts zu seinen Reformen im Bildungswesen.

43 Thomas Oppermann bezeichnet dies als "die Erkenntnis aus den liberalen Traditionen des 19. Jahrhunderts, dass Bildung durch Wissenschaft nur in einem Klima geistiger Freiheit gedeihen kann" ([Oppermann1996], S. 1015) in Anlehnung an Hans Wenke, Die deutsche Hochschule vor den Ansprüchen unserer Zeit, Schriften des Hochschulverbandes Heft 7, 2. Auflage, 1964, S. 13.

44 siehe [Roellecke1996], S. 24.

45 siehe [Roellecke1996], S. 25.

46 laut [Oppermann1996], S. 1016 begann damit "eine neue Ära des deutschen Hochschulwesens“.

47 siehe [Knemeyer1996], S. 246.

48 gemäß BVerfGE 35, 79 [126].

2.1.2 Grundsätzliche Beziehung zwischen Wissenschaftsfreiheit und Universitäten

Das Grundgesetz gewährt in Art. 5 Abs. 3 GG die Wissenschaftsfreiheit („Kunst und Wissenschaft, Forschung und Lehre sind frei. Die Freiheit der Lehre entbindet nicht von der Treue zur Verfassung."). Für die Hochschulen hat aber nicht nur dieses Grundrecht eine zentrale Bedeutung, sondern auch Art. 12 Abs. 1 Satz 1 GG („Alle Deutschen haben das Recht, Beruf, Arbeitsplatz und Ausbildungsstätte frei zu wählen.") und Art. 20 Abs. 1 GG („Die Bundesrepublik Deutschland ist ein demokratischer und sozialer Bundesstaat.")[49]. Damit stellen diese Grundrechte nicht nur Abwehrrechte gegen staatliche Eingriffe dar[50], sondern zugleich auch Teilhaberechte[51] (siehe auch Abschnitt 1.1.2).

Die Wissenschaftsfreiheit schützt[52]

- den Prozess wissenschaftlicher Betätigung in Forschung und Lehre,
- die wissenschaftliche Erkenntnis als 'Objektivation' der Grundrechtsausübung von Forschungs- und Lehrfreiheit und
- die Verbreitung, Publikation bzw. sonstige, namentlich lehrmäßige Vermittlung wissenschaftlicher Erkenntnisse.

Die herrschende Meinung leitet aus der Wissenschaftsfreiheit zugleich eine Einrichtungsgarantie für Universitäten und deren akademische Selbstverwaltung ab[53]. Die Verfassung des Landes Baden-Württemberg gewährt wohl insbesondere deshalb ausdrücklich eine solche institutionelle Garantie in Art. 20; dort heißt es:

Abs. 1: „Die Hochschule ist frei in Forschung und Lehre."

Abs. 2: „Die Hochschule hat unbeschadet der staatlichen Aufsicht das Recht auf eine ihrem besonderen Charakter entsprechende Selbstverwaltung im Rahmen der Gesetze und ihrer staatlich anerkannten Satzungen."

Abs. 3: „Bei der Ergänzung des Lehrkörpers wirkt sie durch Ausübung ihres Vorschlagsrechts mit."

---

[49] Das Zusammenspiel dieser drei Verfassungsgrundsätze wird nach [Bethge2000], S. 1052, Rn 19 auch als "Magna Charta der Studierfreiheit" bezeichnet.

[50] hierauf weist das Bundesverfassungsgericht ausdrücklich hin (BVerfGE 35, 79 [112]).

[51] siehe exemplarisch hierzu [Kimminich1996a], S. 124 unter Berufung auf ein Urteil des Bundesverfassungsgerichts (Zitat im Original in BVerfGE 33, 303 [330f]).

[52] Auflistung aus [Kimminich1996a], S. 142 unter Berufung auf GG-Kommentatoren (Zitat bei Scholz in Maunz/Dürig/Herzog/Scholz, Kommentar zum Grundgesetz, Rn 83 zu Art. 5 Abs. 3).

[53] siehe u.a. [Kimminich1996a], S. 125f.

Grundsätzlich steht aufgrund Art. 70 Abs. 1 GG („Die Länder haben das Recht der Gesetzgebung, soweit dieses Grundgesetz nicht dem Bunde Gesetzgebungsbefugnisse verleiht.“) das Hochschulrecht den Ländern zu[54].

Eingeschränkt ist dieses Landesrecht insbesondere durch die ausschließliche Zuständigkeit[55] des Bundes in auswärtigen Angelegenheiten, dem Schutz des geistigen Eigentums und der Statistik für Bundeszwecke. Im Rahmen der konkurrierenden Gesetzgebung[56] kann der Bund außerdem wissenschaftliche Forschung fördern und ist schließlich dazu berechtigt, Rahmenvorschriften über die allgemeinen Grundsätze des Hochschulwesens und das Beamtenrecht zu beschließen[57]. In diesen Bereichen darf das Landesrecht dem Bundesrecht nicht widersprechen (gemäß Art. 31 GG: „Bundesrecht bricht Landesrecht“).

Rahmenrechtlich ist für die Universitäten festgelegt, dass sie i.d.R. als Körperschaften des öffentlichen Rechts eingerichtet sind[58], weshalb ihr folglich Mitglieder angehören, und zugleich staatliche Aufgaben[59] wahrnehmen (§ 58 Abs. 1 Satz 1 HRG: „Die Hochschulen sind in der Regel Körperschaften des öffentlichen Rechts und zugleich staatliche Einrichtungen.“).

Anmerkung

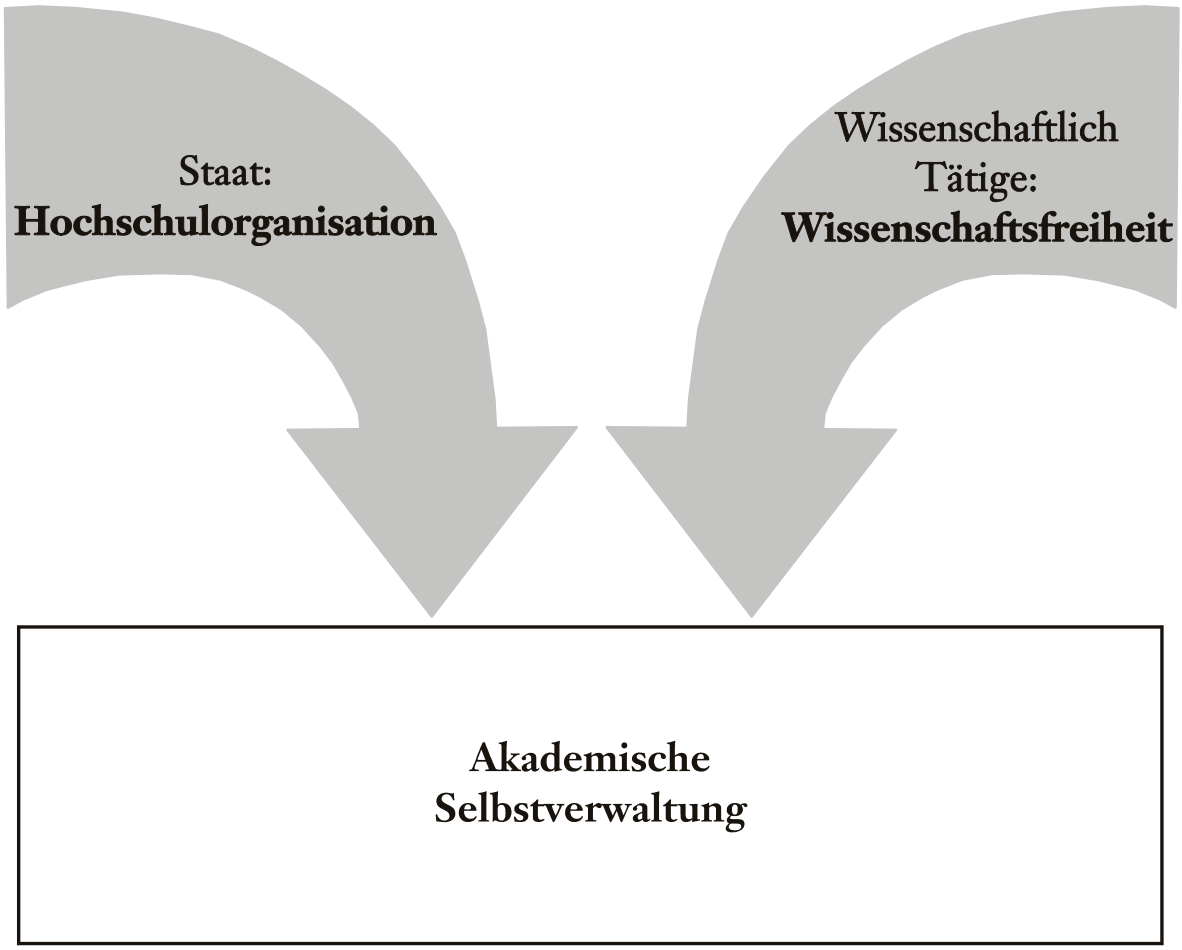
Einzelne Juristen vertreten deshalb die Ansicht, dass in der HRG-Formulierung ein Anstalts-Charakter der Hochschulen begründet sei. In diesem Falle wäre der Zweck das charakteristische Merkmal staatlichen Einflusses und nicht die Personen[60], was Otto Kimminich glaubhaft widerlegt[61]: „Die wissenschaftliche Forschung und ihre Lehre sind kein Staatszweck oder besser: sie sind durch Art. 5 Abs. 3 GG davor bewahrt, zum Gegenstand staatlicher Verwaltung gemacht zu werden.“ Universitäten haben deshalb Mitglieder und keine Nutzer. Die dritte Variante, die Rechtsform einer öffentlich-rechtlichen Stiftung, für die Sachen das charakteristische Merkmal staatlichen Einflusses sind[62], ist aus dem gleichen Grund unzutreffend: Stiftungen werden allenfalls wie Anstalten zu vordefinierten öffentlichen Zwecken eingerichtet[63].

---

54 so [Krüger1996a], S. 158ff.
55 siehe [Krüger1996a], S. 163ff.
56 siehe [Krüger1996a], S. 165ff.
57 siehe [Krüger1996a], S. 168ff.
58 diese Position entspricht auch der herrschenden Meinung unter Juristen (siehe [Kimminich1996b], S. 231).
59 diese Schlussfolgerung zieht jedenfalls Hans v. Mangoldt, Universität und Staat – zur Lage nach dem Hochschulrahmengesetz, Tübingen 1979, in Recht und Staat, Heft 488/489, S. 6f (zitiert nach [Kimminich1996b], S. 235); siehe auch [Oppermann1996], S. 1010ff.
60 siehe [Roellecke1996], S. 26.
61 unter Zitierung von Hans H. Klein, "Demokratisierung" der Universität?, Göttingen 1968, S. 30f (siehe Kimminich1996b], S. 228).
62 siehe [Roellecke1996], S. 26.
63 siehe [Köstlin1996], S. 1419.

Aufgrund ihres Rechtskonstrukts steht den Universitäten ein differenziertes Selbstverwaltungsrecht zu[64]: je eher Aspekte der freien Forschung und Lehre zu berücksichtigen sind, desto weiter geht die Hochschulautonomie – und desto mehr Zurückhaltung ist vom Staat im Rahmen seiner Rechtsaufsicht geboten[65], während ihm seine Fachaufsicht, die ihn dazu berechtigt, Vorschriften gegenüber Hochschulen zu erlassen, nur in den staatlichen Belangen zusteht, die den Hochschulen per Gesetz zugewiesen wurden[66]. Wesentliches Merkmal dieser Autonomie ist das Satzungsrecht der Universitäten, also das Recht, sich insbesondere eine Grundordnung geben zu dürfen, mit der die Gesamtorganisation der Universität geregelt wird[67].

Abb. 5 Ausschlaggebende Parameter der akademischen Selbstverwaltung



64 siehe [Knemeyer1996], S. 247ff.
65 siehe [Oppermann1996], S. 1025
66 siehe [Wiedmann2001], S. 41, Rn 124 und 125 bzw. S. 48f, Rn 143 und 144.
67 so [Oppermann1996], S. 1020ff.

2.2 Auszüge aus dem Grundrechts-Urteil zur Wissenschaftsfreiheit

2.2.1 Zur Wissenschaftsfreiheit im Allgemeinen

Das Bundesverfassungsgericht bestimmt in seinem Hochschulurteil[68]: „Art. 5 Abs. 3 Satz 1 GG gewährleistet dem Wissenschaftler einen gegen Eingriffe des Staates geschützten Freiraum, der vor allem die auf wissenschaftlicher Eigengesetzlichkeit beruhenden Prozesse, Verhaltensweisen und Entscheidungen bei dem Auffinden von Erkenntnissen, ihrer Deutung und Weitergabe umfasst. Art. 5 Abs. 3 GG ist zugleich eine das Verhältnis der Wissenschaft zum Staat regelnden Wert entscheidende Grundsatznorm. Danach hat der Staat im Bereich des mit öffentlichen Mitteln eingerichteten und unterhaltenen Wissenschaftsbetriebs durch geeignete organisatorische Maßnahmen dafür zu sorgen, dass das Grundrecht der freien wissenschaftlichen Betätigung soweit unangetastet bleibt, wie das unter Berücksichtigung der anderen legitimen Aufgaben der Wissenschaftseinrichtungen und der Grundrechte der verschiedenen Beteiligten möglich ist."

In der Begründung zu diesem Urteil hält das oberste Gericht fest[69]: „Das in Art. 5 Abs. 3 GG enthaltene Freiheitsrecht schützt als Abwehrrecht die wissenschaftliche Betätigung gegen staatliche Eingriffe und steht jedem zu, der wissenschaftlich tätig ist oder tätig werden will (...). Damit sich Forschung und Lehre ungehindert an dem Bemühen um Wahrheit als 'etwas noch nicht ganz Gefundenes und nie ganz Aufzufindendes' (Wilhelm von Humboldt) ausrichten können, ist die Wissenschaft zu einem von staatlicher Fremdbestimmung freien Bereich persönlicher und autonomer Verantwortung des einzelnen Wissenschaftlers erklärt worden. (...) Art. 5 Abs. 3 GG (...) erstreckt sich (...) auf jede wissenschaftliche Tätigkeit, d.h. auf alles, was nach Inhalt und Form als ernsthafter planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist. Dies folgt unmittelbar aus der prinzipiellen Unabgeschlossenheit jeglicher wissenschaftlichen Erkenntnis. Der gemeinsame Oberbegriff 'Wissenschaft' bringt den engen Bezug von Forschung und Lehre zum Ausdruck. Forschung als 'die geistige Tätigkeit mit dem Ziele, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen' (...) bewirkt angesichts immer neuer Fragestellungen den Fortschritt der Wissenschaft; zugleich ist sie die notwendige Voraussetzung, um den Charakter der Lehre als der wissenschaftlich fundierten Übermittlung der durch die Forschung gewonnen Erkenntnisse zu gewährleisten. Andererseits befruchtet das in der Lehre stattfindende wissenschaftliche Gespräch wiederum die Forschungsarbeit. Wie auch die Geschichte der Wissenschaftsfreiheit bestätigt, umfasst die Freiheit der Forschung insbesondere die Fragestellung und die Grundsätze der Methodik sowie die Bewertung des Forschungsergebnisses und seine Verbreitung; die Freiheit

---

[68] zitiert aus BVerfGE 35, 79 [79].
[69] zitiert aus BVerfGE 35, 79 [112f].

der Lehre, insbesondere deren Inhalt, den methodischen Ansatz und das Recht auf Äußerung von wissenschaftlichen Lehrmeinungen".

Und es folgert[70]: „Hieraus ergeben sich Postulate in zweifacher Richtung: a) Der Staat hat die Pflege der freien Wissenschaft und ihre Vermittlung an die nachfolgende Generation durch Bereitstellung von personellen, finanziellen und organisatorischen Mitteln zu ermöglichen und zu fördern. Das bedeutet, dass er funktionsfähige Institutionen für einen freien Wissenschaftsbetrieb zur Verfügung zu stellen hat. (...) b) Im Bereich des mit öffentlichen Mitteln eingerichteten und unterhaltenen Wissenschaftsbetriebs, d.h. in einem Bereich der Leistungsverwaltung, hat der Staat durch geeignete organisatorische Maßnahmen dafür zu sorgen, dass das Grundrecht der freien wissenschaftlichen Betätigung soweit unangetastet bleibt, wie das unter Berücksichtigung der anderen legitimen Aufgaben der Wissenschaftseinrichtungen und der Grundrechte der verschiedenen Beteiligten möglich ist."

2.2.2 Zu den Hochschulen im Besonderen

Zum Verhältnis zwischen Staat und Hochschulen bestimmt das Bundesverfassungsgericht in seinem Hochschulurteil grundsätzlich[71]: „Dem Gesetzgeber steht es zu, innerhalb der aufgezeigten Grenzen die Organisation der Hochschulen nach seinem Ermessen zu ordnen und sie den heutigen gesellschaftlichen und wissenschaftssoziologischen Gegebenheiten anzupassen. (...) Kriterium für eine verfassungsgemäße Hochschulorganisation kann hier nur sein, ob mit ihr 'freie' Wissenschaft möglich ist und ungefährdet betrieben werden kann."

Des Weiteren hält das Gericht fest[72]: „Zwar muss hiernach der Staat für die Organisation des Wissenschaftsbetriebs in seinen Hochschulen das irgend erreichbare Maß an Freiheit für die Forschungs- und Lehrtätigkeit jedes einzelnen Wissenschaftlers verwirklichen. Das bedeutet aber nicht, dass er die anderen schutzwürdigen Interessen und Bedürfnisse vernachlässigen dürfte, zu deren Befriedigung die Hochschule ebenfalls berufen ist. Die Hochschulen haben nicht nur die Pflege der reinen Wissenschaft zur Aufgabe; sie erfüllen vor allem auch die Funktion von Ausbildungsstätten für bestimmte Berufe. Diese Funktionen durchdringen sich; sie können nicht losgelöst für sich betrachtet werden; denn auch die Ausbildung soll eine wissenschaftliche sein. (...) Insoweit ist die Universität nicht nur der Raum für die sich in wissenschaftlicher Eigengesetzlichkeit vollziehenden einzelnen Forschungs- und Bildungsprozesse, sondern Gegenstand und Mittel einer öffentlich kontrollierten Bildungs- und Forschungspolitik. Bei der Ausgestaltung der 'Wissenschaftsorganisation' in der Universität muss diesen verschiedenartigen Funktionen Rechnung getragen werden. Es müssen ferner die

---

70 zitiert aus BVerfGE 35, 79 [114f].
71 zitiert aus BVerfGE 35, 79 [116f].
72 zitiert aus BVerfGE 35, 79 [121ff].

Interessen der verschiedenen Hochschulangehörigen, der Wissenschaftler, ihrer Mitarbeiter und der Studenten sowie der übrigen Bediensteten miteinander abgestimmt und koordiniert werden. Sie alle müssen sich – bedingt durch das Zusammenwirken mit den anderen Grundrechtsträgern und mit Rücksicht auf den Ausbildungszweck der Universität – Einschränkungen gefallen lassen. In diesem Spannungsfeld konkurrierender Rechte und Interessen kann sich naturgemäß die Wissenschaftsfreiheit des Einzelnen nicht schlechthin und schrankenlos durchsetzen."

2.3 Beziehungen zwischen Datenschutzrecht und Wissenschaftsfreiheit

2.3.1 Datenschutz versus Wissenschaftsfreiheit?

Viele Wissenschaftsgebiete haben den Menschen zum Forschungsgegenstand (exemplarisch seien hier Medizin, Sozialwissenschaften, Pädagogik, Psychologie, Zeitgeschichte und Kriminologie genannt[73]), so dass Konflikte der Wissenschaftsfreiheit mit dem informationellen Selbstbestimmungsrecht der zu untersuchenden Personen auftreten können[74]. Insofern prallen hier auch zwei Grundtypen aufeinander: „Die Forscher" gegen „Die Datenschützer".

Die Position „der Forscher": Die Forschungsfreiheit sei allenfalls durch die Treue zur Verfassung begrenzt, die Beachtung des Datenschutzes verteuere oder behindere Forschung[75]. Wenn gesetzliche Hürden Forschungen behindern würden (etwa in der Gentechnik oder Embryonenforschung), würden diese eben im Ausland durchgeführt, doch manche Forschungen (z.B. über deutsche Lebensverhältnisse) könnten nicht verlagert werden[76]. Personendaten würden nur zum Zweck wissenschaftlicher Erkenntnis verarbeitet, die Zweckbindung selbst sei zu eng gegenüber dem offenen Wissenschaftsprozess gefasst, es gebe keine absolut anonymisierte Daten (solange wenigstens noch eine Information darin enthalten sei) und wissenschaftliche Ergebnisse müssten jederzeit für eine Überprüfung durch andere Forscher zur Verfügung stehen[77].

Die Position „der Datenschützer": Die einzelne Person sei im Rahmen der informationellen Selbstbestimmung Subjekt und dies stünde höher als die Betrachtung des Menschen als Objekt der Forschung. Da es keine wertfreie Forschung gebe, seien vom Forscher subjektiv stark beeinflusste Personendaten nicht auszuschließen. Es bestehe bei Betroffenen insbesondere ein „Recht auf Nichtwissen"

---

73 Aufzählung aus [Krüger1996b], S. 301.

74 siehe hierzu insbesondere [Metschke2000], S. 9.

75 so zusammenfassend [Kilian1998], S. 787ff, ohne diese "Argumente" selbst zu übernehmen. Indirekt spricht sich aber z.B. [Krüger1996b], S. 301f für diese Ansicht aus.

76 so ein Beispiel der "Abschreckung der Forschung durch Datenschutz" von [Bochnik1996], S. 263.

77 so die wesentlichen Argumente in [Wagner1999], S. 377ff.

(z.B. in der Medizin und Genetik), das die Wissenschaft zu achten habe. Im Übrigen sei die Forschung eher an eine vom Einzelfall abstrahierende Betrachtung interessiert[78].

2.3.2 Regelungen zur Auflösung von Konflikten unterschiedlicher Grundrechte

In ständiger Rechtsprechung hat das Bundesverfassungsgericht entschieden[79], dass „die einzelnen Artikel des Grundgesetzes so ausgelegt werden müssen, dass sie mit den elementaren Grundsätzen des Grundgesetzes, insbesondere den Grundrechten, und seiner Werteordnung vereinbar sind."

Insofern ist also auch die Forschungsfreiheit als Teil der Wissenschaftsfreiheit nicht schrankenlos, auch wenn im zugrunde liegenden Artikel keine explizite Einschränkung aufgeführt ist[80]; hinsichtlich der Lehrfreiheit nimmt schon das Grundgesetz selbst eine Einschränkung vor (Satz 2 im Art. 5 Abs. 3)[81]. Das Bundesverfassungsgericht hat explizit festgestellt[82], dass sich ein Forscher „nicht über die Rechte seiner Mitbürger auf Leben, Gesundheit oder Eigentum hinwegsetzen (darf). (...) Die Konflikte zwischen der Gewährleistung der Wissenschaftsfreiheit und dem Schutz anderer verfassungsrechtlich garantierter Rechtsgüter müssen nach Maßgabe der grundgesetzlichen Werteordnung und unter Berücksichtigung der Einheit dieses Wertsystems durch Verfassungsauslegung gelöst werden." Dabei sind die zu schützenden Güter so einander zuzuordnen, dass beide trotz einer jeweiligen Grenzziehung optimal wirken können (dies wird als das „Prinzip praktischer Konkordanz" bezeichnet)[83].

In Baden-Württemberg sind in diesem Zusammenhang außerdem die Bestimmungen zur wissenschaftlichen Redlichkeit (nach § 56a UG) einzuhalten.

Treten Konflikte zwischen Grundrechte nicht nur im Sonderfall auf, ist der Gesetzgeber gefordert, die Grundrechte möglichst weitgehend zu realisieren und den Ausgleich somit herbeizuführen[84].

---

78 so [Weichert1997], S. 5ff, ausführlicher zum "Recht auf Nichtwissen" siehe Thilo Weichert in [Kilian2002], S. 11, Rn 44 im Teil 13, Kapitel 130.

79 zitiert nach [Kimminich1996a], S. 121f unter Berufung auf diverse Urteile des BVerfG, z.B. BVerfGE 19, 206 [220], BVerfGE 7, 198 [205] und BVerfGE 1, 13 [32].

80 so [Kimminich1996a], S. 146.

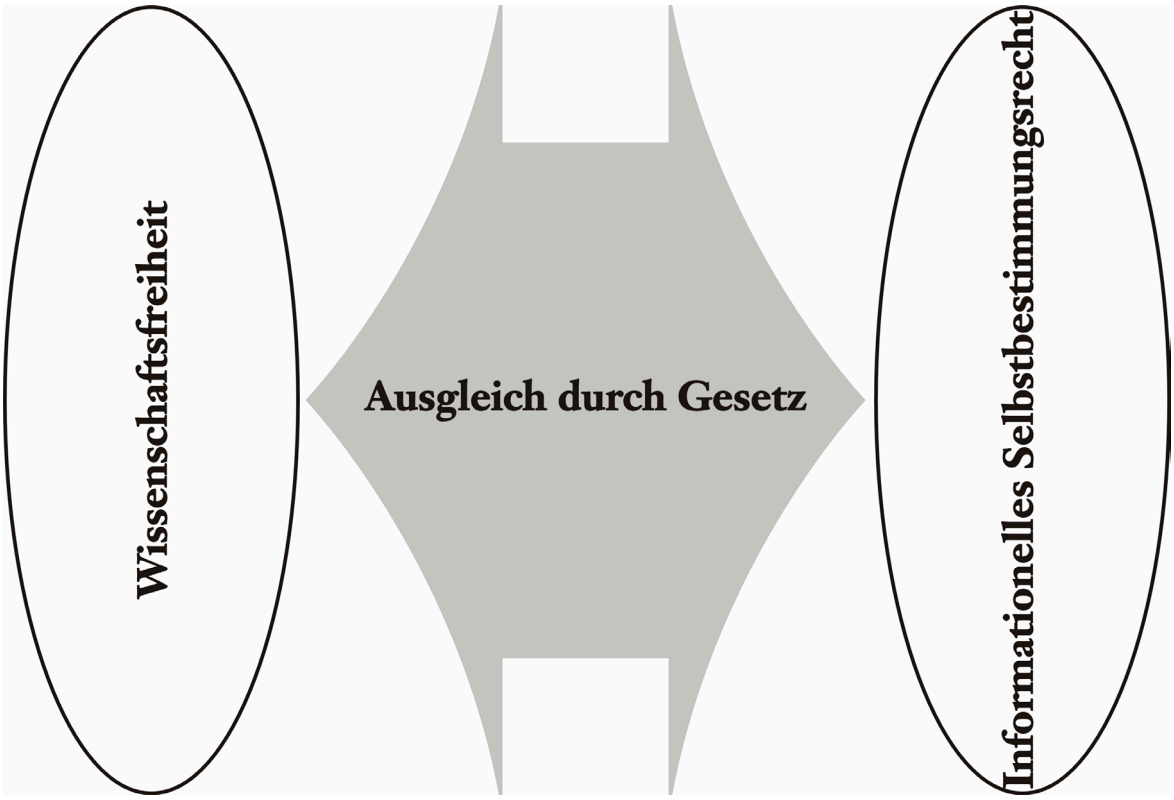
81 auch hierauf weist [Kimminich1996a], S. 146 ausdrücklich hin.

82 zitiert nach [Kimminich1996a], S. 146 – Originalzitat in BVerfGE 47, 327 [369].

83 so [Weichert1996], S. 260 in Anlehnung an ein BVerfG-Urteil (BVerfGE 30, 195 bzw. BVerfGE 67, 228).

84 so [Metschke2000], S. 9.

Abb. 6 Auflösung des Konfliktes zwischen Wissenschaftsfreiheit und Datenschutz



2.4 Ausdrückliche Regelungen zum Datenschutz an Universitäten

2.4.1 Datenschutz in der Forschung nach dem Landesdatenschutzgesetz

Im Landesdatenschutzgesetz Baden-Württemberg selbst finden sich gesonderte und damit bereichsspezifische Regelungen zum Datenschutz in der Forschung[85]:

- § 19 LDSG regelt, unter welchen Voraussetzungen öffentliche Stellen dort vorhandene personenbezogene Daten an Forschungseinrichtungen übermitteln dürfen.
- § 35 LDSG bestimmt, unter welchen Voraussetzungen öffentliche Forschungseinrichtungen personenbezogene Daten erheben dürfen und wie sie damit umzugehen haben.

Diese Forschungsklauseln sind gegenüber den allgemeinen Datenschutzvorschriften des LDSG vorrangig[86] und zugleich erforderlich, weil Hochschulen und Wissenschaft aufgrund der Wissenschaftsfreiheit in vielen Bereichen anderen Regelungen unterliegen (wie in diesem Kapitel gezeigt wurde). So erlaubte das Bundesverfassungsgericht in seinem Volkszählungsurteil explizit[87], dass z.B. die Weitergabe der Volkszählungsdaten zu wissenschaftlichen Zwecken erlaubt sei.

---

85 siehe auch [LfD2000], S. 15ff zu § 19 und § 35 LDSG.
86 siehe auch [Bergmann2002], S. 13f, Ziffer 5.6 im Überblick in Teil V.
87 siehe BVerfGE 65, 1 [2].

Außerdem kann im Rahmen der wissenschaftlichen Forschung unter Umständen die Einwilligung des Betroffenen bei der Erhebung personenbezogener Daten unterbleiben (siehe § 4 Abs. 5 LDSG) bzw. können unter bestimmten Voraussetzungen selbst höchst sensible Daten hierbei verarbeitet werden (siehe § 33 Abs. 2 LDSG).

Das grundlegende Problem bei der Weitergabe von Personendaten zu wissenschaftlichen Zwecken liegt darin, dass die ursprünglich erhobenen Daten im Zuge der Übermittlung i.d.R. eine Zweckänderung erfahren[88] (Beispiel: Werden verschiedene Krankheitsbilder einer Person näher auf Zusammenhänge untersucht, tritt der ursprüngliche Zweck, Behandlung einer konkret vorliegenden Krankheit, in den Hintergrund). Aus diesem Grund sind die Hürden für die Übermittlung hochgesteckt, so dass als vorrangige Alternativen die Beschaffung der Daten beim Betroffenen selbst bzw. mit dessen Einwilligung sind oder anonymisierte bzw. allgemein zugängliche Daten verwendet werden. Für die Durchbrechung des Zweckbindungsgrundsatzes müssen deshalb folgende Voraussetzungen vorliegen[89]:

- Die Übermittlung muss zur Durchführung wissenschaftlicher Forschung erforderlich sein,
- das Forschungsinteresse muss das Betroffeneninteresse erheblich überwiegen (es muss dabei ein konkretes und bedeutendes Allgemeininteresse vorliegen[90]) und
- der Forschungszweck kann nur mit unverhältnismäßigem Aufwand oder nicht auf andere Weise erreicht werden.

Als Forschungsvorhaben[91] gelten sowohl zeitlich und thematisch genau festgelegte Projekte als auch auf die wissenschaftliche Infrastruktur gerichtete und damit längerfristige Vorhaben.

Zu Forschungszwecken dürfen aber nur ausdrücklich benötigte Daten übermittelt werden. Ob dies zulässig ist[92], ist anhand der Beschreibung des Vorhabens zu überprüfen, in der insbesondere das aufgeführte Ziel und der Umfang des Forschungsvorhabens näher zu bestimmen sind.

Personenbezogene Daten dürfen im Rahmen eines Forschungsvorhabens (gemäß § 35 Abs. 3 LDSG) schließlich nur veröffentlicht werden, wenn der Betroffene zugestimmt hat oder die Daten über die Darstellung von Ereignissen der Zeitge-

---

88 siehe auch [Bergmann2002], S. 2, Ziffer 2 im Kommentar zu § 19 LDSG.
89 zitiert nach [Bergmann2002], S. 2, Ziffer 3 im Kommentar zu § 19 LDSG.
90 so [OLG-Hamm1998], S. 108.
91 gemäß [Bergmann2002], S. 2, Ziffer 2.2 im Kommentar zu § 19 LDSG in Form eines Zitats aus einem Kommentar zu § 4 BDSG, Rn 19 (Simitis/Dammann/Geiger/Mallmann/Walz: Kommentar zum Bundesdatenschutzgesetz).
92 so [Bergmann2002], S. 2f, Ziffer 3.1 im Kommentar zu § 19 LDSG.

schichte unerlässlich sind und keine schutzwürdigen Interessen des Betroffenen überwiegen.

2.4.2 Erhebung von Daten über Studienbewerber, Studierende und Prüfungskandidaten nach dem Universitätsgesetz

Es gibt gleich mehrere Sondervorschriften zur Erhebung von Personendaten, die auch in Universitäten zur Anwendung gelangen (wie § 113 Abs. 4 Landesbeamtengesetz, § 45 Landeskrankenhausgesetz und die §§ 19 bis 25 des Polizeigesetzes)[93] und insofern als bereichsspezifische Regelungen Vorrang vor den Datenschutzgesetzen haben. Allerdings sind für die Universitäten im Besonderen die Bestimmungen über die Erhebung von Studierendendaten nach § 125a UG vorrangig[94].

Demnach sind Studienbewerber, Studierende und Prüfungskandidaten verpflichtet, persönliche Daten für Verwaltungszwecke anzugeben. Das nähere gemäß § 125a Abs. 1 UG regelt die Verordnung des Wissenschaftsministeriums zur Erhebung und Verarbeitung personenbezogener Daten der Studienbewerber, Studierenden und Prüfungskandidaten für Verwaltungszwecke der Hochschulen (Hochschul-Datenschutzverordnung) vom 28.08.1992, in der am 27.09.1999 geänderten Fassung. Eine Weitergabe oder Zweckänderung ist (gemäß § 125a Abs. 3 UG) nur zulässig, wenn:

- dies eine Rechtsvorschrift erlaubt oder der Betroffene zur Angabe der Daten verpflichtet ist,
- der Betroffene eingewilligt hat oder dessen Einwilligung offensichtlich zu erwarten wäre,
- Straftaten oder Ordnungswidrigkeiten verfolgt werden und die ersuchende Stelle die Daten nicht auf andere Weise beschaffen kann,
- im Rahmen der öffentlichen Sicherheit die Abwehr von schwerwiegenden Beeinträchtigungen der Rechte Anderer oder von erheblicher Nachteile für das Gemeinwohl bzw. von einer unmittelbar drohenden Gefahr erforderlich ist.

Keine Zweckänderung stellt (gemäß § 125a Abs. 3 UG) dar, wenn:

- Aufsichts- und Kontrollbefugnisse wahrgenommen werden,
- Organisationsuntersuchungen durchgeführt werden,

---

[93] Auflistung aus [Bergmann2002], S. 2, Ziffer 3.2 im Kommentar zu § 13 LDSG.

[94] siehe ebenfalls [Bergmann2002], S. 2, Ziffer 3.2 im Kommentar zu § 13 LDSG bzw. S. 29, Ziffer 4.3.2 in der systematischen Darstellung des Datenschutzrechts im Teil I; der Paragraph gibt darüber hinaus noch die Erlaubnis, Angaben über die Erreichbarkeit von Bediensteten veröffentlichen zu dürfen (§ 125a Abs. 5 UG).

- automatisierte Verfahren der Datenverarbeitung geprüft oder gewartet werden,
- Statistiken erstellt werden.

Außerdem dürfen Teilnehmende von Lehrveranstaltungen (gemäß § 125a Abs. 4 UG) befragt werden, wobei hier keine Auskunftspflicht besteht. Die Ergebnisse der Auswertungen dürfen nur zur Bewertung der Lehre (Lehrevaluation) verwendet werden.

Anmerkung

Bei der Evaluation von Lehrveranstaltungen kann ein Spannungsverhältnis zu § 4a Abs. 3 UG auftreten, durch den Universitätsmitglieder (ohne jedwede Ausnahme) zur Angabe personenbezogener Daten im Rahmen von Evaluationen verpflichtet sind. Es wird daher an dieser Stelle davon ausgegangen, dass zwischen der Erhebung als solcher (im Rahmen von § 125a UG) und der Angabe personenbezogener Daten im Besonderen (auf Grundlage von § 4a UG) zu unterscheiden ist.

2.4.3 Evaluation von Forschung und Lehre

Die Universitäten in Baden-Württemberg sind angehalten, regelmäßig über ihre Tätigkeiten in Forschung und Lehre zu berichten (§ 4a Abs. 1 UG) und sollen dabei durch Eigen- und Fremdevaluation regelmäßig und öffentlich bewertet werden (§ 4a Abs. 2 UG). Schließlich ermächtigt § 4a Abs. 3 UG zur Erhebung der erforderlichen Auskünfte und verpflichtet die betroffenen Mitglieder der Universität (und ihre Angehörigen![95]) zur Mitwirkung und zur Angabe entsprechender personenbezogener Daten. Das Nähere, insbesondere welche personenbezogenen Daten im Rahmen einer Evaluation erhoben, bewertet und veröffentlicht werden dürfen, wird in Satzungen der jeweiligen Universität geregelt.

Diese gesetzliche Bestimmung kann neben § 125a UG als weitere bereichsspezifische datenschutzrelevante Regelung angesehen werden[96]. Im Rahmen des universitären Satzungsrechts dürfen jedoch weder die Grundsätze des Datenschutzes (siehe Abschnitt 1.3.1) noch andere Gesetzesbestimmungen außer Kraft gesetzt werden.

Der Selbstreport im Rahmen der Eigenevaluation wird dabei durch die Universität angefertigt, zur Durchführung der externen Evaluation hat das Land Baden-Württemberg dagegen eine Evaluationsagentur in Form einer Stiftung eingerich-

---

[95] in der Begründung der Regelung verweist der Gesetzgeber darauf, dass diese Ausweitung aufgrund des Professorenprivilegs im Erfindungsrecht vorgenommen wurde, so dass auch Erben eines Professors verpflichtet werden können, die erforderlichen Daten zur Evaluierung von Forschungsleistungen zu liefern (siehe Landtags-Drucksache 12/4404, S. 303).

[96] so Hanns Seidler in [Hailbronner2002], S. 3, Rn 4 im Kommentar zu § 6 HRG.

tet. In der Stiftungs-Satzung[97] sind als Aufgaben (in § 2 zum Stiftungszweck) bestimmt:

- die Durchführung regelmäßiger und vergleichender Evaluationen von Forschung und Lehre unter Berücksichtigung hochschulspezifischer Aufgaben,
- die Unterstützung des Landesforschungsbeirats bei der Durchführung anlassorientierter, strategischer Evaluationen der Forschung und
- die Unterstützung der Hochschulen bzw. des Wissenschaftsministeriums bei der Durchführung anlassbezogener Evaluationen.

[97] abgedruckt als Anhang 2 in: Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg (Pressestelle): Die Evaluationsagentur Baden-Württemberg, Aktuelle Reihe Nr. 10, Stuttgart, Schwäbische Druckerei, 2001.

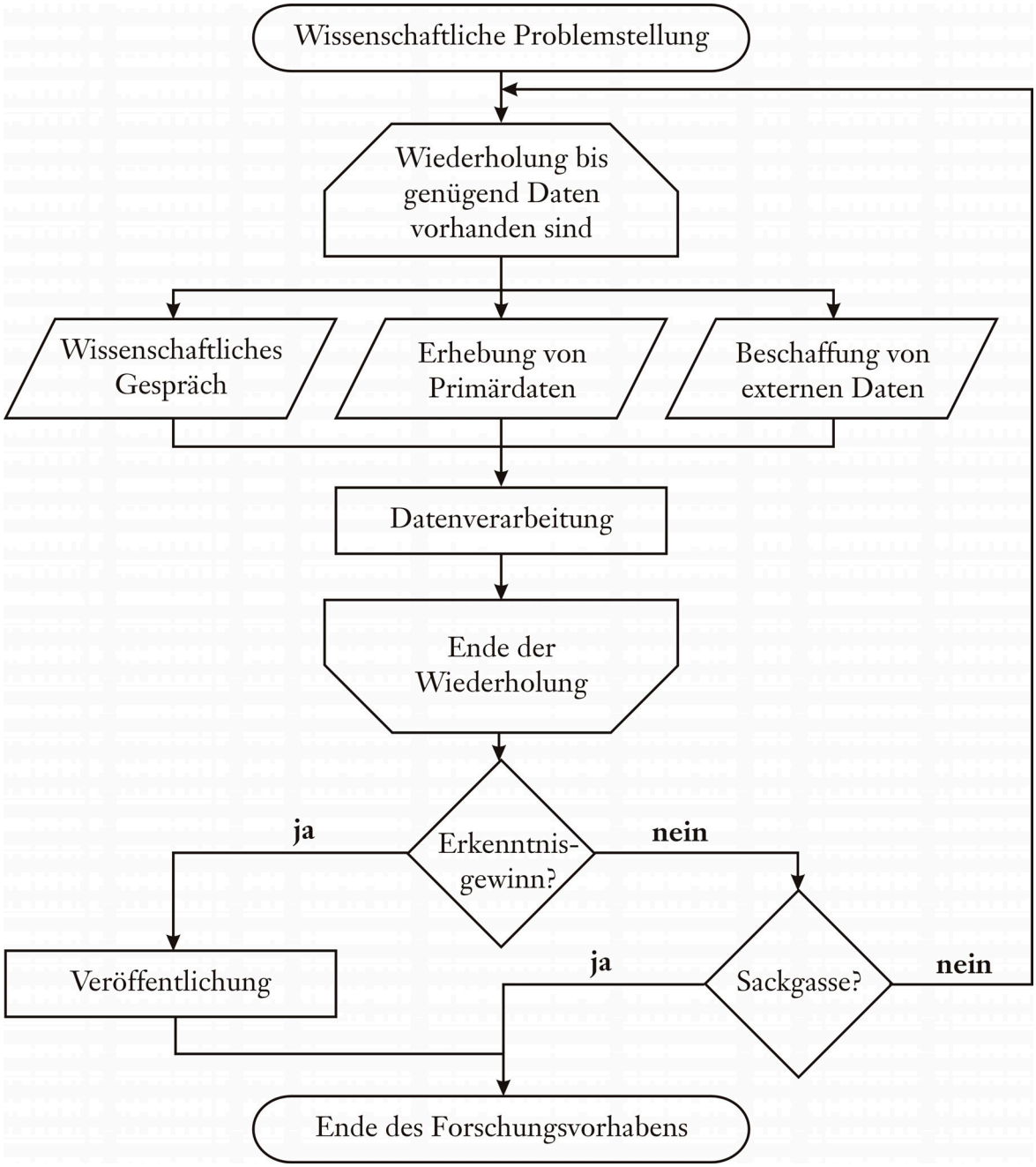
3. Der Datenschutz in zentralen Bereichen der Hochschulselbstverwaltung

3.1 Datenschutz im Bereich universitärer Forschung

3.1.1 Datenschutzgerechter Umgang mit Daten im Rahmen universitärer Forschung

Der wissenschaftliche Prozess kann vereinfacht so dargestellt werden:

Abb. 7 Vereinfachte Sicht auf den Forschungszyklus



Daraus ist ersichtlich, dass als kritische Bereiche im Sinne des Datenschutzes alle Tätigkeiten bezeichnet werden können, in denen Daten verarbeitet werden (im obigen Diagramm sind das die Parallelogramme und Rechtecke).

Sensible Daten können also erhoben bzw. verarbeitet werden bei:

- den wissenschaftlichen Gesprächen (Konferenzen, Tagungen etc.),
- der Erhebung von Primärdaten (also gegenüber dem Betroffenen),
- der Beschaffung von externen Daten (also gegenüber der verantwortlichen Stelle, von der die Daten bezogen werden; z.B. Forschungsdatenbanken oder Forschungsregister),
- der Datenverarbeitung im eigentlichen Sinn, sowie
- der Veröffentlichung.

Grundsätzlich können bei der Datenverarbeitung im Rahmen universitärer Forschung zwei Richtungen unterschieden werden:

1. An der Universität wird selbst geforscht und die Daten (in deren Auftrag) verarbeitet: hierbei ist die Universität selbst verantwortliche Stelle im Sinne des Datenschutzes.
2. An die Universität wird im Rahmen eines externen Forschungsprojekts durch Dritte die Anfrage auf Verarbeitung von Datenmaterial gestellt: Somit stellt dies eine Datenverarbeitung im Auftrag einer anderen verantwortlichen Stelle dar.

Im ersten Fall muss die Universität zwingend selbst für die Einhaltung des Datenschutzes (entsprechend der in Baden-Württemberg geltenden Rechtsvorschriften) sorgen, im zweiten Fall muss sie hierzu durch die verantwortliche Stelle verpflichtet werden. Dies ist zu unterscheiden von der Übermittlung von Daten der verantwortlichen Stelle, denn übermittelt die Universität ihre personenbezogenen Daten, bleibt sie selbst verantwortliche Stelle und hat für die Einhaltung des Datenschutzes zu sorgen.

Bei der Auftragsdatenverarbeitung ist zu beachten, dass sich möglicherweise die Vorschriften gegenüber denen in Baden-Württemberg unterscheiden: So können besondere Bereichsregelungen relevant sein (insbesondere im Rahmen der medizinischen Forschung sind dies[98] z.B. § 9 Krebsregistergesetz oder § 46 Krankenhausgesetz) oder andere Datenschutzgesetze (ggf. z.B. das BDSG, wenn eine Bundeseinrichtung oder keine öffentliche Einrichtung Auftraggeber ist; oder gar gesetzliche Bestimmungen in anderen Staaten, die im Regelfall nicht der EG-Datenschutzrichtlinie[99] widersprechen dürfen) ausschlaggebend sein.

---

[98] nach [Bergmann2002], S. 2, Ziffer 2.1 im Kommentar zu § 19 LDSG.

[99] vollständig abgedruckt u.a. in [Bergmann2002], Anlage 3 zu Teil I.

Zu beachten gilt beim Umgang mit personenbezogenen Daten (siehe auch Abschnitt 2.4.1):

- (Faktisch) Anonymisierte Daten (bzw. gänzlich personenunbezogene Daten) können ohne Beachtung von Datenschutz-Vorschriften verarbeitet werden![100] Deshalb sollten frühestmöglich personenbezogene Daten (faktisch) anonymisiert werden.
- Ist der Personenbezug für das Forschungsvorhaben wichtig (z.B. im Rahmen einer persönlichen Langfriststudie), sind die personenbezogenen Daten in einem ersten Schritt frühestmöglich zu pseudonymisieren, wobei die identifizierenden Daten durch Zuordnungstabellen und Verschlüsselungsverfahren verändert (und getrennt gespeichert) werden. U.U. kann dabei vorgesehen werden, dass der Betroffene selbst ein Pseudonym vergibt[101]. Soll ein Pseudonym systematisch erzeugt werden, empfiehlt sich z.B. eine Hash-Funktion gemäß der Norm von ISO/IEC 10118[102]. Wenn der Personenbezug nicht zwingend erforderlich ist, sollten die Daten gleich (faktisch) anonymisiert werden.
- Personenbezogene Daten, zu deren Verarbeitung der Betroffene sein Einverständnis erklärt hat (d.h. die Einwilligung des Betroffenen liegt vor), dürfen im Rahmen der getroffenen Vereinbarungen (und natürlich der gesetzlichen Bestimmungen) verarbeitet werden.
- Personenbezogene Daten, die aufgrund gesetzlicher Regelungen (im Rahmen so genannter Forschungsklauseln, wie z.B. § 19 und 35 LDSG) auch ohne Einwilligung des Betroffenen verarbeitet werden dürfen, unterliegen strengeren gesetzlichen Vorschriften. Beispielswiese darf der Zweck von Daten, die einem Berufsgeheimnis (z.B. Ärzte, Notare, Sozialarbeiter) oder besonderen Amtsgeheimnis (z.B. Statistikgeheimnis, Sozialgeheimnis, Steuergeheimnis) nur aufgrund anderer expliziter gesetzlicher Bestimmungen verändert werden (siehe § 39 BDSG)[103].
- Personenbezogene Daten, die zu wissenschaftlichen Zwecken erhoben und verarbeitet werden, dürfen nicht für andere Zwecke verwendet werden (wie z.B. Verwaltungs-, Polizei- oder Werbezwecke), können jedoch auch für andere als

[100] siehe [Metschke2000], S. 20ff.
[101] siehe [Metschke2000], S. 23ff.
[102] siehe [AKT1998], S. 19.
[103] siehe [Bergmann2002], S. 2f im Teil III, Kommentar zu § 39 BDSG, Rn 12 – 14.

das ursprüngliche Forschungsvorhaben verwendet werden, sofern keine Einschränkungen z.B. im Rahmen der Einwilligung des Betroffenen vorliegen[104]. Allerdings existieren besondere Beschränkungen bei der Veröffentlichung von personenbezogenen Daten im Rahmen wissenschaftlicher Zwecke (siehe § 40 BDSG bzw. § 35 LDSG).

Personenbezogene Primärdaten sollen zur wissenschaftlichen Überprüfbarkeit gemäß einer Empfehlung der Deutschen Forschungsgemeinschaft zehn Jahre lang aufbewahrt werden[105]. Danach sind sie folglich zu löschen.

Gesonderte Verfahren, mit denen personenbezogene Daten ohne Einwilligung des Betroffenen verarbeitet werden können, sind[106]:

- das **Adressmittlungsverfahren**: hier werden entsprechende Anfragen im Auftrage Dritter verschickt, die Adressen selbst jedoch nicht der anfragenden Stelle übermittelt und
- der **Datentreuhänder**: hier erfolgt die Auswertung im Interesse der anfragenden Stelle der personenbezogenen Daten der Daten besitzenden Stelle durch einen unabhängigen Dritten, der einer besonderen Schweigepflicht unterliegt (z.B. Notar).

3.1.2 Urheberrecht im Bereich universitärer Forschung

Grundsätzlich erfährt jede „persönliche geistige Schöpfung“ (gemäß § 2 Abs. 1 UrhG) urheberrechtlichen Schutz. Dazu zählen insbesondere wissenschaftliche Darstellungen. Allerdings tritt ein Konflikt bei der Verwertung wissenschaftlicher Ergebnisse auf:

- Das Recht zur kommerziellen Verwertung zählt nach einem Urteil des Bundesverfassungsgerichts zum Schutzbereich des Eigentums in Verbindung mit dem allgemeinen Persönlichkeitsrecht[107]. Demgegenüber stellt die Novellierung des Arbeitnehmererfindungsgesetzes wissenschaftliche Erfindungen im Rahmen eines universitären Beschäftigungsverhältnisses anderen Diensterfindungen gleich, so dass der Dienstherr (und eben nicht der Erfinder) vorrangig über die Verwertung entscheiden kann[108].

---

[104] siehe [Bergmann2002], S. 3 im Teil III, Kommentar zu § 40 BDSG, Rn 12 – 17.
[105] siehe Empfehlung Nr. 7 aus der Pressemitteilung der Deutschen Forschungsgemeinschaft Nr. 31 vom 16.12.1997 (Auszug abgedruckt in [DFG1998], S. 1765).
[106] siehe [Metschke2000], S. 41ff.
[107] so [Bizer2001], S. 727, in Anlehnung an BVerfGE 79, 29 (38ff) und BVerfGE 31, 229/238/239.
[108] so [Böhringer2002], S. 953.

- Die Wissenschaftsfreiheit erlaubt wissenschaftlich Tätigen grundsätzlich, selbst darüber zu entscheiden, was von ihren wissenschaftlichen Ergebnissen veröffentlicht werden soll (von dieser Entscheidungsfreiheit sind vorgeschriebene „Pflichtexemplare“ ausgenommen[109]). Andererseits ist im wissenschaftlichen Bereich alles benutzbar, was in der Lehre oder als (publiziertes) Forschungsergebnis, selbst in geschützten Werken, offenbart wurde[110].

Verwertungsinteresse einerseits und Publizitätsinteresse andererseits stehen also in einem Spannungsverhältnis, das unter den aktuellen Voraussetzungen gerichtlich noch nicht abschließend geklärt ist.

Ein Sonderfall liegt vor, wenn ein wissenschaftlich Tätiger im Rahmen seiner Datenerhebung anonym urheberrechtlich geschützte Online-Dienste in Anspruch nehmen will, denn im Internet werden i.d.R. die Nutzer elektronischer Diensten mitprotokolliert. Es besteht kein Zweifel, dass in diesem Fall die Datenschutz-Bestimmungen höher gewichtet sind: So ist z.B. die EG-Datenschutzrichtlinie gegenüber der EG-Urheberrichtlinie vorrangig[111].

Regelmäßig finden sich in der Neuen Juristischen Wochenschrift Berichte über rechtliche Entwicklungen dieses Themenkomplexes. Zuletzt ist dort erschienen:

- Axel Nordemann, Jan Bernd Nordemann und Christian Czychowski: Die Entwicklung der Gesetzgebung und Rechtsprechung zum Urheberrecht in den Jahren 2000 und 2001, in: Neue Juristische Wochenschrift 8/2002, S. 562 – 572.

Da viele der dort angesprochenen Themen nicht von Universitäts-Spezifika handeln, wurde bewusst auf eine nähere Darstellung wichtiger juristischer Fragen hieraus verzichtet.

3.1.3 Datenschutz im Rahmen der Evaluation der Forschung

Die Forschung unterliegt insbesondere im Rahmen der Drittmitteleinwerbung (z.B. bei Sonderforschungsbereichen der Deutschen Forschungsgemeinschaft) einer (externen) Begutachtung und Bewertung[112]. Ebenso wird die Forschung im Rahmen anlassorientierter Evaluationen im Auftrag des Landesforschungsbeirats

---

[109] siehe [Wiese2000], S. 1579f.

[110] so [Homma1996], S. 1562 und S. 1564f; ergibt sich weitgehend auch aus dem Umstand, dass Veröffentlichungen als allgemein zugängliche Quellen angesehen werden (siehe Abschnitt 1.5.4).

[111] so [Bizer2001], S. 727; die EG-Urheberrichtlinie 2001/29/EG weist ausdrücklich in Artikel 9 der EG-Datenschutzrichtlinie 95/46/EG demnach eine höhere Rangfolge ein (ebenso die Erläuterung gemäß "Erwägungsgrund" 57).

[112] siehe auch Hanns Seidler in [Hailbronner2002], S. 9ff, Rn 16 – 18 im Kommentar zu § 6 HRG.

untersucht (siehe Abschnitt 2.4.3). In beiden Fällen geht es also in erster Linie darum, ob finanzielle Mittel den Forschenden (weiterhin) zur Verfügung gestellt werden sollen. Da hierzu die mitteleinwerbende Stelle die nötigen Angaben (im rechtlichen Sinne) freiwillig zur Verfügung stellt, ist dieser Fall datenschutzrechtlich unbedenklich (es liegt faktisch eine Einwilligungserklärung vor).

Aspekte der Forschung werden, soweit sie mit der Lehre in Zusammenhang stehen, auch im Rahmen der regelmäßigen und vergleichenden Evaluation der Evaluationsagentur bewertet[113] (siehe außerdem Abschnitt 3.2.4). Grundsätzlich gibt es keine datenschutzrechtlichen Bedenken über die Weitergabe und Veröffentlichung von Evaluationsergebnissen, soweit die gesamte untersuchte Einheit betroffen ist und nicht ein Forscher alleine[114].

Bei einer Evaluation der Forschung im Allgemeinen (also unabhängig von der Mittelakquisition) lässt sich eine (faktische) Anonymisierung nur schwer erreichen, da untersuchte Forschungsprojekte eindeutig zumindest der Verantwortung von Professoren zugeordnet werden können. Völlig unproblematisch ist allerdings die Darstellung, was geforscht wurde, während eine Bewertung der Forschungstätigkeiten Probleme aufwerfen kann. Werden z.B. die Ergebnisse der Bewertung ihrer Forschungstätigkeit veröffentlicht, wie das im Rahmen der Arbeit der Evaluationsagentur vorgesehen ist, greifen Datenschutz-Aspekte. Dieser Umstand wird bisher in der juristischen Fachliteratur überwiegend als vernachlässigbar angesehen[115]. Es wird aber als verfassungsrechtlich problematisch angesehen, wenn staatlicherseits Konsequenzen aus Evaluationen gezogen werden (z.B. in Form von Mittelkürzungen)[116]. Je eher etwaige Konsequenzen durch die Universität selbst erfolgen, desto unbedenklicher ist dies jedoch.

Der Schwerpunkt forschungsbezogener Evaluation liegt aktuell eher bei quantitativen Kriterien und nicht in qualitativer Bewertung[117]. Dennoch ist grundsätzlich bei der Evaluation ein wissenschaftsadäquates Verfahren anzuwenden, etwa durch den Einsatz von Peers (gleichrangigen Gutachtern)[118]. Die wissenschaftliche Aus-

---

[113] so [Herberger2001], S. 200, Rn 630.

[114] siehe Hanns Seidler in [Hailbronner2002], S. 10, Rn 17 im Kommentar zu § 6 HRG.

[115] als generell unbedenklich sowohl in Fragen der Forschungs- als auch der Lehrevaluation sieht dies aufgrund des bewertungsimmanenten Wesens der Wissenschaft Hanns Seidler in [Hailbronner2002], S. 18, Rn 30 im Kommentar zu § 6 HRG, während es in der Frage der Lehrevaluation jedoch unterschiedliche Sichtweisen gibt: problematisch sieht dies (allerdings im Kontext des Fehlens einer zwingend festgeschriebenen professoralen Mehrheit bei Entscheidungen über Lehrevaluationen) [Bethge2000], S. 1108, Rn 179, unproblematisch dagegen [Herberger2001], S. 198, Fußnote 342.

[116] siehe Hanns Seidler in [Hailbronner2002], S. 19, Rn 31 im Kommentar zu § 6 HRG.

[117] siehe Hanns Seidler in [Hailbronner2002], S. 12, Rn 20 im Kommentar zu § 6 HRG.

[118] siehe Hanns Seidler in [Hailbronner2002], S. 21, Rn 35 im Kommentar zu § 6

einandersetzung um die Ergebnisse von Forschung hat aus Sicht des Bundesverwaltungsgerichts[119] primär im Rahmen der üblichen Regeln des wissenschaftlichen Diskurses (Fachzeitschriften, Konferenzen etc.) zu erfolgen.

Anmerkung

Im untersuchten Fall des Bundesverwaltungsgerichts ging es zwar um Fragen wissenschaftlicher Redlichkeit und nicht um Evaluationen von Forschung, aber diese Argumentationsweise durchzieht doch mehrere juristische Quellen (siehe die Angaben im unmittelbar vorangehenden Absatz), so dass hier davon ausgegangen wird, dass dies auch allgemein gilt.

3.1.4 Weitere Aspekte wissenschaftlicher Forschung

Einen detaillierten Überblick über datenschutzgerechten Umgang mit medizinischer Forschung liefert:

- Horst G. Abel (Hrsg.): Praxishandbuch Datenschutz, Band 4, Teil 8/5.5 Datenschutz in der Medizin, Kissing, Interest Verlag, 2001.

Auf die grundlegenden Datenschutz-Fragen aus der Praxis im Rahmen der epidemiologischen Forschung antwortet:

- Deutsche Arbeitsgemeinschaft für Epidemiologie (in Zusammenarbeit mit dem Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder): Epidemiologie und Datenschutz, in: [Hamm1999], S. 97 – 107.

Auf eine Darstellung der jeweiligen Aspekte wird daher im Rahmen dieser Arbeit verzichtet.

Regelmäßig finden sich in der Neuen Juristischen Wochenschrift Berichte über rechtliche Entwicklungen dieses Themenkomplexes. Zuletzt ist dort erschienen:

- Andreas Spickhoff: Medizin und Recht zu Beginn des neuen Jahrhunderts – Die Entwicklung des Medizinrechts 2000/2001, in: Neue Juristische Wochenschrift 24/2001, S. 1757 – 1768.

Da viele der dort angesprochenen Themen nicht von Universitäts-Spezifika handeln, sondern insbesondere das Arzt-/Patientenverhältnis behandeln, wurde bewusst auf eine nähere Darstellung wichtiger juristischer Fragen hieraus verzichtet.

HRG.

[119] siehe BVerwGE 102, 304 [312].

3.2 Datenschutz im Bereich der Studienorganisation

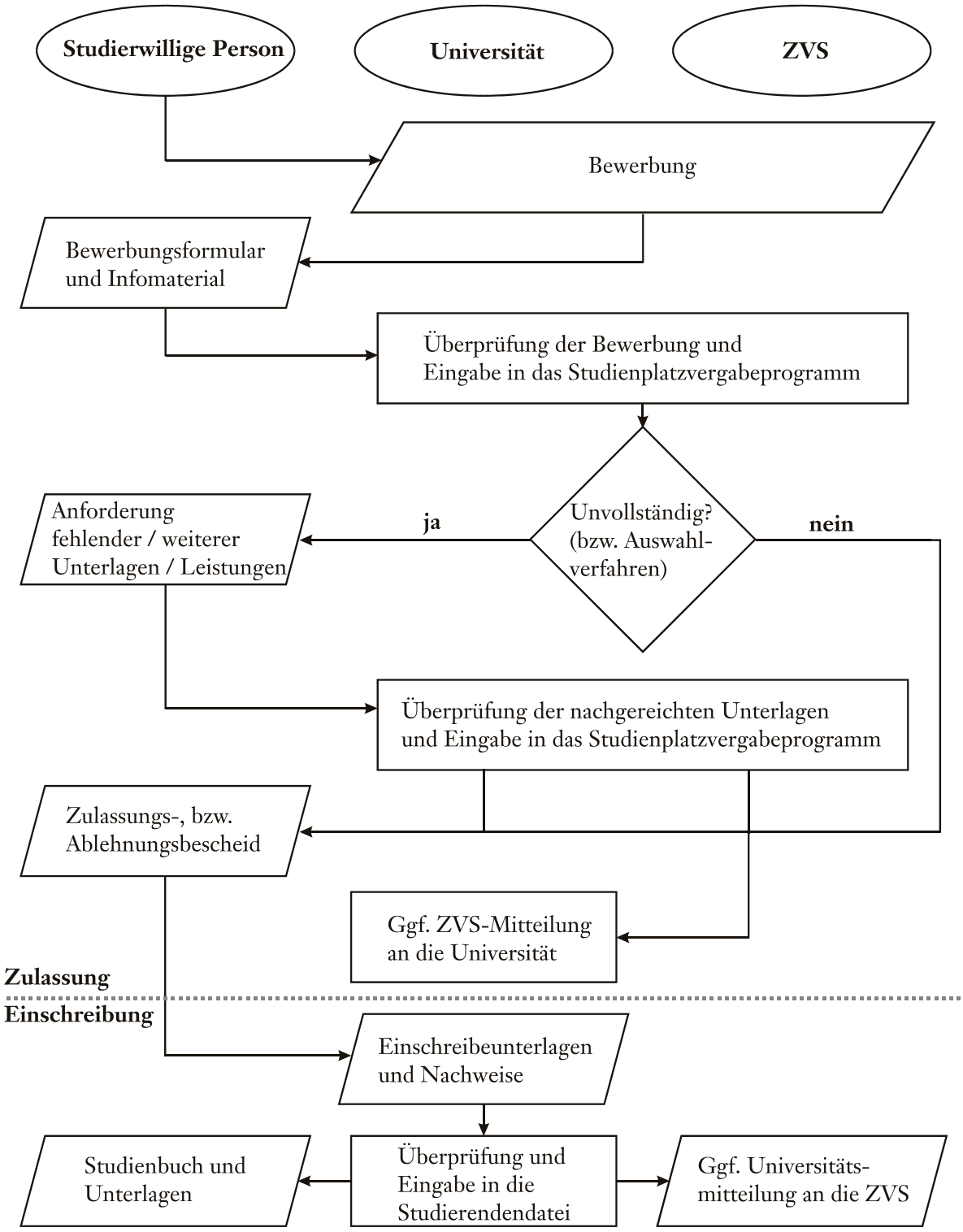
3.2.1 Datenschutzgerechter Umgang mit Zulassungs- und Immatrikulationsdaten

Die Zulassung ist notwendige Voraussetzung zur Aufnahme im spezifischen universitären Studiengang, die Immatrikulation wiederum begründet die Mitgliedschaft des Studierenden an der gewählten Universität und gewährt die damit verbundenen Rechte und Pflichten.

Im Rahmen des Zulassungsverfahrens und der Einschreibung von Studienbewerbern lassen sich folgende Verfahrensschritte ausmachen[120]:

[120] siehe auch [Rechnungshof1994], S. 28 – 31 und S. 34 – 35.

Abb. 8 Verfahrensschritte bei der Zulassung und Einschreibung von Studierenden



Als kritische Bereiche im Sinne des Datenschutzes lassen sich also folgende Tätigkeiten benennen:

- Eingang der Bewerbungsunterlagen und deren Eingabe in das Studienplatzvergabeprogramm (insbesondere HISZUL)
- Erstellung und Versand der Einschreibeunterlagen (ggf. unter Beachtung von Zulassungsbeschränkungen)
- Eingang der Einschreibeunterlagen und deren Eingabe in die Studierendendatei (i.d.R. in HISSOS, womit eine gesonderte Erfassung in Studierendenakten hinfällig ist[121])

Anmerkung

Bei Studiengängen, die in das zentrale Vergabeverfahren einbezogen sind, ist die Zentralstelle für die Vergabe von Studienplätzen an der Datenverarbeitung beteiligt. Nach Art. 2 ZVS-StV sind die Datenschutzvorschriften in Nordrhein-Westfalen maßgeblich, da der Sitz der ZVS in Dortmund liegt. Insofern können einzelne Datenschutzbestimmungen von denen in Baden-Württemberg abweichen. Allerdings konnte dafür kein Hinweis gefunden werden. Im Nachfolgenden werden deshalb die in Baden-Württemberg zu beachtenden Datenschutzbestimmungen näher betrachtet.

Es gilt zu beachten, dass der Studienbewerber die nötigen Unterlagen zur Zulassung (gemäß § 1 und § 3 Abs. 1 der Hochschul-Datenschutzverordnung) und zur Immatrikulation (gemäß § 2 und § 3 Abs. 2 der Hochschul-Datenschutzverordnung) einzureichen hat. In beiden Fällen ist die Universitätsverwaltung ausdrücklich dazu berechtigt, diese personenbezogenen Daten für Verwaltungszwecke oder auch für andere Zwecke zu nutzen, sofern der Studienbewerber auch immatrikuliert wurde (§ 12 Abs. 2 Hochschul-Datenschutzverordnung). Allerdings wird nicht bei jedem Zulassungsantrag darauf hingewiesen, auf welcher rechtlichen Grundlage die Angabe von Daten zu erfolgen hat und welche Konsequenzen bei fehlenden Angaben gezogen werden[122].

Nur eingeschränkt nutzbar für die Universitätsverwaltung sind dagegen die zusätzlich vom Studienbewerber zu tätigenden Angaben im Rahmen eines Eignungsfeststellungsverfahrens (gemäß § 42 Abs. 4 UG bzw. § 11a HVVO): Denn die einzige Rechtsgrundlage stellt in diesen Fällen die von der Universität hierzu erlassenen Satzungen (auf Basis von § 94 Abs. 3 UG bzw. § 6 Abs. 3 HZG) dar. Hierbei wird hochschulrechtlich unterschieden[123] zwischen:

- vorgeschalteten „hochschuleigenen Eignungsfeststellungsverfahren“, durch die geregelt wird, welche Studienbewerber

[121] siehe [Rechnungshof1994], S. 47f.
[122] siehe z.B. [LDSB1994], S. 92f.
[123] siehe auch [Haug2001], S. 279, Rn 853 und 854 sowie S. 281f, Rn 859 – 865.

sich überhaupt für den betreffenden Studiengang eignen und daher als zur Zulassung berechtigt angesehen werden (Grundlage: § 42 Abs. 4 UG), und
- Eignungsfeststellungsverfahren im Rahmen der Auswahlverfahren bei örtlichen NCs, durch die eine Reihung der (berechtigten) Studienbewerber vorgenommen wird, die bis zur Ausschöpfung der Kapazitäten (also nur bis zu einer bestimmten Position innerhalb der Reihe) abgearbeitet wird (Grundlage: § 11a HVVO).

Nach § 11a Abs. 2 HVVO sind beim Auswahlverfahren die erhobenen Daten unverzüglich nach Abschluss des Vergabeverfahrens zu löschen, soweit nicht durch eine andere Vorschrift eine Weiterverarbeitung erlaubt ist. Spätestens jedoch nach Abschluss des Prüfungsverfahrens (mit dem Erwerb des Abschlussgrades bzw. dem Verlust des Prüfungsanspruchs), i.d.R. aber mit der Exmatrikulation, sind diese Daten unverzüglich zu löschen (§ 12 Abs. 1 Hochschul-Datenschutzverordnung).

Liegen im Falle der jeweiligen Eignungsfeststellungsverfahren keine bereichsspezifischen Regelungen vor, so gelten die Bestimmungen aus dem LDSG. Im Sinne von § 23 Abs. 2 LDSG sind die zusätzlich erhobenen personenbezogenen Daten zu löschen, wenn sie zur Aufgabenerfüllung[124], also der Zulassung einschließlich etwaiger Dokumentationspflichten (z.B. im Rahmen von Rechtsstreitigkeiten), nicht mehr benötigt werden (i.d.R. also nach einem Semester[125]). Eine Weiterverarbeitung dieser Daten für andere Zwecke ist nicht erlaubt.

Bei der Einschreibung sind neben dem Studiensekretariat, in dem die Studierendendaten verarbeitet werden, auch die Universitätskasse (zur Überprüfung der Zahlungseingänge für Semesterbeitrag und ggf. angefallenen Gebühren) und die Krankenkasse (für den Nachweis der Krankenversicherung) beteiligt.

Bei Promotionsstudierenden sind die entsprechenden Regelungen im Rahmen universitärer Satzungen, insbesondere der Promotionsordnung, maßgeblich. Auch hier ist in Ermangelung etwaiger ausdrücklicher Regelungen im Rahmen der zugrunde liegenden Satzungen grundsätzlich § 23 Abs. 2 LDSG bzw. § 12 Abs. 1 der Hochschul-Datenschutzverordnung anzuwenden.

Gleiches gilt für Gasthörer, für die allerdings in § 6 Hochschul-Datenschutzverordnung exakt vorgeschrieben ist, welche personenbezogenen Daten die Universität erheben darf.

---

[124] siehe auch [Bergmann2002], S. 35, Anm. 3.1 und 4.1 im Kommentar zu § 19 a.F. LDSG – der neue § 23 LDSG entspricht wortgleich dem § 19 a.F. LDSG, ist jedoch zum Zeitpunkt der Erstellung dieser Arbeit noch nicht gesondert kommentiert.

[125] siehe [Rechnungshof1994], S. 47.

3.2.2 Datenschutzgerechter Umgang mit Rückmeldedaten

Nach Ablauf eines Semesters kann sich ein Studierender (auf der Grundlage von § 89 UG bzw. § 4 Hochschul-Datenschutzverordnung) zurückmelden, um weiterhin im gewählten Studiengang eingeschrieben zu sein[126]. Hierzu ist die Angabe personenbezogener Daten erforderlich, die im Rahmen von § 12 Hochschul-Datenschutzverordnung zu verarbeiten sind. Der Ablauf entspricht im Wesentlichen der Einschreibung (siehe vorstehenden Abschnitt), wobei kein gesonderter Antrag mehr auszufüllen ist.

3.2.3 Datenschutzgerechter Umgang mit Prüfungsdaten

Im Regelfall sind von den Studierenden im Verlauf ihres Studiums Prüfungsleistungen im Sinne einer (fachlichen) Leistungsüberprüfung zu erbringen. Anforderungen hierzu sind sowohl im UG, in Rechtsverordnungen und örtlichen Prüfungsordnungen (sowie z.B. durch Rahmenordnungen[127]) ausformuliert.

Grundsätzlich orientiert sich ein Prüfungsverfahren (ohne Berücksichtigung von etwaigen Sonderfällen) an folgendem Ablauf[128]:

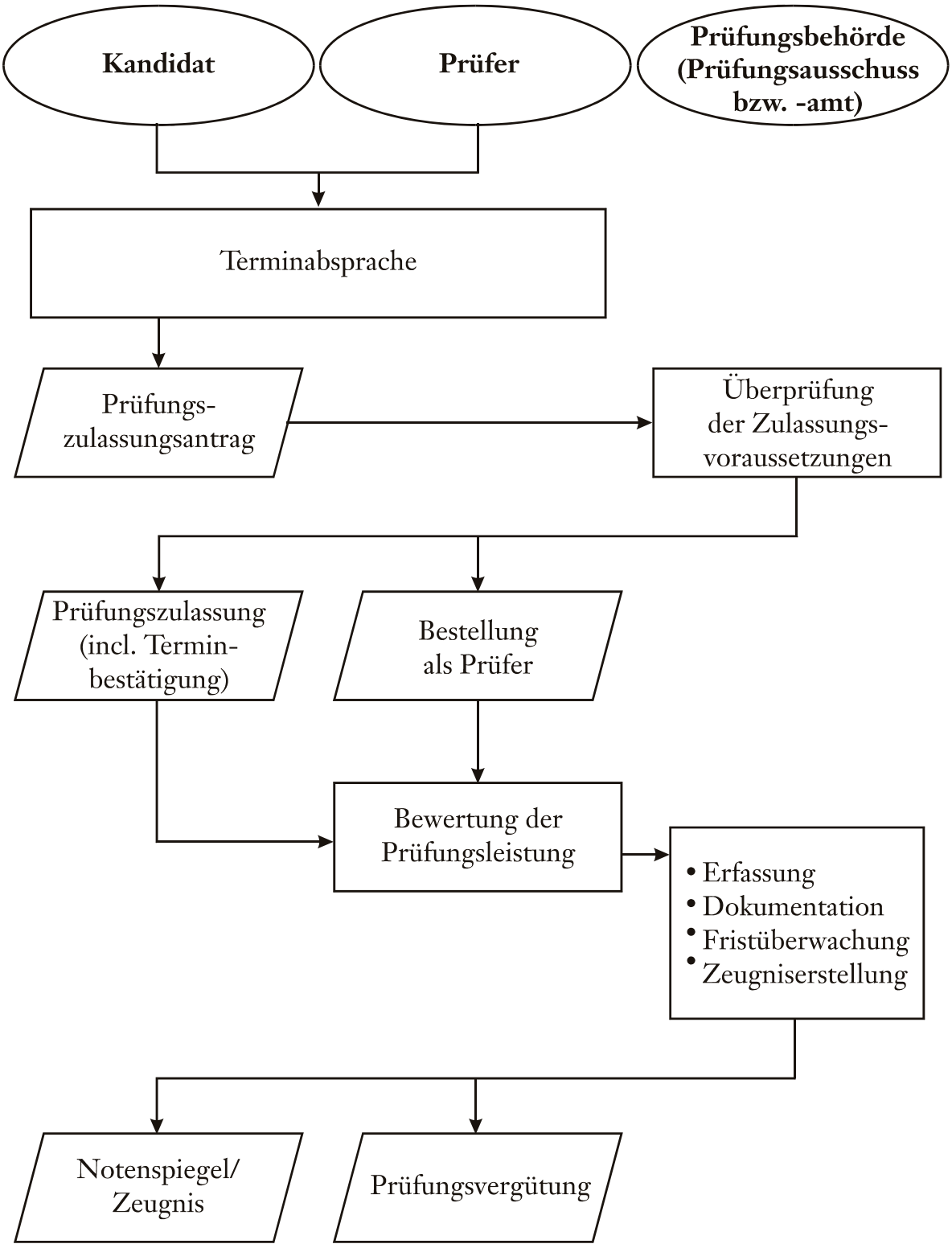
---

[126] siehe auch [Rechnungshof1994], S. 40 – 45.

[127] Die Gleichwertigkeit von Studien- und Prüfungsleistungen kann außerdem auch im Rahmen einer Akkreditierung erfolgen (siehe auch Stephan Becker in [Hailbronner2002], S. 12, Rn 28 in der Kommentierung von § 9 HRG), wodurch indirekt Anforderungen formuliert sein können, die ebenfalls aber einer rechtlichen Absicherung bedürfen.

[128] siehe auch [Rechnungshof1994], S. 90f, S. 99, S. 101, S. 104 und S. 108.

Abb. 9 Ablauf von Prüfungsverfahren



Kritisch im Sinne des Datenschutzes sind also:

- die Prüfung der Zulassungsvoraussetzung zur angemeldeten Prüfung,
- die Erfassung und Dokumentation von Prüfungsleistungen (vor allem in HISPOS) und
- die Behandlung von Sonderfällen (wie z.B. Anerkennung von Prüfungsleistungen, Abmeldungen von Prüfungen aufgrund ärztlicher Atteste, Gewährung längerer Prüfungsfristen durch Kindeserziehung, Prüfungswiederholungen, Härtefälle)

Grundlage zur Angabe personenbezogener Daten ist sowohl § 9 der Hochschul-Datenschutzverordnung wie auch Bestimmungen in der jeweils zugrunde liegenden Prüfungsordnung (auf Basis von § 51 UG). Beim Prüfungsverfahren können ausdrücklich auch Daten verarbeitet werden, die bereits im Zuge der Zulassung bzw. Rückmeldung erhoben wurden. Die im Zuge eines Prüfungsverfahrens erhobenen Daten können wiederum für Verwaltungszwecke oder auch sonstige Zwecke genutzt werden. Hierbei sind nur die wesentlichen Daten (wie Name und Matrikelnummer, aber auch Prüfungsergebnisse und -daten) 40 Jahre zu speichern, jedoch vom Zeitpunkt der Exmatrikulation (bzw. spätestens nach Abschluss des Prüfungsverfahrens) an zu sperren.

Personenbezogene Daten, die im Rahmen etwaiger Sonderfälle erhoben werden, unterliegen im Sinne von § 23 Abs. 2 LDSG bzw. § 12 Abs. 1 Hochschul-Datenschutzverordnung i.d.R. schon nach einem Semester der Löschungspflicht, sofern sie nicht unter andere Kategorien fallen, wie dies bei der Anerkennung von Prüfungsleistungen oder natürlich den Prüfungsergebnissen der letzten Prüfungswiederholung der Fall sein dürfte.

Ist neben der allgemein üblichen Anmeldung zur Prüfung durch persönliches Erscheinen mit Antragstellung vor der Prüfungsbehörde (i.d.R. dem zuständigen Prüfungsamt) auch eine Prüfungsanmeldung via Internet (z.B. mittels HISQIS) vorgesehen, muss die Hochschule sicherstellen, dass dies dem Prüfling auch wirklich möglich ist[129]. Ferner muss sichergestellt sein, dass sich im Sinne von § 126a BGB wirklich der Prüfling selbst mit einer qualifizierten elektronischen Signatur gem. § 7 SigG angemeldet hat (diese Anforderungen erfüllen insbesondere Signaturen nach ISO/IEC 9796 (elliptische Kurven bzw. El Gamal-Schema) sowie ISO/IEC 14888 (DSA)[130]).

Datenschutzrechtliche Probleme im Rahmen der Dokumentation von Prüfungsleistungen treten in erster Linie allenfalls bei schriftlichen Prüfungsleistungen auf, wenn die Noten nicht – wie bei mündlichen Prüfungsleistungen – im direk-

---

[129] siehe [Zimmerling1998], S. 3221f.
[130] nach [Fumy2000], S. 387.

ten persönlichen Gespräch, sondern durch Aushang bzw. Internet bekannt gegeben werden, da hierbei (aufgrund von § 9 Abs. 4 LDSG) die Studierenden nur ihre persönlichen Leistungen „erkennen“ dürfen[131] (die Veröffentlichung von Namens- bzw. Matrikelnummern-Listen ist folglich nicht gestattet – gleiches gilt auch für Klausurergebnisse zum Erwerb von Leistungsnachweisen[132]). Außerdem liegen bei schriftlichen Prüfungen zumindest auf Zeit in der die Prüfung abnehmenden Universitätseinheit (Lehrstuhl, Institut, Abteilung o.ä.) die Listen (häufig in elektronischer Form) vor. Nach Ablauf der Einspruchsfrist bzw. der Frist zur Einsichtnahme in die Prüfungsakten (geregelt in der Prüfungsordnung) ist hierfür aber keine Grundlage mehr gegeben, da dies sonst gegen den Grundsatz der Datensparsamkeit verstoßen würde (siehe Abschnitt 1.3.1).

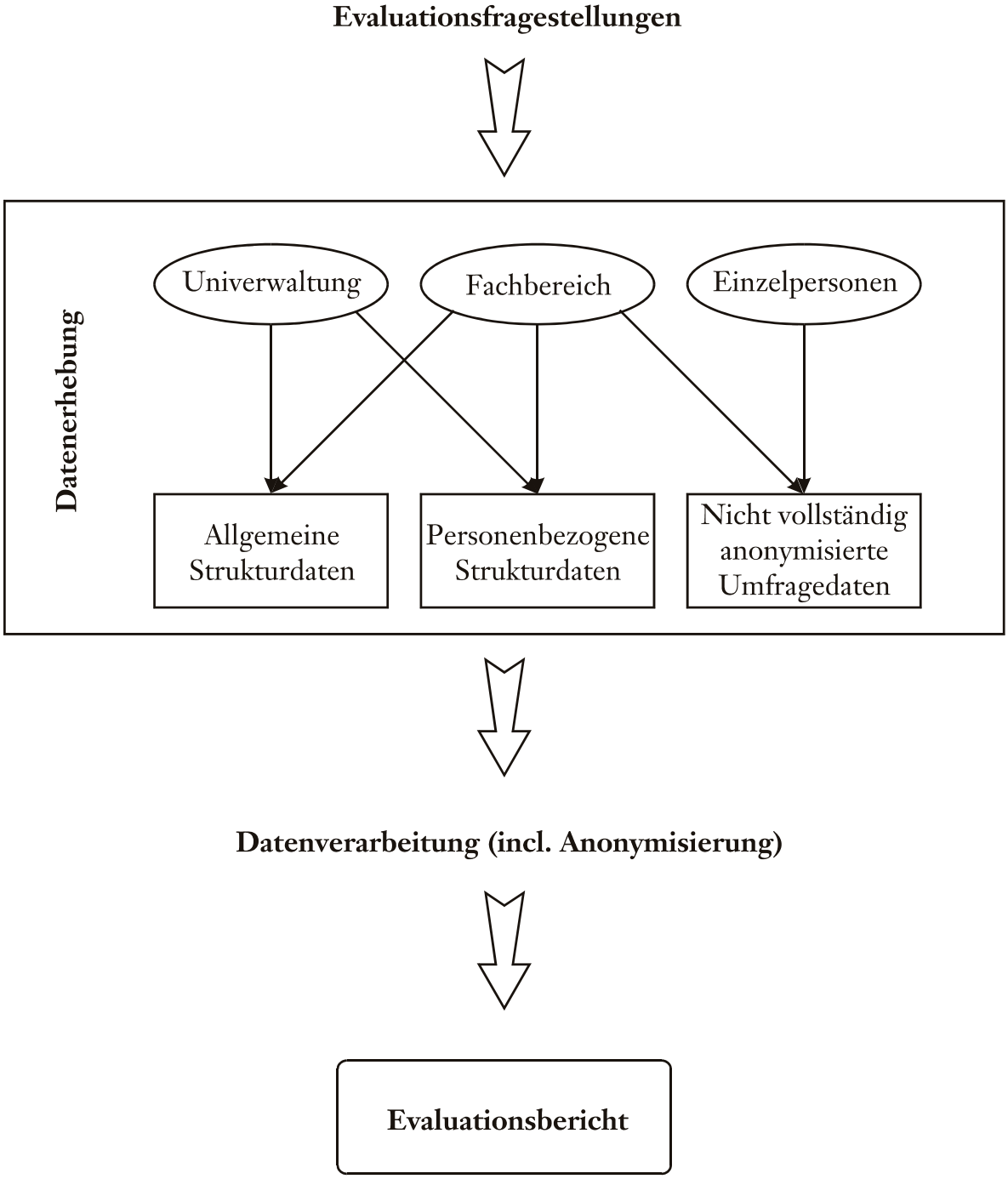
[131] siehe [LDSB2000], S. 78.

[132] siehe http://www.datenschutz.hessen.de/tb26/k16p2.htm (Stand: 10.12.2002), denn es existiert keine gesonderte Rechtsvorschrift, die dies erlaubt, und § 9 Abs. 4 LDSG ist wortidentisch zu § 10 (2) HDSG.

3.2.4 Datenschutzgerechter Umgang mit der Evaluation der Lehre

Der prinzipielle Ablauf einer (umfassenden) Lehrevaluation im Sinne von § 4a UG (siehe auch Abschnitt 2.4.3) lässt sich wie folgt darstellen:

Abb. 10 Struktureller Ablauf einer Lehrevaluation



Im Rahmen der Evaluation der Lehre sind also folgende im Sinne des Datenschutzes kritische Bereiche bei den Verfahren zur Erhebung von Daten voneinander zu unterscheiden[133]:

- Erhebung von Strukturdaten über die zu untersuchende Organisationseinheit (Universität, Fakultät, Fachbereich, Studiengang), deren Daten durch Sonderauswertungen bestehender Datenbestände in anonymisierter Form (als Statistikdaten) gewonnen werden können, wie etwa die Angabe und Entwicklung der Studierendenzahlen, der Erfolgsquoten bei Zwischen- und Abschlussprüfungen, der Betreuungsrelation zwischen Lehrenden und Lernenden, verfügbarer Lehr- und Lernflächen sowie der Geräteausstattungen. Diese Daten sind i.d.R. nicht personenbezogen, werden zum Teil im Rahmen der Hochschulstatistik bereits erhoben und sind insoweit datenschutzrechtlich unkritisch. Insbesondere erlauben die Regelungen der Hochschul-Datenschutzverordnung (vor allem § 11 Hochschul-Datenschutzverordnung) die Verarbeitung personenbezogener studentischer Daten auch für diese Zwecke.
- Erhebung, Auswertung und Bericht über personenbezogene Strukturdaten, wie etwa die Einhaltung des Lehrdeputats, die fachliche Ausrichtungen und die Prüfungsbelastung des Lehrkörpers sowie die Bereitstellung von Lehrmaterial. Diese Daten sind (faktisch) zu anonymisieren, wozu sich insbesondere die Form der Aggregation der Daten anbietet[134].
- Erhebung, Auswertung und Bericht über Umfragen zur Ermittlung insbesondere der studentischen Bewertung von Lehrindikatoren, wie Veranstaltungskritiken, Vorschläge für Lehrpreise, Darstellung der Studienbedingungen und des Studienumfeldes, zur Studienmotivation und zu den Erwartung an das Studium sowie dem Grad ihrer Einhaltung. Diese Daten weisen i.d.R. einen gewissen Grad an personenbezogenen Daten auf (sind also noch nicht vollständig anonymisiert – i.d.R. alleine schon wegen der Handschrift) und sind daher erst (faktisch) zu anonymisieren, bevor sie weitergereicht werden (es sei denn, auf dem Umfragebogen wurde ausdrücklich die unveränderte Weitergabe angekün-

---

[133] als exemplarische Beispiele wurden die Kriterien für Lehrbewertungen von Ulrich Karpen aus [Hailbronner2002], S. 31f, Rn 76 sowie eigene Erfahrungen aus der Fakultät für Informatik an der Universität Ulm (siehe z.B. Helmuth Partsch: Lehrbericht Informatik 1994 – 1998) herangezogen.

[134] siehe die Ausführungen des hessischen Datenschutzbeauftragten in http://www.datenschutz.hessen.de/o-hilfen/evaluation.htm (Stand: 10.12.02).

digt und das Ausfüllen des Bogens war freigestellt). Dies gilt sowohl für die Betroffenen wie auch für die Befragten, denn eine Vielzahl von Studierenden würde keine Antworten geben, wenn die Gefahr bestünde, dass potentielle Prüfer ihre Schrift wieder erkennen könnten[135]. Deshalb schreibt § 14 Abs. 1 LDSG vor, dass beabsichtigte Empfänger bei der Erhebung anzugeben sind. Betroffene (aus dem Lehrkörper) dürfen aufgrund des Verhältnismäßigkeitsprinzips keinesfalls „an den Pranger" gestellt werden[136], was jedoch im Rahmen einer Veröffentlichung personenbezogener Daten möglich ist[137]. Generell setzt eine Veröffentlichung personenbezogener Daten in erster Linie das Vorliegen einer Einwilligung der Betroffenen voraus[138] und nur im Ausnahmefall reicht aufgrund der Schwere des Eingriffs in dessen informationelle Selbstbestimmung (siehe Abschnitt 1.5.1) auch eine Rechtsgrundlage, die aber auf die Grundsätze des Datenschutzes Rücksicht nehmen muss (gemäß Abschnitt 1.3.1). Personalrechtliche Folgen sind allerdings in jedem Falle nichtöffentlich zu behandeln[139].

Besonders zu berücksichtigen ist, dass die Daten einerseits im Rahmen einer Selbstevaluation abgefragt werden können, als auch im Rahmen einer externen Evaluation. In beiden Fällen dürfte aber eher eine strukturelle Analyse maßgeblich sein und weniger ein Interesse an personenbezogenen Daten bestehen.

Unterschiedlich in ihrer Auswirkung sind Evaluationen, die nur im Binnenverhältnis der Universität Wirkung entfalten sollen (und folglich weit reichender geregelt werden können) gegenüber solchen, an denen staatliche Finanztransfers gebunden sind[140]. Im letzteren Fall ist bei der Berücksichtigung nicht ausschließ-

---

135 darauf verweist [Hage1996], S. 108f ausdrücklich hin.

136 so [Tinnefeld2001], S. 22.

137 überhaupt ist eine detaillierte Veröffentlichung von Lehrbewertungen höchst problematisch und birgt die Gefahr in sich, das eigentliche Ziel zu konterkarieren – siehe auch http://www.informatik.uni-ulm.de/JusoHSG/evaluation.htm (Stand: 10.12.2002).

138 so [Jendro2000], S. 28 (allerdings in Ermangelung spezifischer Rechtsgrundlagen in Berlin; in Baden-Württemberg lässt dagegen § 4a UG eine Veröffentlichung auf der Grundlage einer universitären Satzung zu).

139 so auch der hessische Datenschutzbeauftragte in http://www.datenschutz.hessen.de/o-hilfen/evaluation.htm (Stand: 10.12.02), der jedoch bei einer Lehrbewertung nach fachlichen Kriterien keinen Eingriff in das informationelle Selbstbestimmungsrecht sieht, selbst wenn dienstliche Konsequenzen daraus gezogen werden. Ein "an den Pranger"-Stellen von Betroffenen ist seiner Ansicht nach dennoch nicht zulässig.

140 siehe auch Hanns Seidler in [Hailbronner2002], S. 19ff, Rn 31 – 35 im Kommentar zu § 6 HRG. So sieht [Tinnefeld2001], S. 25 beispielsweise schon eine zu detaillierte Berichtspflicht gegenüber dem Land als Verstoß gegen die Wissen-

lich quantitativer Kriterien ein wissenschaftsadäquates Bewertungsverfahren unter Gleichrangigen (Peers) vonnöten[141].

Es ist daher davon auszugehen, dass im Rahmen der Lehrberichte (nach § 25 Abs. 4 UG) keine personenbezogenen Daten mit Ausnahme der in § 125a Abs. 5 UG aufgeführten Personaldaten angegeben werden dürfen (denn der entsprechende Abschnitt ist ausdrücklich aus § 4a Abs. 2 UG ausgenommen), soweit die Betroffenen nicht schriftlich einer Veröffentlichung ausdrücklich zugestimmt haben[142].

Soweit nicht spezifische Regelungen angewendet werden können (z.B. im Rahmen der Hochschul-Datenschutzverordnung) sind personenbezogene Daten zu löschen, wenn sie nicht mehr zur Erfüllung ihrer Aufgabe erforderlich sind (§ 23 LDSG). Sind erhobene Daten nicht (oder nur mit erheblichem Aufwand) zu deanonymisieren, existiert keine vorgesehene Löschungsfrist, es sei denn, mit Betroffenen wurden entsprechende Fristen vereinbart.

Bei Akkreditierungsverfahren ist analog zur Evaluation vorzugehen, da unter datenschutzrechtlichen Aspekten ein Akkreditierungsverfahren im Wesentlichen einer externen Evaluation entspricht. Allerdings fehlen hierzu teilweise für Eingriffe in das informationelle Selbstbestimmungsrecht nötige rechtliche Bestimmungen, die für Evaluationen explizit vorgesehen sind (und für Akkreditierungen allenfalls durch freundliche Auslegung anwendbar sind[143]). Außerdem unterscheidet sich (neben der Zielsetzung der Qualitätskontrolle) fundamental der Blickwinkel: bei Evaluationen sind in erster Linie Fachbereiche Untersuchungsgegenstand, bei Akkreditierungen dagegen Studiengänge[144]. Häufig bilden aber Evaluationen die Grundlage für Akkreditierungen[145].

---

schaftsfreiheit an.

141 Ulrich Karpen lehnt die Einbeziehung studentischer Lehrbewertungen in lehrleistungsorientierte Finanzzuweisungen in [Hailbronner2002], S. 29f, Rn 73 im Kommentar zu § 5 HRG ab, während Hanns Seidler in [Hailbronner2002], S. 11, Rn 19 diesem widerspricht, sofern entsprechende Regelungen in universitären Satzungen getroffen wurden.

142 zumal der Effekt einer Veröffentlichung hinsichtlich des Zieles, der Verbesserung der Lehre, umstritten ist – siehe [Hage1996], S. 146.

143 denn in der Begründung zur Änderung des Universitätsgesetzes wurde nur eine Umsetzung von § 6 HRG angegeben (siehe Landtags-Drucksache 12/4404, S. 302f) und dieser Paragraph beinhaltet eben nicht Fragen der Akkreditierung.

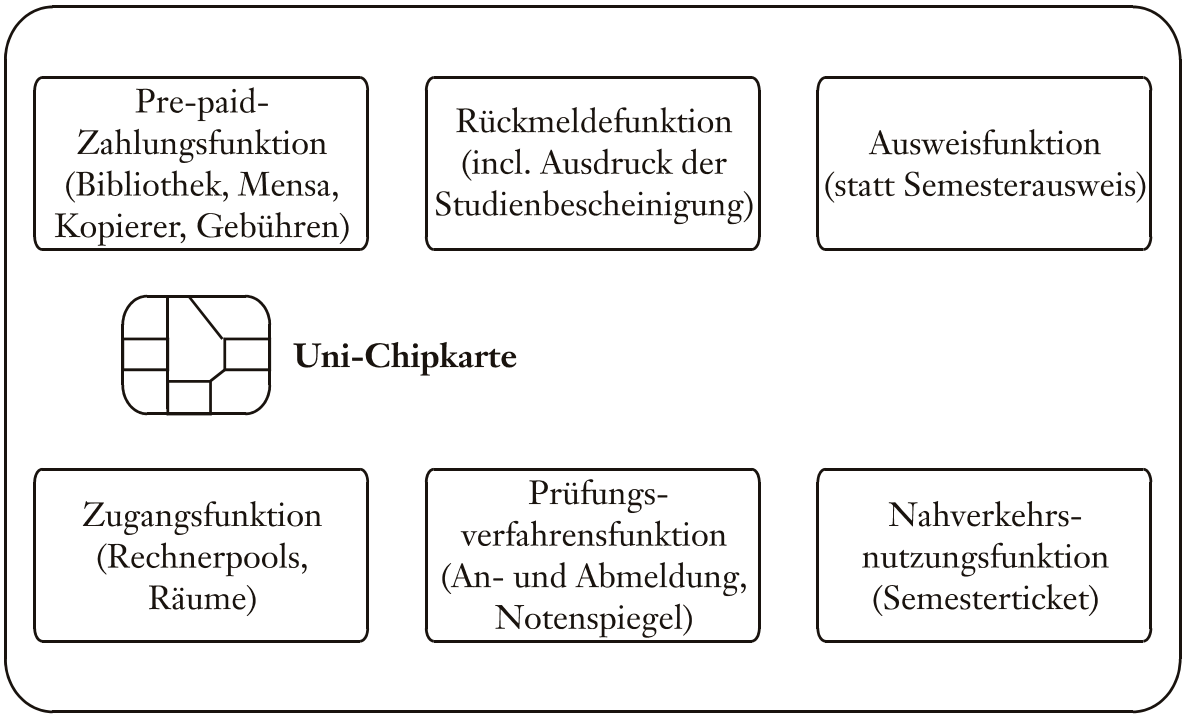
144 siehe hierzu exemplarisch [Reuke2001], S. 36.

145 so [HRK2000], S. 9.

3.2.5 Datenschutzgerechter Umgang mit Chipkarten bzw. bei ihrer Einführung

Zunehmend kommen an den Universitäten (für Studierende) mobile Datenträger (Chipkarten) zum Einsatz. Diese erfüllen i.d.R. folgende Funktionen[146]:

Abb. 11 Mögliche Funktionen einer Chipkarte an einer Hochschule



Die von einem solchen Einsatz Betroffenen sind auf ihre Rechte (siehe Abschnitt 1.5.2) ausdrücklich hinzuweisen, über Maßnahmen und Folgen des Verlustes einer Chipkarte aufzuklären und müssen erkennen können, wann Daten von der Chipkarte gelesen und verarbeitet werden (§5 Abs. 2 LDSG).

Nach § 12 LDSG hat eine Vorabkontrolle vor Einführung von Chipkarten durch den (behördlichen) Datenschutzbeauftragten stattzufinden. Im Rahmen dieser Vorabkontrolle ist für das zum Einsatz kommende Chipkarten-System sicherzustellen, dass keine besondere Gefahren für das Persönlichkeitsrecht bestehen. Deshalb ist u.a. eine fristgerechte Löschung der gespeicherten Daten sowie von Protokolldaten, die durch die Chipkarte ausgelöst werden, zu gewährleisten und zu verhindern, dass Unbefugte Daten lesen können (dies ist insbesondere bei einer Multifunktionskarte wichtig)[147]. Zumindest implizit sind demnach im Rahmen der Vorabkontrolle auch die weitergehenden Rechte aus § 6c BDSG zu berücksichtigen: Betroffenen ist außerdem in allgemein verständlicher Form die Funktionsweise und die Art der zu verarbeitenden personenbezogenen Daten mitzutei-

---

[146] siehe auch die Übersicht des HIS zum aktuellen Stand der Einführung von Chipkarten (Stand: 05.10.2002) auf: http://www.his.de/Abt1/HISQIS/einfstand.pdf (Stand: 10.12.2002).

[147] siehe [LDSB2000], S. 20ff und [LDSB2001], S. 36.

len und es muss unentgeltlich und im angemessenen Umfang die Möglichkeit zur Abfrage der auf der Chipkarte gespeicherten Daten eingeräumt werden[148].

Als bundesweit erstmals Chipkarten in der Erprobung waren, wurden sie als sehr risikoreich eingestuft[149]. Deshalb sollte es den Betroffenen freigestellt sein, ob sie eine Chipkarte erhalten und damit nutzen wollen oder nicht[150]. Die angebotenen Funktionen sollten folglich auch ohne Chipkarte (und ohne etwaige Benachteiligungen) nutzbar sein, die Möglichkeit zur Erstellung von Nutzungsprofilen ist zu verhindern. Es ist daher davon auszugehen, dass diese Aspekte im Rahmen der Vorabkontrolle Berücksichtigung finden, obwohl sie nicht gesetzlich vorgeschrieben sind.

Hinsichtlich der Löschungsfristen gelten die jeweiligen Fristen zu den jeweiligen Funktionen: in den meisten Fällen also § 12 Hochschul-Datenschutzverordnung, ansonsten § 23 LDSG.

An dieser Stelle wurde davon ausgegangen, dass Chipkarten in erster Linie für Studierende eingeführt wurden bzw. werden. Für Beschäftigte ergeben sich u.U. noch andere (vor allem personalrechtliche) Aspekte, die zu berücksichtigen wären (siehe auch Kapitel 3.4).

Die Arbeitsgruppe Chipkarten des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben folgende Mindestanforderungen für ein Sicherheitskonzept für Chipkarten formuliert[151]:

- die Chipkarte selbst muss fälschungssichere Authentisierungsmerkmale (Unterschrift und Foto des Besitzers, Hologramme) und Sicherheitsmechanismen gegen unbefugte Auswertungen ihrer Inhalte bzw. Sicherheitsfunktionen aufweisen (also insbesondere durch kryptographische Methoden gesichert sein),
- Zugriffs- und Nutzungsberechtigungen sind durch die Chipkarte selbst zu steuern,
- die Kommunikation mit Nutzungsgeräten ist insbesondere durch kryptographische Maßnahmen und einer abhör- und

---

148 auf Letzteres verweist ausdrücklich [LfD2000], S. 9

149 siehe [Sokol1997], S. 14.

150 diese Wahlmöglichkeit wird in Baden-Württemberg im § 5 (2) LDSG aber im Gegensatz zu § 29a DSG NRW nicht gesetzlich gewährleistet. Sie ist aber für die Akzeptanz von Chipkarten weiterhin von essentieller Bedeutung – siehe auch: http://www.informatik.uni-ulm.de/JusoHSG/chipkarten.htm (Stand: 10.12.2002).

151 siehe "Anforderungen zur informationstechnischen Sicherheit bei Chipkarten" zum 02.12.1996 auf http://www.datenschutz.hessen.de/o-hilfen/chipkart.htm (Stand: 10.12.2002); veröffentlicht im 26. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten unter Ziffer 26.

fälschungssicheren Datenübertragung abzuschotten (siehe Norm ISO/IEC 9798),
- zur Verschlüsselung von Daten, Aufnahme von Signaturfunktionen auf der Chipkarte und Generierung von Zufallszahlen sind allgemein anerkannte und veröffentlichte Algorithmen zu verwenden (also symmetrische Verschlüsselungsalgorithmen wie DES oder asymmetrische Verfahren wie RSA; siehe auch ISO/IEC 7816),
- unterschiedliche Anwendungen dürfen sich nicht gegenseitig beeinflussen,
- der Chipkartenhersteller darf nicht über ein „Gesamtwissen" verfügen,
- es sind zumindest Wahlmöglichkeiten anonymer Nutzungsmöglichkeit vorzusehen,
- gespeicherte Daten und Funktionalitäten einer Chipkarte sollten von Betroffenen auf neutralen und zertifizierten Systemumgebungen einsehbar sein,
- die gesamte mit der Chipkarte in Verbindung stehende Infrastruktur ist zu dokumentieren und strafrechtlich abzusichern,
- alle datenkritischen Systemkomponenten sind regelmäßig zu überprüfen,
- die Echtheit und Gültigkeit von Informationsstrukturen sind regelmäßig zu kontrollieren,
- sicherheitsrelevante Karten (z.B. mit Zahlungsfunktion) sind über den gesamten „Lebenszyklus" der Chipkarte kryptographisch zu sichern.

3.2.6 Datenschutzgerechter Umgang bei besonderen Berichtspflichten

Die Universitätsverwaltung unterliegt (auf der Grundlage von § 125a Abs. 3 UG) besonderen Berichtspflichten und ist dazu angehalten, insbesondere Studierendendaten, die gemäß der Hochschul-Datenschutzverordnung auch für sonstige Zwecke verarbeitet werden dürfen, in folgenden Fällen an Dritte weiterzuleiten:

- zur Überprüfung des Studierendenstatus von wissenschaftlichen Hilfskräften, zumal deren Beschäftigungsdaten an die jeweiligen Sozialträger zu übermitteln sind (gem. § 3 DEÜV – siehe auch Abschnitt 3.4.3).
- für Einzelfall-Anfragen von Polizeibehörden, Staatsanwaltschaften, Gerichten, Behörden der Gefahrenabwehr, Justiz-Vollzugs-Anstalten und zur Durchsetzung öffentlich-rechtlicher Ansprüche nach § 69 SGB X i.V.m. § 67a Abs. 2 X SGB

und § 68 SGB X[152], sowie für Auskunftspflichten nach § 47 BAföG, § 10 BKGG, § 25 WoGG und § 116 BSHG[153] und zur Wehrüberwachung nach § 24 Wehrpflichtgesetz.

Auch an den Universitäten in Baden-Württemberg wurde nach den Terroranschlägen vom 11. September 2001 in New York eine **Rasterfahndung** zur vorbeugenden Bekämpfung von Straftaten durch das Landeskriminalamt auf der Grundlage von § 40 PolG in Gang gesetzt. Bei einer Rasterfahndung werden Daten aus unterschiedlichen Datenbeständen anhand eines Rasters (entsprechend dem konkret vorliegenden Täterprofil) miteinander verglichen, um Personen herauszufiltern, von denen möglicherweise eine Gefährdung der inneren bzw. äußeren Sicherheit ausgehen könnte. Die Maßnahme Rasterfahndung ist in Baden-Württemberg zur Abwehr von Straftaten erheblicher Bedeutung erlaubt[154] (gem. § 22 Abs. 5 PolG), andere Bundesländer schreiben außerdem eine gegenwärtige Gefahr vor[155]. Strittig ist jedoch, ob im Zuge der Rasterfahndung auch Daten abweichend zu den konkret gestellten Anforderungen übermittelt werden dürfen[156], wie es z.B. § 40 Abs. 2 PolG nur zulässt, wenn die Aussonderung aus dem zugrunde liegenden Datenbestand nur mit einem unverhältnismäßigen Aufwand verbunden ist. Nicht angeforderte Daten dürfen nicht weiter verarbeitet werden (§ 40 Abs. 2 PolG) und sind unverzüglich zu löschen (§ 40 Abs. 4 PolG i.V.m. § 38 Abs. 1 PolG), die angeforderten Studierendendaten sind dagegen i.d.R. nach 2 Jahren (§ 38 Abs. 4 PolG), spätestens jedoch nach 10 Jahren zu löschen (§ 38 (2 und 3) PolG).

3.2.7 Datenschutzgerechter Umgang mit sonstigen Studierendendaten

Im laufenden Betrieb einer Universität fallen noch eine Reihe weiterer Anlässe an, zu denen personenbezogene Daten verarbeitet werden, zu denen in Ermangelung spezifischer Rechtsvorschriften die Regelungen des LDSG heranzuziehen sind:

- nach § 51 Abs. 2 UG ist in den studiengangbezogenen Prüfungsordnungen festzulegen, welche **Leistungsnachweise**

---

[152] siehe [Bergmann2002], S. 22, Rn 26f im Kommentar zu § 67a SGB X im Teil VII, Bereichsspezifischer Datenschutz im Sozialgesetzbuch

[153] siehe [Bergmann2002], S. 25, Rn 6 im Kommentar zu § 67b SGB X im Teil VII, Bereichsspezifischer Datenschutz im Sozialgesetzbuch.

[154] ihr Effekt wird allerdings vielfach in Frage gestellt, siehe z.B. [LDSB2001], S. 13.

[155] siehe [Gerling2001], S. 746; als zeitlich letzte Instanz hat das Kammergericht Berlin in ihrem Beschluss Rasterfahndung vom 16.04.2002 (1 W 89 bis 98/02), abgedruckt in Datenschutz und Datensicherheit 11/2002, S. 692 – 700, übereinstimmend mit einigen anderen Gerichtsinstanzen anderer Bundesländer das Vorliegen der gegenwärtigen Gefahr bejaht.

[156] siehe hierzu insbesondere [Gola2002], S. 2437 mit Verweis auf [Achelpöhler2002], S. 244f: in diesem Gerichtsbeschluss wurde es als unverhältnismäßig angesehen, wenn die Daten eines deutschen Staatsangehörigen übermittelt werden, obwohl nach Personen mit anderen Staatsangehörigkeiten gesucht wird.

zur Prüfungszulassung erforderlich sind (siehe auch Abschnitt 3.2.3). Bevor diese Daten gemäß § 9 Hochschul-Datenschutzverordnung zur Prüfungsanmeldung vorzulegen sind, können diese Leistungsnachweise noch bei den Stellen vorliegen, die sie ausgestellt haben, wenn sie der Prüfling bis dahin noch nicht abgeholt und in seinem Studienbuch abgelegt hat. Gemäß § 23 Abs. 4 LDSG ist davon auszugehen, dass die Ableistung der Prüfung und die Vorlage der hierzu erforderlichen Leistungsnachweise ein schutzwürdiges Interesse des Betroffenen darstellt, so dass diese Leistungsnachweise nicht vorzeitig gelöscht werden sollten, sondern erst mit vollzogener Exmatrikulation des Studierenden bzw. dem Abschluss des Prüfungsverfahrens gemäß § 12 Abs. 1 Hochschul-Datenschutzverordnung. Nach § 12 Hochschul-Datenschutzverordnung sind diese Daten erst nach der Exmatrikulation (spätestens aber nach Abschluss des Prüfungsverfahrens) zu löschen. Das wirft die Frage auf, ob die Leistungsnachweise ausstellende Stelle in regelmäßigen Abständen etwa durch Nachfrage bei der Universitätsverwaltung festzustellen hat, welcher Studierende noch eingeschrieben ist bzw. wessen Prüfungsverfahren noch nicht abgeschlossen ist. In den Prüfungsordnungen dürften der Lösung dienliche Regelungen nur selten zu finden sein. Es wird daher vorgeschlagen, bei der Universitätsverwaltung nach 5 Jahren (in Anlehnung an § 35 Abs. 2 BDSG) anzufragen, ob der Studierende noch immatrikuliert ist (bzw. sich noch im Prüfungsverfahren befindet) und bei negativer Antwort diese Daten zu löschen. Analog ist mit Klausurergebnissen, Praktikumsberichten, Softwaredokumentationen, Teilnehmerlisten etc. verfahren, aufgrund derer ein Leistungsnachweis ausgestellt wurde. Anmeldungen für Kurse[157] sind dagegen binnen eines Semesters zu löschen, denn dieses Verfahren ist mit der Erstellung des Leistungsnachweises abgeschlossen, sofern nicht etwa in den Prüfungsordnungen Beschränkungen für die Anzahl von Kurswiederholungen existieren. In einigen Studiengängen können gemäß vorliegender Prüfungsordnungen Prüfungen über Seminararbeiten abgehalten werden. Deshalb wird an dieser Stelle vorgeschlagen, analog zu den Leistungsnachweisen zu verfahren.

[157] dies gilt auch für nicht leistungsnachweis-relevante Anmeldungen wie Hochschulsport, Sprachkurse etc.

- Gemäß § 49 UG werden Studierende und studierwillige Personen von der zentralen wie auch der fachbezogenen **Studienberatung** hinsichtlich etwaiger Fragen zum Studium unterstützt. Dies kann auch z.B. mittels EDV-gestützten Systemen erfolgen – in diesem Fall siehe auch Kapitel 3.3. Personenbezogene Daten im Rahmen der Studienberatung dürfen nach § 49 Abs. 4 UG nur mit ausdrücklicher Einwilligungserklärung der Betroffenen weitergeleitet werden. Die Verarbeitung von anderen Studierendendaten, die insbesondere im Zusammenhang mit den Prüfungsverfahren erhoben wurden (siehe Abschnitt 3.2.3), ist nur zulässig, wenn sie nach der Hochschul-Datenschutzverordnung erlaubt ist oder vom Betroffenen genehmigt wurde. In Ermangelung etwaiger bereichsspezifischer Rechtsvorschriften, wie lange diese Daten verarbeitet werden dürfen, ist davon auszugehen, dass die hierbei erhobenen Daten nach einem Semester im Sinne von § 23 LDSG gelöscht werden, sofern vom Betroffenen nicht ausdrücklich längere Verarbeitungsfristen genehmigt wurden.
- Nach § 24 Abs. 6 UG sind Studierende berechtigt, **Beschwerden** über Mängel bei der Durchführung des Lehr- und Studienbetriebs bzw. die Nichteinhaltung von Prüfungsvorschriften gegenüber dem Studiendekan zu äußern. Dabei kann auch verlangt werden, dass die Beschwerden in der zuständigen Studienkommission behandelt werden. Es ist davon auszugehen, dass diese bei der Überprüfung und Beratung vertraulich behandelt werden (gemäß § 112 Abs. 4 UG). Es wird daher an dieser Stelle empfohlen, diese Beschwerden nur pseudonymisiert weiter zu leiten. Im Rahmen von solchen Beschwerden angefallene personenbezogene Daten sind unverzüglich nach Unterrichtung des Betroffenen über das Ergebnis der Überprüfung und Beratung gemäß § 23 LDSG zu löschen.
- In besonderen Fällen kann es sinnvoll sein, Studierenden **Mitteilungen über den laufenden Lehrbetrieb** zukommen zu lassen, wenn etwa eine Lehrveranstaltung verlegt wurde oder ausfällt. Sofern die Betroffenen hierzu nicht im Vorhinein ihr Einverständnis erklärt haben, ist die Übermittlung der personenbezogenen Daten an die anfragende Universitätseinrichtung in diesem Fall dennoch im Interesse des Betroffenen gemäß § 125a UG und daher zulässig. Allerdings hat diese Stelle die Daten unverzüglich nach Mitteilung des Betroffenen zu löschen, da keine Datensammlung

auf Vorrat zulässig ist. Es ist aber auch ein Adressmittlungsverfahren (siehe Abschnitt 3.1.1) zulässig.

3.3 Datenschutz im Bereich der Nutzung der Technik

3.3.1 Datenschutzgerechter Umgang bei der Nutzung von Soft- und Hardware

Hinsichtlich des Umgangs mit Hard- und Software sind zwei unterschiedliche Sichtweisen zu unterscheiden:

- der datenschutzgerechte Umgang mit personenbezogenen Daten im Rahmen dienstlicher Aktivitäten (die hierbei zu beachtenden Aspekte sind jeweils in den Einzel-Themen aufgelistet) und
- der datenschutzgerechte Umgang des Einzelnen mit seinen eigenen personenbezogenen Daten (in diesem Fall gilt weder das LDSG noch das BDSG, da dann die Erhebung, Verarbeitung oder Nutzung ausschließlich für persönliche Tätigkeiten erfolgt gem. § 1 Abs. 2 BDSG; erst in der Interaktion mit Dritten erhalten die Daten Relevanz und in diesem Fall wurden an den entsprechenden Stellen dieser Arbeit die Einzel-Themen behandelt).

Zur datenschutzkonformen Einrichtung von Hard- und Software durch die verantwortende Stelle sind zu berücksichtigen:

- Hinweise des Landesbeauftragten für den Datenschutz Baden-Württemberg zur Datensicherheit beim Einsatz von Personal Computern (Stand: 22.11.1996) [158], auch veröffentlicht im Anhang 9 des 17. Tätigkeitsberichts des Landesbeauftragten für den Datenschutz in Baden-Württemberg, Stuttgart, 1996, S. 105 – 107.
- Hinweise des Landesbeauftragten für den Datenschutz Baden-Württemberg zum Umgang mit Passwörtern (Stand: 15.09.2000)[159]

Hilfreich ist auch die Checkliste für Datenschutzmaßnahmen in:

- Wolfram Gass: Datenschutzrecht – Internet-Sicherheit für Unternehmen, Ulm, Rechtsanwälte Gass & Partner, 2002 (Stand: 05.03.2002), S. 81 – 86.

---

[158] siehe auch die aktuellere Version der Hinweise des Landesbeauftragten für den Datenschutz Baden-Württemberg zur Datensicherheit beim Einsatz von PC und lokalen Netzwerken (Stand: 4. September 2002) auf http://www.baden-wuerttemberg.datenschutz.de/material-lfd/pcln.html (Stand: 10.12.2002).

[159] siehe auch: http://www.baden-wuerttemberg.datenschutz.de/material-lfd/passwort.html (Stand: 10.12.2002)

An dieser Stelle wird daher nur auf besonders wichtige Aspekte hingewiesen. So muss die verantwortliche Stelle stets darauf achten, dass die Datensicherheitsmaßnahmen greifen (siehe Abschnitt 1.5.3). Das gilt auch für Funknetzwerke (WLAN)[160].

Es ist daher anzuraten, in die Nutzungsbestimmungen von Hard- und Software Hinweise zum Datenschutz aufzunehmen und auf freiwilliger Basis eine Datenschutzerklärung abzugeben. Im Rahmen des Datenschutz-Audits mittels einer Datenschutzerklärung teilt die datenverarbeitende Universitätseinrichtung mit, aufgrund welcher Rechtsgrundlage sie Daten erhebt, wie sie diese Daten verarbeitet und welche Risiken zur Datensicherheit bestehen.

Vor Einführung eines automatisierten Abrufverfahrens (kennzeichnend hierfür ist die programmgesteuerte Datenverarbeitung) ist (nach § 8 LDSG) der zuständige (behördliche) Datenschutzbeauftragte zu informieren und eine Vorabkontrolle (nach § 12 LDSG) durchzuführen. Dabei ist sicherzustellen, dass durch das zum Einsatz kommende System keine besonderen Gefahren für das Persönlichkeitsrecht entstehen. In diesem Zusammenhang ist eine fristgerechte Löschung der gespeicherten Daten sicherzustellen und zu verhindern, dass Unbefugte Daten lesen können.

Außerdem ist beim zuständigen (behördlichen) Datenschutzbeauftragten gemäß § 11 LDSG ein Verfahrensverzeichnis zu führen, in dem dokumentiert ist, welche personenbezogene Daten (Art der Einzelmerkmale und Kreis der Betroffenen) die Universitätseinrichtung mit Hilfe welcher automatisierter Verfahren (unter Verwendung welcher Hard- und Software incl. der Vernetzung) auf welche Weise (aufgrund welcher Rechtsgrundlage sowie zu welchem Zweck) verarbeitet und welche Datenschutzmaßnahmen (insbesondere zur Datensicherung) sie dabei getroffen hat[161]. Ferner ist aufzuführen, wer als Empfänger der Daten vorgesehen ist, welche Fristen für Löschung bzw. Sperrung gelten und wer zugriffsberechtigt ist.

Es ist ferner darauf zu achten[162], dass nur geeignete Systemkomponenten zum Einsatz kommen, mit denen insbesondere die nötigen Datensicherheitsmaßnahmen ergriffen werden können, und nur die zur konkreten Aufgabenstellung erforderliche Hard- und Software installiert wird. Schließlich ist sicherzustellen, dass in Ein- und Ausgabemasken nur solche Daten eingegeben bzw. ausgegeben werden können, die für die konkrete Aufgabe benötigt werden, und praxisgerech-

---

[160] siehe hierzu [Dornseif2002], S. 226ff.

[161] siehe hierzu: Hinweise des Landesbeauftragten für den Datenschutz Baden-Württemberg zum Verfahrensverzeichnis (Stand: 31.10.2000) bzw. die aktuellere Version auf http://www.baden-wuerttemberg.datenschutz.de/material-lfd/verfahrensverzeichnis.html (Stand: 10.12.2002)

[162] siehe http://www.baden-wuerttemberg.datenschutz.de/material-lfd/pcln.html (Stand: 10.12.2002).

te Löschungsfunktionen eingebaut sind. Es sollte zumindest angezeigt werden können, welche Benutzer Zugriffsrechte haben, und eine vollständige und aussagekräftige Dokumentation der miteinander interagierenden Komponenten geben.

Über einzelne datenschutzrechtliche Aspekte innerhalb des Computerrechts informiert:

- Wolfgang Kilian und Benno Heussen: Computerrechts-Handbuch, Loseblattsammlung, München, Verlag C. H. Beck, 2002, Stand: 15. März 2002.

Über einzelne datenschutzrechtliche Aspekte innerhalb des Multimediarechts informiert:

- Thomas Hoeren und Ulrich Sieber: Handbuch Multimedia-Recht, Loseblattsammlung, München, Verlag C. H. Beck, 2002, Stand: Dezember 2001.

Regelmäßig finden sich in der Neuen Juristischen Wochenschrift Berichte über rechtliche Entwicklungen aus diesen Themen. Zuletzt sind dort insbesondere erschienen:

- Abbo Junker: Die Entwicklung des Computerrechts in den Jahren 2000/2001, in: Neue Juristische Wochenschrift 41/2002, S. 2992 – 2999.
- Dieter Dörr und Nicole Zorn: Die Entwicklung des Medienrechts, in: Neue Juristische Wochenschrift 39/2001, S. 2837 – 2854.

Da viele der dort angesprochenen Themen nicht von Universitäts-Spezifika handeln, wurde bewusst auf eine nähere Darstellung wichtiger juristischer Fragen hieraus verzichtet.

3.3.2 Datenschutzgerechter Umgang bei Datenübertragungen via Internet/Intranet

Einen detaillierten Überblick über den aktuellen Stand der datenschutzrechtlichen Vorgaben für das Internet (und vereinzelte Vorschläge für datenschutzgerechten Umgang) liefert:

- Peter Schaar: Datenschutz im Internet, München, Verlag C. H. Beck, 2002 (Stand: Dezember 2001).

Eine Orientierungshilfe für Datenschutzfragen bei der Nutzung von Internet und Intranet öffentlicher Verwaltungen (wie z.B. Hochschulen) bieten:

- Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder: Datenschutz bei der Nutzung von In-

ternet und Intranet, Schwerin, CLUB WIEN und cw Obotritendruck, 2000 (Stand: Dezember 2000).

- Hinweise des Landesbeauftragten für den Datenschutz Baden-Württemberg zu Internet und Datenschutz (Stand: 5. September 2002)[163].

Einen ersten Überblick über hilfreiche internationale Standards zur Datensicherheit (mit besonderem Schwerpunkt auf kryptographische Verfahren) liefert:

- Walter Fumy: Von Common Criteria bis zu elliptischen Kurven – Sicherheitsstandards von ISO/IEC JTC 1/SC 27, in: Datenschutz und Datensicherheit 7/2000, S. 385 – 391.

Auf eine Darstellung der jeweiligen Aspekte wird daher im Rahmen dieser Arbeit verzichtet.

Regelmäßig finden sich in der Neuen Juristischen Wochenschrift Berichte über rechtliche Entwicklungen aus diesem Themenkomplex. Zuletzt ist dort erschienen:

- Helmut Hoffmann: Die Entwicklung des Internet-Rechts von Anfang 2001 bis Mitte 2002, in: Neue Juristische Wochenschrift 36/2002, S. 2602 – 2610, als Fortsetzung der Beilage der Neuen Juristischen Wochenschrift 14/2001.

Da viele der dort angesprochenen Themen nicht von Universitäts-Spezifika handeln, wurde bewusst auf eine nähere Darstellung wichtiger juristischer Fragen hieraus verzichtet.

3.3.3 Datenschutzgerechter Umgang mit sonstigen technischen Einrichtungen

Es würde an dieser Stelle ebenfalls zu weit führen, für alle weiteren relevanten technischen Einrichtungen darzustellen, welche Datenschutzbestimmungen wie zu beachten sind, zumal Telefon, Telefax etc. keine Universitäts-Spezifika darstellen. Es wird deshalb an dieser Stelle empfohlen, insbesondere diese Quelle näher zu studieren:

- Bundesbeauftragte für den Datenschutz: Datenschutz in der Telekommunikation, BfD-Info 5, 5. Auflage, Magdeburg, Gebrüder Garloff, 2001 (Stand: September 2001).

Auf eine Darstellung der jeweiligen Aspekte wird daher im Rahmen dieser Arbeit verzichtet.

---

[163] siehe hierzu: http://www.baden-wuerttemberg.datenschutz.de/material-lfd/internet.html (Stand: 10.12.2002)

3.4 Datenschutz im Bereich der Verwaltung

3.4.1 Umgang mit Personaldaten an einer Universität

An einer Universität gibt es zahlreiche, rechtlich unterschiedlich zu behandelnde Beschäftigungsverhältnisse[164]. In einzelnen Rechtsfragen unterscheiden sich zum Teil die Bestimmungen über die Beamten im gehörigen Maße von denen anderer Beschäftigungsverhältnisse. Im Rahmen der Neufassung des Landesdatenschutzgesetzes wurde jedoch ein erster Schritt in Richtung einer Harmonisierung vorgenommen[165]: Für Beamte ist der Umgang mit deren Personalakten vorrangig vor dem LDSG geregelt in den §§ 113 bis 113f LBG; gemäß § 36 Abs. 2 LDSG gelten diese Bestimmungen entsprechend für die anderen Beschäftigten, sofern keine besonderen Rechtsvorschriften oder tarifliche Vereinbarungen andere Regelungen vorsehen.

Für das universitäre Personal, das nicht den Professoren, Hochschuldozenten, Gastprofessoren, Oberassistenten, Oberingenieuren, wissenschaftlichen und künstlerischen Assistenten bzw. Lehrbeauftragten an Hochschulen zugeordnet werden kann[166], ist deshalb die Rahmen-Dienstvereinbarung über Einführung, Einsatz und Ausbau der Informations- und Kommunikationstechnik in den Universitäten des Landes Baden-Württemberg (IuK-R-DV) vom 16.12.1999 vorrangig. Bei Beschäftigten, die gehobene Funktionen in der Universität wahrnehmen (dies trifft vor allem auf diejenigen zu, für die die IuK-R-DV nicht gilt), dürfen nach § 125a UG in Veröffentlichungen ohne deren Einwilligung nur Angaben über ihre dienstliche Erreichbarkeit (Name, Amts-, Dienst- und Funktionsbezeichnung sowie Telefon-/Telefax-Nummer, e-mail-/Internet-Adressen) angegeben werden, sofern sie der Veröffentlichung nicht widersprochen haben und ihr Interesse höher als das der Universität zu gewichten ist. Darüber hinausgehende personenbezogene Daten dürfen nur auf Einwilligung der Betroffenen veröffentlicht werden.

Bei Professoren gibt es nochmals Sonderregelungen, da diese berufen und nicht im herkömmlichen Sinne eingestellt werden (siehe insbesondere § 66 UG).

Zum Umgang mit Personaldaten im Rahmen von Evaluationen siehe die Abschnitte 3.1.3 und 3.2.4.

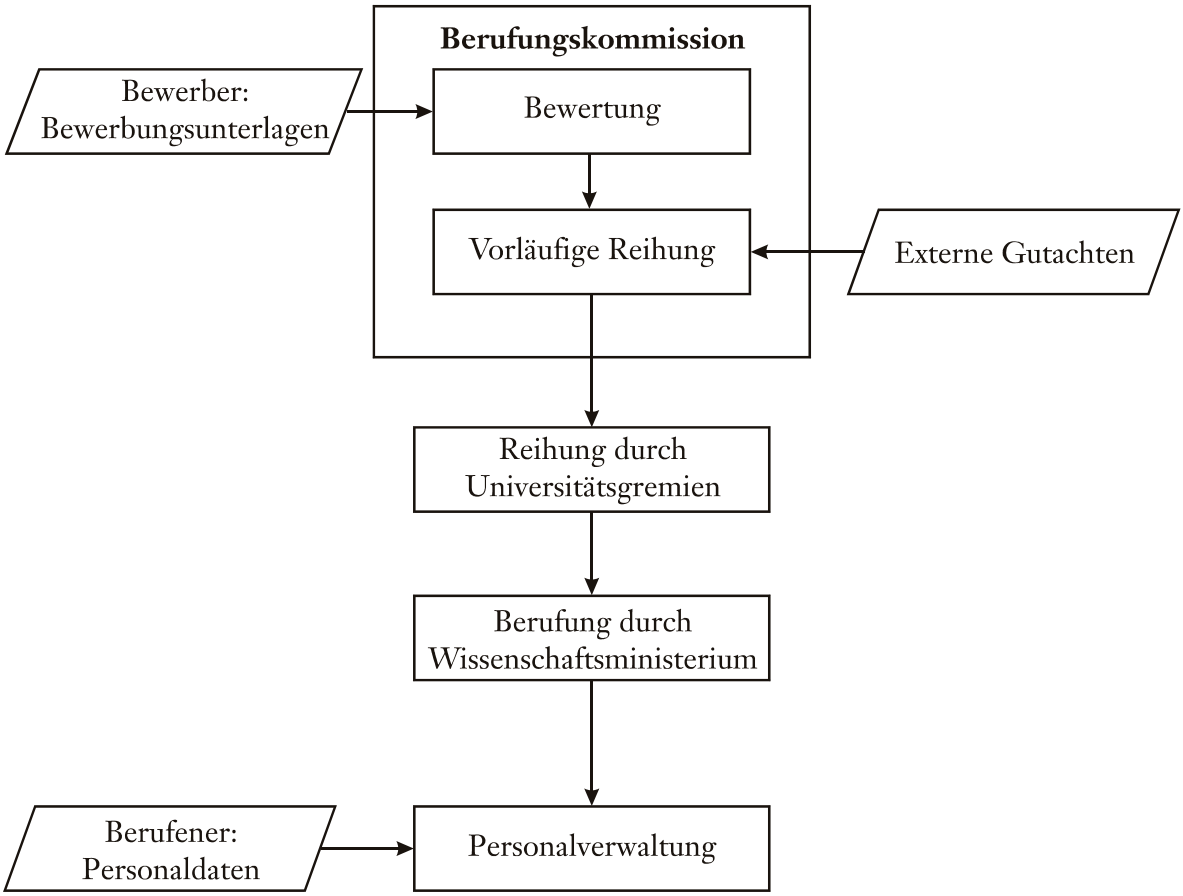
---

[164] siehe auch [Rechnungshof1994], S. 113.
[165] siehe auch [LfD2000], S. 21 zu § 36 LDSG.
[166] diese Einschränkung wurde in Fußnote 3 zu § 2 (1) IuK-R-DV in Anlehnung an Bestimmungen aus dem Landespersonalvertretungsgesetz beim Geltungsbereich der Dienstvereinbarung getroffen.

3.4.2 Datenschutzgerechter Umgang mit Personaldaten von Professoren

Ein Berufungsverfahren und der Umgang der Personaldaten hierbei sieht im Wesentlichen so aus:

Abb. 12 Ablauf eines Berufungsverfahrens



Als kritische Bereiche im Sinne des Datenschutzes lassen sich demnach festhalten:

- Eingang der Bewerbungsunterlagen und deren Bewertung durch die Berufungskommission,
- Beschlussfassung über die endgültige Reihung (unter Berücksichtigung externer und vergleichender Gutachten) und Berufung durch das Wissenschaftsministerium sowie
- Führung der Personalakten (z.B. unter Nutzung von HIS-SVA) ab Berufung.

Personalangelegenheiten sind nach § 112 UG stets vertraulich und nicht öffentlich. Sie unterliegen daher einem besonderen Schutz. Kommt eine Berufung nicht zustande, so sind die Bewerbungsunterlagen dem Betroffenen nach § 36 Abs. 3 LDSG unverzüglich zurückzusenden und gespeicherte Daten spätestens innerhalb eines Jahres zu löschen, sofern der Betroffene nicht einer weiteren Verarbeitung zugestimmt hatte oder ein anhängiger Rechtsstreit noch nicht abgeschlossen ist.

Kommt hingegen das neue Dienstverhältnis zustande, so dürfen nach § 113 LBG nur Unterlagen in die Personalakten, die im unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis stehen. Die Personalakten dürfen nur im Rahmen der Personalverwaltung verwendet werden, sofern der Betroffene nicht einer anderweitigen Verwendung zugestimmt hat. Fünf Jahre nach Abschluss des Dienstverhältnisses werden die Personalakten i.d.R. gelöscht, sofern sie nicht vom zuständigen Archiv übernommen wurden (§ 113f LBG).

3.4.3 Datenschutzgerechter Umgang mit anderen Personaldaten

Personenbezogene Daten sind grundsätzlich unmittelbar beim betroffenen Beschäftigten zu erheben (§ 7 Abs. 5 IuK-R-DV). Nach § 6 IuK-R-DV sind die Beschäftigten anlässlich einer erstmaligen Speicherung personenbezogener Daten umfassend darüber zu informieren, welche Daten gespeichert wurden (Datenspiegel).

Die personenbezogenen Daten der Beschäftigten sind an die Sozialträger gem. § 3 DEÜV zu übermitteln; hat die Universität die Lohn- und Gehaltsabrechnung nicht nur im Rahmen der Beamtenbezüge an das Landesamt für Besoldung und Versorgung Baden-Württemberg übertragen, meldet diese ersatzweise die erforderlichen Daten[167]. Gemäß § 25 DEÜV ist der Beschäftigte mindestens einmal pro Jahr über die versandten Daten zu unterrichten.

Kommt ein Arbeits- bzw. Dienstverhältnis nicht zustande, so sind die Bewerbungsdaten dem Betroffenen nach § 36 Abs. 3 LDSG unverzüglich zurückzusenden und gespeicherte Daten spätestens innerhalb eines Jahres zu löschen, sofern der Betroffene nicht einer weiteren Vereinbarung zugestimmt hatte oder ein anhängiger Rechtsstreit noch nicht abgeschlossen ist.

3.4.4 Datenschutzgerechter Umgang mit personenbezogenen Daten in der universitären Mittelbewirtschaftung

Im Rahmen der Reisekostenabrechnungen wie auch der Drittmittelverwaltung wird insoweit auf personenbezogene Daten zugegriffen, da diese (etwa im Rahmen von HISMBS und HISCOB) der verursachenden bzw. einwerbenden Stelle zugeordnet werden müssen[168]. In zunehmendem Maße wird auch an den Universitäten eine leistungs- und belastungsorientierte Mittelbewirtschaftung eingeführt. Diese greift teilweise ebenfalls bis auf die Ebene einzelner Professoren durch. Im Rahmen der Mittelkontrolle wie auch etwaiger Berichtspflichten gegenüber dem Wissenschaftsministerium (nach § 8 Abs. 4 UG) ist sicherzustellen,

---

[167] siehe auch [Rechnungshof1994], S. 115.

[168] die Überprüfung etwa der Berechtigung von Studierenden zur Teilnahme an einer Exkursion ist nach [Rechnungshof1994], S. 151 nicht nötig, wenn der Exkursionsleiter die Richtigkeit der Angaben bestätigt, so dass auch keine weitere Verarbeitung dieser Daten erforderlich ist.

dass keine personenbezogenen Daten in diesem Zusammenhang übermittelt werden, da hierfür keine Rechtsgrundlage existiert. Wenn die Mittelbewirtschaftung direkt auf die entsprechende Datenbank der Personalverwaltung (i.d.R. HISSVA) zugreift, sind hier keine speziellen Löschungsfristen erforderlich. Allerdings sind die personenbezogenen Daten gemäß § 24 LDSG unverzüglich nach Abschluss der Abrechungsperiode zu sperren, da die Mittelbewirtschaftung der Kontrolle durch den Rechnungshof unterliegt (siehe auch Abschnitt 3.4.5).

3.4.5 Datenschutzgerechter Umgang mit externen Untersuchungen

Eine Universität unterliegt neben der Rechts- bzw. Fachaufsicht des Wissenschaftsministeriums auch der Kontrolle durch den Rechnungshof. Dieser kann im Rahmen seiner Untersuchungen auch personenbezogene Daten einsehen[169]. Nach Abschluss der Kontrolle sind aber die entsprechenden personenbezogenen Daten unverzüglich nach § 23 LDSG zu löschen.

Dritte treten immer wieder an eine Universität heran, um eigene Untersuchungen durchführen zu können, für die sie auf personenbezogene Daten zugreifen müssen. Hier hat die Universität zu beachten, dass sie diese Daten nur herausgeben darf, wenn sie von den Betroffenen (oder einer Rechtsvorschrift) hierzu ermächtigt wurde bzw. die anderen Voraussetzungen aus Abschnitt 3.1.1 zutreffen. Ansonsten hat sie entweder ein Adressmittlungsverfahren anzuwenden oder als Datentreuhänder zu fungieren (siehe ebenfalls Abschnitt 3.1.1). Gleiches gilt auch für den Fall, dass z.B. im Auftrag einer universitären Einrichtung Umfragen unter ehemaligen Mitgliedern der Universität (wie beispielsweise Absolventen) durchgeführt werden sollen.

Oftmals wird sich aber der Auftraggeber einer Studie von vorneherein mit einer anonymisierten Auswertung seiner Anfragen zufrieden geben. Könnte die Universität diese Anonymisierung nur mit einem unverhältnismäßigen Aufwand (gem. § 15 Abs. 5 LDSG) erreichen, kann dieses auch durch andere Stellen im Sinne der Datenverarbeitung im Auftrag (gem. § 7 Abs. 5 LDSG) erfolgen. Dabei ist sicherzustellen, dass unverzüglich nach erfolgter Anonymisierung der Personenbezug gelöscht wird.

3.4.6 Datenschutzgerechter Umgang bei Gremienwahlen

Im Rahmen universitärer Gremienwahlen gibt es drei kritische Bereiche im Sinne des Datenschutzes:

- bei der Abgabe und Überprüfung der Wahlvorschläge,
- bei der Bekanntmachung der Wahlvorschläge und

[169] siehe auch den Beschluss des Bundesverfassungsgerichts vom 29.04.1996 (1 BvR 1226/89) zu Patientenakten und Rechnungshofkontrolle, abgedruckt in: Neue Juristische Wochenschrift 24/1997, S. 1633 – 1634.

- bei der eigentlichen Stimmabgabe.

Auf der Grundlage von § 107 Abs. 9 UG wurde eine Verordnung des Kultusministeriums zur Durchführung der Wahlen an den Universitäten (Stand: 14.12.1977) erlassen, das insbesondere Regelungen über den Umgang mit personenbezogenen Daten enthält und insoweit dem LDSG vorgeht. Nach § 10 Abs. 5 dieser Verordnung ist bei studentischen Wahlvorschlägen u.a. die Matrikel-Nummern von Kandidierenden und nach § 10 Abs. 3 auch von Unterstützenden anzugeben. In der Bekanntmachung der Wahlvorschläge (§ 12) sowie auf den jeweiligen Stimmzetteln (§ 17 Abs. 2) werden die Angaben aus § 10 Abs. 5 veröffentlicht. Die jeweilige Matrikel-Nummer ist aber bei der Bekanntmachung und dem Stimmzettel entbehrlich und ein schützenswertes personenbezogenes Datum zugleich (siehe auch Abschnitt 3.2.3). Die Veröffentlichung dieses Datums stellt deshalb m.E. einen unverhältnismäßigen Eingriff in das informationelle Selbstbestimmungsrecht dar. Bei einer Überarbeitung der Verordnung sollte daher dieser Umstand beseitigt werden. Bis dahin sollte auf eine Veröffentlichung von Matrikel-Nummern bei Gremienwahlen abgesehen werden (wie dies bereits von einigen Universitäten gehandhabt wird).

Immer häufiger wird darüber diskutiert, ob nicht Wahlen online durchgeführt werden sollten. Dies stellt insbesondere hohe Anforderungen an die Systemsicherheit, da sichergestellt sein muss, dass die Wahlen entsprechend den Wahlgrundsätzen aus § 107 Abs. 1 UG, also frei, gleich und geheim, durchgeführt werden können. Vor allem eine gleiche und geheime Wahl stellt große Herausforderungen dar[170] wie auch die Gewährleistung der Transparenz bisheriger Wahlen.

Erst wenn diese Anforderungen (siehe hierzu auch Abschnitt 1.5.3) erfüllt sind, kann ein solches Wahlverfahren durchgeführt werden. Entsprechend der Vorschrift aus § 35 der zugrunde liegenden Verordnung sind auch in diesem Fall die personenbezogenen Daten nach Ablauf der Amtsperiode des gewählten Gremiums zu löschen.

[170] mögliche Lösungsansätze skizziert [Ullmann2001], S. 645f.

4. Der Datenschutz in ausgewählten Fallbeispielen

In diesem Hauptteil werden durch aussagekräftige Beispiele aus dem universitären Alltag die wichtigsten Datenschutzbestimmungen aufgezeigt. Dabei wird die Datenverarbeitung aufgrund unterschiedlicher Bedeutung beim Eingriff in das informationelle Selbstbestimmungsrecht (entsprechend der Schlussbemerkungen in Abschnitt 1.5.1) aufgeteilt in drei Datenverarbeitungsphasen:

- dem Erheben personenbezogener Daten,
- dem Speichern, Verändern, Nutzen, Übermitteln, Löschen und Sperren personenbezogener Daten, im weiteren „Bearbeiten personenbezogener Daten“ genannt, und
- dem Veröffentlichen personenbezogener Daten.

Da die Angaben dazu dienen sollen, Richtlinien für einen datenschutzgerechten Umgang zu liefern, wurde eine weitgehend schematische Form gewählt.

Zur konkreten Veranschaulichung wurden einzelne Fallbeispiele auf die Fakultät für Informatik an der Universität Ulm bezogen. Da die Rechtsgrundlagen aber nicht wesentlich von anderen Fakultäten, Studiengängen oder Landesuniversitäten abweichen, ist eine Übertragung ohne weiteres möglich.

4.1 Beispiele aus der Forschung

4.1.1 Durchführung von Studien mit personenbezogenen Daten

Situationsbeschreibung:

Eine Abteilung will eine Studie im Rahmen eines Forschungsvorhabens anfertigen, zu der personenbezogene Daten verarbeitet werden sollen.

Verantwortliche Stelle ist die Abteilung.

Uneingeschränkt geltende Grundsätze zum datenschutzgerechten Umgang:

1. Grundsätze der Datenverarbeitung:
   - Der Zweck, zu dem personenbezogene Daten verarbeitet werden sollen, ist konkret festzulegen.
   - Die erhobenen Daten müssen für den Zweck geeignet und erforderlich sein.
   - Bei der Datenverarbeitung ist darauf zu achten, dass möglichst wenig personenbezogene Daten verarbeitet werden.

2. Einfluss der Einwilligung:
- Ohne Einwilligung des Betroffenen dürfen personenbezogene Daten nur auf der Grundlage einer ausdrücklichen Rechtsvorschrift (Gesetz, Verordnung) verarbeitet werden.
- Mit Einwilligung des Betroffenen (siehe hierzu auch das entsprechende Formblatt in der Anlage) dürfen personenbezogene Daten nur im Rahmen der getroffenen Vereinbarungen (und natürlich unter Einhaltung gesetzlicher Vorschriften) verwendet werden.
- Eine Einwilligung von Betroffenen erfordert, dass der Betroffene über die beabsichtigte Datenverarbeitung (incl. der Benennung der verantwortlichen Stelle, Art und Weise der Datenverarbeitung, dem Kreis der Zugangsberechtigten und dem Zeitpunkt der Löschung), deren Zweck und etwaige Empfänger der Daten aufgeklärt wird. Außerdem ist er über seine Rechte auf Auskunft über gespeicherte Daten, auf Berichtigung, Löschung bzw. Sperrung unrichtiger oder unzulässiger bzw. nicht mehr erforderlicher Daten und auf sein Recht zur Anrufung des zuständigen Datenschutzbeauftragten hinzuweisen. Die Einwilligung muss schriftlich erklärt werden, um wirksam werden zu können.

Fallspezifische Grundsätze zum datenschutzgerechten Umgang:

- Wenn für die Studie personenbezogene Daten an sich nicht wichtig sind, so sollten diese entweder anonymisiert erhoben oder so früh wie möglich anonymisiert werden. Ein erster Zwischenschritt hierzu ist die Pseudonymisierung (siehe auch unter technische Hinweise). Je eher die Daten (faktisch) anonymisiert sind, desto weniger Restriktionen unterliegt die Datenverarbeitung.
- Öffentlich zugängliche Daten dürfen jederzeit verarbeitet werden.
- Wurden Daten bereits in einem anderen Zusammenhang ausdrücklich zu wissenschaftlichen Zwecken erhoben, können diese auch für andere wissenschaftliche Zwecke (aber nicht für wissenschaftsfremde Zwecke wie z.B. zur Werbung oder Strafverfolgung) verarbeitet werden.
- Die Notwendigkeit zur Einwilligung der Betroffenen entfällt, wenn das konkrete Forschungsziel diesem widerspricht, weil z.B. das Nutzungsverhalten von Software-Anwendern untersucht werden soll.

- Sollen die im Rahmen der Studie verarbeiteten personenbezogenen Daten auch für weitergehende Fragestellungen zur Verfügung stehen, muss darauf explizit hingewiesen werden.
- Es kann vorkommen, dass bereichspezifisches Datenschutzrecht anzuwenden ist, das im zugrunde liegenden Fall vorrangig ist. Dieser Fall wird hier nicht behandelt.

Erheben

Im Rahmen eines wissenschaftlichen Forschungsprojekts ist es möglich, von anderen Stellen die gewünschten Daten erhalten zu können und sie somit nicht selbst erheben zu müssen. Die Übermittlung ist aber nur zulässig, wenn dies erforderlich ist, das Interesse des Betroffenen deutlich übertroffen wird und der Forschungszweck auf andere Weise gar nicht oder nur mit erheblichem Aufwand realisiert werden könnte.

Personenbezogene Daten können auch über Dritte erhoben werden. Hierbei bietet sich an: ein Adressmittlungsverfahren (Befragungsunterlagen werden über Dritte an die Betroffenen gesandt, die Adressen bleiben der Abteilung unbekannt) oder ein Datentreuhänder-Modell (Auswertung erfolgt über einen unabhängigen Dritten, der einer besonderen Schweigepflicht unterliegt, wie z.B. ein Notar).

Grundlagen: §§ 19 und 35 LDSG i.V.m. §§ 13 und 14 LDSG

Bearbeiten

Ein Übermitteln der Daten für ein anderes Forschungsprojekt ist zulässig, wenn die Daten ausdrücklich zu wissenschaftlichen Zwecken erhoben wurden.

Personenbezogene Daten sind entsprechend der mit Betroffenen vereinbarten Frist bzw. auf der Grundlage einer DFG-Empfehlung nach 10 Jahren zu löschen. Wurden diese jedoch veröffentlicht, entfällt eine Löschungsfrist.

Grundlagen: §§ 19 und 35 LDSG i.V.m. §§ 15 bis 18 LDSG und §§ 20 bis 25 LDSG

Veröffentlichen

Personenbezogene Daten dürfen nur veröffentlicht werden, wenn dies vom Betroffenen genehmigt wurde oder der Betroffene eine Person der Zeitgeschichte ist, deren Interesse geringer als das der Öffentlichkeit ist.

Grundlagen: §§ 19 und 35 LDSG i.V.m. § 15 LDSG

Technische Hinweise:

- Bei einer Pseudonymisierung sind die identifizierenden Daten durch Zuordnungstabellen und Verschlüsselungsverfahren zu verändern und getrennt zu speichern. Dabei kann vorgesehen werden, dass der Betroffene selbst ein Pseudonym vergibt. Als automatisierte Verschlüsselungsverfahren bieten sich Hash-Funktionen nach ISO/IEC 10118 an.
- Verwendete Datenverarbeitungssysteme sind im Verfahrensverzeichnis zu dokumentieren, das vom zuständigen Datenschutzbeauftragten geführt wird (hier: der Landesdatenschutzbeauftragte). Hierbei ist darzulegen, welche personenbezogenen Daten (Art der Einzelmerkmale, Kreis der Betroffenen) in welchem Verfahren mit Hilfe welcher automatisierter Verfahren (welche Hard- und Software incl. der Vernetzung verwendet wird) auf welche Weise (und aufgrund welcher Rechtsgrundlage sowie zu welchem Zweck) verarbeitet werden und welche Datenschutzmaßnahmen (insbesondere zur Datensicherung) die verantwortliche Stelle dabei getroffen hat. Es ist außerdem aufzuführen, wer als Empfänger der Daten vorgesehen ist, welche Fristen für Löschung bzw. Sperrung vorgesehen sind und wer zugriffsberechtigt ist (siehe auch Datenschutzerklärungsmuster in der Anlage).

4.1.2 Durchführung von externen Studien mit personenbezogenen Daten

Situationsbeschreibung:

Eine Abteilung will im Auftrag Dritter eine Studie anfertigen, zu der personenbezogene Daten erhoben werden sollen.

Verantwortliche Stelle ist der Dritte, der die Abteilung (als übermittelnde Stelle) zur Einhaltung der Datenschutzbestimmungen zu verpflichten hat. Da die für den Dritten geltenden Datenschutzbestimmungen i.d.R. keinen gravierenden Unterschied in diesem Fall darstellen, wird nur der Fall betrachtet, dass der Auftraggeber („Dritte“) ein Unternehmen ist (ansonsten siehe im Wesentlichen Abschnitt 4.1.1).

Uneingeschränkt geltende Grundsätze zum datenschutzgerechten Umgang:

1. Grundsätze der Datenverarbeitung:
- Der Zweck, zu dem personenbezogene Daten verarbeitet werden sollen, ist konkret festzulegen.
- Die erhobenen Daten müssen für den Zweck geeignet und erforderlich sein.

- Bei der Datenverarbeitung ist darauf zu achten, dass möglichst wenig personenbezogene Daten verarbeitet werden.

2. Einfluss der Einwilligung:
- Ohne Einwilligung des Betroffenen dürfen personenbezogene Daten nur auf der Grundlage einer ausdrücklichen Rechtsvorschrift (Gesetz, Verordnung) verarbeitet werden.
- Mit Einwilligung des Betroffenen (siehe hierzu auch das entsprechende Formblatt in der Anlage) dürfen personenbezogene Daten nur im Rahmen der getroffenen Vereinbarungen (und natürlich unter Einhaltung gesetzlicher Vorschriften) verwendet werden.
- Eine Einwilligung von Betroffenen erfordert, dass der Betroffene über die beabsichtigte Datenverarbeitung (incl. der Benennung der verantwortlichen Stelle, Art und Weise der Datenverarbeitung, dem Kreis der Zugangsberechtigten und dem Zeitpunkt der Löschung), deren Zweck und etwaige Empfänger der Daten aufgeklärt wird. Außerdem ist er über seine Rechte auf Auskunft über gespeicherte Daten, auf Berichtigung, Löschung bzw. Sperrung unrichtiger oder unzulässiger bzw. nicht mehr erforderlicher Daten und auf sein Recht zur Anrufung des zuständigen Datenschutzbeauftragten hinzuweisen. Die Einwilligung muss schriftlich erklärt werden, um wirksam werden zu können.

Fallspezifische Grundsätze zum datenschutzgerechten Umgang:

- Wenn für die Studie personenbezogene Daten an sich nicht wichtig sind, so sollten diese entweder anonymisiert erhoben oder so früh wie möglich anonymisiert werden. Ein erster Zwischenschritt hierzu ist die Pseudonymisierung (siehe auch unter technische Hinweise). Je eher die Daten (faktisch) anonymisiert sind, desto weniger Restriktionen unterliegt die Datenverarbeitung.
- Öffentlich zugängliche Daten dürfen jederzeit verarbeitet werden.
- Wurden Daten bereits in einem anderen Zusammenhang ausdrücklich zu wissenschaftlichen Zwecken erhoben, können diese auch für andere wissenschaftliche Zwecke (aber nicht für wissenschaftsfremde Zwecke wie z.B. zur Werbung oder Strafverfolgung) verarbeitet werden.
- Die Notwendigkeit zur Einwilligung der Betroffenen entfällt, wenn das konkrete Forschungsziel diesem widerspricht, weil z.B. das Nutzungsverhalten von Software-Anwendern untersucht werden soll.

- Sollen die im Rahmen der Studie verarbeiteten personenbezogenen Daten auch für weitergehende Fragestellungen zur Verfügung stehen, muss darauf explizit hingewiesen werden.
- Es kann vorkommen, dass bereichspezifisches Datenschutzrecht anzuwenden ist, das im zugrunde liegenden Fall vorrangig ist. Dieser Fall wird hier nicht behandelt.
- Bei Studien, die im Auftrag Dritter durchgeführt werden, ist das Datenschutzrecht maßgeblich, dass für den Dritten gilt. Ist der Dritte eine öffentliche Einrichtung des Landes, gilt das jeweilige Landesdatenschutzgesetz (LDSG). Ist der Dritte eine öffentliche Einrichtung des Bundes oder ein privater Auftraggeber, gilt das Bundesdatenschutzgesetz (BDSG). Ist der Dritte außerhalb der Bundesrepublik beheimatet, gilt die EG-Datenschutzrichtlinie.

Erheben

Im Rahmen eines wissenschaftlichen Forschungsprojekts ist es möglich, von anderen Stellen die gewünschten Daten erhalten zu können und sie somit nicht selbst erheben zu müssen. Die Übermittlung ist aber nur zulässig, wenn dies erforderlich ist, das Interesse des Betroffenen deutlich übertroffen wird und der Forschungszweck auf andere Weise gar nicht oder nur mit erheblichem Aufwand realisiert werden könnte.

Personenbezogene Daten können auch über Dritte erhoben werden. Hierbei bietet sich an: ein Adressmittlungsverfahren (Befragungsunterlagen werden über Dritte an die Betroffenen gesandt, die Adressen bleiben der Abteilung unbekannt) oder ein Datentreuhänder-Modell (Auswertung erfolgt über einen unabhängigen Dritten, der einer besonderen Schweigepflicht unterliegt, wie z.B. ein Notar).

Grundlagen: §§ 11, 28 und 40 BDSG sowie §§ 19 und 35 LDSG i.V.m. §§ 13 und 14 LDSG

Bearbeiten

Ein Übermitteln der Daten für ein anderes Forschungsprojekt ist zulässig, wenn die Daten ausdrücklich zu wissenschaftlichen Zwecken erhoben wurden.

Personenbezogene Daten sind entsprechend der mit Betroffenen vereinbarten Frist bzw. auf der Grundlage einer DFG-Empfehlung nach 10 Jahren zu löschen. Wurden diese jedoch veröffentlicht, entfällt eine Löschungsfrist.

Grundlagen: §§ 11, 28 und 40 BDSG i.V.m. §§ 33 bis 35 BDSG sowie §§ 19 und 35 LDSG i.V.m. §§ 15 bis 18 LDSG und §§ 20 bis 25 LDSG

Veröffentlichen

Personenbezogene Daten dürfen nur veröffentlicht werden, wenn dies vom Betroffenen genehmigt wurde oder der Betroffene eine Person der Zeitgeschichte ist, deren Interesse geringer als das der Öffentlichkeit ist.

Grundlagen: §§ 11, 28 und 40 BDSG sowie §§ 19 und 35 LDSG i.V.m. § 15 LDSG

Technische Hinweise:

- Bei einer Pseudonymisierung sind die identifizierenden Daten durch Zuordnungstabellen und Verschlüsselungsverfahren zu verändern und getrennt zu speichern. Dabei kann vorgesehen werden, dass der Betroffene selbst ein Pseudonym vergibt. Als automatisierte Verschlüsselungsverfahren bieten sich Hash-Funktionen nach ISO/IEC 10118 an.
- Verwendete Datenverarbeitungssysteme sind im Verfahrensverzeichnis zu dokumentieren, das vom zuständigen Datenschutzbeauftragten geführt wird (hier: der Landesdatenschutzbeauftragte). Hierbei ist darzulegen, welche personenbezogenen Daten (Art der Einzelmerkmale, Kreis der Betroffenen) in welchem Verfahren mit Hilfe welcher automatisierter Verfahren (welche Hard- und Software incl. der Vernetzung verwendet wird) auf welche Weise (und aufgrund welcher Rechtsgrundlage sowie zu welchem Zweck) verarbeitet werden und welche Datenschutzmaßnahmen (insbesondere zur Datensicherung) die verantwortliche Stelle dabei getroffen hat. Es ist außerdem aufzuführen, wer als Empfänger der Daten vorgesehen ist, welche Fristen für Löschung bzw. Sperrung vorgesehen sind und wer zugriffsberechtigt ist (siehe auch Datenschutzerklärungsmuster in der Anlage).

4.1.3 Durchführung einer internen Evaluation der Forschung

Situationsbeschreibung:

Eine Fakultät bzw. ein Fachbereich soll innerhalb der Universität bewertet werden und fertigt hierzu einen Selbstreport an.

Verantwortliche Stelle ist die Fakultät bzw. der Fachbereich.

Uneingeschränkt geltende Grundsätze zum datenschutzgerechten Umgang:

1. Grundsätze der Datenverarbeitung:
- Der Zweck, zu dem personenbezogene Daten verarbeitet werden sollen, ist konkret festzulegen.
- Die erhobenen Daten müssen für den Zweck geeignet und erforderlich sein.
- Bei der Datenverarbeitung ist darauf zu achten, dass möglichst wenig personenbezogene Daten verarbeitet werden.

2. Einfluss der Einwilligung:
- Ohne Einwilligung des Betroffenen dürfen personenbezogene Daten nur auf der Grundlage einer ausdrücklichen Rechtsvorschrift (Gesetz, Verordnung) verarbeitet werden.
- Mit Einwilligung des Betroffenen (siehe hierzu auch das entsprechende Formblatt in der Anlage) dürfen personenbezogene Daten nur im Rahmen der getroffenen Vereinbarungen (und natürlich unter Einhaltung gesetzlicher Vorschriften) verwendet werden.
- Eine Einwilligung von Betroffenen erfordert, dass der Betroffene über die beabsichtigte Datenverarbeitung (incl. der Benennung der verantwortlichen Stelle, Art und Weise der Datenverarbeitung, dem Kreis der Zugangsberechtigten und dem Zeitpunkt der Löschung), deren Zweck und etwaige Empfänger der Daten aufgeklärt wird. Außerdem ist er über seine Rechte auf Auskunft über gespeicherte Daten, auf Berichtigung, Löschung bzw. Sperrung unrichtiger oder unzulässiger bzw. nicht mehr erforderlicher Daten und auf sein Recht zur Anrufung des zuständigen Datenschutzbeauftragten hinzuweisen. Die Einwilligung muss schriftlich erklärt werden, um wirksam werden zu können.

Fallspezifische Grundsätze zum datenschutzgerechten Umgang:

- Wenn für die Evaluation personenbezogene Daten an sich nicht wichtig sind, so sollten diese entweder anonymisiert erhoben oder so früh wie möglich anonymisiert werden. Ein erster Zwischenschritt hierzu ist die Pseudonymisierung (siehe auch unter technische Hinweise). Je eher die Daten (faktisch) anonymisiert sind, desto weniger Restriktionen unterliegt die Datenverarbeitung.
- Öffentlich zugängliche Daten dürfen jederzeit verarbeitet werden.
- Sollen die im Rahmen der Evaluation verarbeiteten personenbezogenen Daten auch für weitergehende Fragestellun-

gen zur Verfügung stehen, muss darauf explizit hingewiesen werden.
- Eine Evaluation verfolgt in erster Linie das Ziel der Qualitätsverbesserung. Je eher etwaige Konsequenzen innerhalb der Universität gezogen werden, desto unproblematischer ist dies. Eine Evaluation setzt jedoch ein wissenschaftsäquivalentes Verfahren (gleichrangige Gutachter, wissenschaftliche Redlichkeit etc.) voraus und räumt Betroffenen grundsätzlich das Recht zur Gegendarstellung ein.

Erheben

Universitäre Mitglieder und deren Angehörige sind zur Mitwirkung und Angabe notwendiger personenbezogener Daten verpflichtet.

Welche personenbezogenen Daten erhoben werden sollen, ist in einer universitären Satzung festzuschreiben.

Grundlagen: § 4a UG i.V.m. §§ 13 und 14 LDSG

Bearbeiten

Welche personenbezogenen Daten in welcher Form verarbeitet und bewertet werden sollen, ist in einer universitären Satzung festzuschreiben.

Grundlagen: § 4a UG i.V.m. §§ 15 bis 25 LDSG

Veröffentlichen

Welche personenbezogenen Daten veröffentlicht werden sollen, ist in einer universitären Satzung festzuschreiben.

Von Professoren, Hochschul- und Privatdozenten, Mitarbeitern des wissenschaftlichen Dienstes, Lehrbeauftragten, Lehrkräften für besondere Aufgaben sowie sonstigen Mitarbeitern, die herausgehobene Funktionen in der Universität wahrnehmen, dürfen Name, Amts-, Dienst- und Funktionsbezeichnung, Telefon- und Telefaxnummern sowie E-Mail- und Internet-Adressen veröffentlicht werden, sofern die Betroffenen kein höher zu bewertendes schutzwürdiges Interesse geltend machen können.

Die Veröffentlichung von Evaluationsergebnissen ist unbedenklich, wenn die gesamte untersuchte Einheit betroffen ist und nicht nur ein Forscher alleine.

Es darf dargestellt werden, was geforscht wurde. Eine Bewertung der Forschungsleistungen Einzelner ist hingegen nur bei deren ausdrücklicher Einwilligung oder in eingeschränkter Form bei nachweisbaren Verstößen gegen die wissenschaftliche Redlichkeit des Betroffenen erlaubt.

Grundlagen: §§ 4a und 125a Abs. 5 UG i.V.m. § 15 LDSG

Technische Hinweise:

- Bei einer Pseudonymisierung sind die identifizierenden Daten durch Zuordnungstabellen und Verschlüsselungsverfahren zu verändern und getrennt zu speichern. Dabei kann vorgesehen werden, dass der Betroffene selbst ein Pseudonym vergibt. Als automatisierte Verschlüsselungsverfahren bieten sich Hash-Funktionen nach ISO/IEC 10118 an.
- Verwendete Datenverarbeitungssysteme sind im Verfahrensverzeichnis zu dokumentieren, das vom zuständigen Datenschutzbeauftragten geführt wird (hier: der Landesdatenschutzbeauftragte). Hierbei ist darzulegen, welche personenbezogenen Daten (Art der Einzelmerkmale, Kreis der Betroffenen) in welchem Verfahren mit Hilfe welcher automatisierter Verfahren (welche Hard- und Software incl. der Vernetzung verwendet wird) auf welche Weise (und aufgrund welcher Rechtsgrundlage sowie zu welchem Zweck) verarbeitet werden und welche Datenschutzmaßnahmen (insbesondere zur Datensicherung) die verantwortliche Stelle dabei getroffen hat. Es ist außerdem aufzuführen, wer als Empfänger der Daten vorgesehen ist, welche Fristen für Löschung bzw. Sperrung vorgesehen sind und wer zugriffsberechtigt ist (siehe auch Datenschutzerklärungsmuster in der Anlage).

4.1.4 Durchführung einer externen Evaluation der Forschung

Situationsbeschreibung:

Eine Fakultät bzw. ein Fachbereich soll durch Dritte, z.B. der Evaluationsagentur Baden-Württemberg, bewertet werden.

Verantwortliche Stelle ist die Evaluationsagentur, die die Fakultät bzw. den Fachbereich (als übermittelnde Stelle) zur Einhaltung der Datenschutzbestimmungen zu verpflichten hat.

Uneingeschränkt geltende Grundsätze zum datenschutzgerechten Umgang:

1. Grundsätze der Datenverarbeitung:
- Der Zweck, zu dem personenbezogene Daten verarbeitet werden sollen, ist konkret festzulegen.
- Die erhobenen Daten müssen für den Zweck geeignet und erforderlich sein.
- Bei der Datenverarbeitung ist darauf zu achten, dass möglichst wenig personenbezogene Daten verarbeitet werden.

2. Einfluss der Einwilligung:
- Ohne Einwilligung des Betroffenen dürfen personenbezogene Daten nur auf der Grundlage einer ausdrücklichen Rechtsvorschrift (Gesetz, Verordnung) verarbeitet werden.
- Mit Einwilligung des Betroffenen (siehe hierzu auch das entsprechende Formblatt in der Anlage) dürfen personenbezogene Daten nur im Rahmen der getroffenen Vereinbarungen (und natürlich unter Einhaltung gesetzlicher Vorschriften) verwendet werden.
- Eine Einwilligung von Betroffenen erfordert, dass der Betroffene über die beabsichtigte Datenverarbeitung (incl. der Benennung der verantwortlichen Stelle, Art und Weise der Datenverarbeitung, dem Kreis der Zugangsberechtigten und dem Zeitpunkt der Löschung), deren Zweck und etwaige Empfänger der Daten aufgeklärt wird. Außerdem ist er über seine Rechte auf Auskunft über gespeicherte Daten, auf Berichtigung, Löschung bzw. Sperrung unrichtiger oder unzulässiger bzw. nicht mehr erforderlicher Daten und auf sein Recht zur Anrufung des zuständigen Datenschutzbeauftragten hinzuweisen. Die Einwilligung muss schriftlich erklärt werden, um wirksam werden zu können.

Fallspezifische Grundsätze zum datenschutzgerechten Umgang:

- Wenn für die Evaluation personenbezogene Daten an sich nicht wichtig sind, so sollten diese entweder anonymisiert erhoben oder so früh wie möglich anonymisiert werden. Ein erster Zwischenschritt hierzu ist die Pseudonymisierung (siehe auch unter technische Hinweise). Je eher die Daten (faktisch) anonymisiert sind, desto weniger Restriktionen unterliegt die Datenverarbeitung.
- Öffentlich zugängliche Daten dürfen jederzeit verarbeitet werden.
- Sollen die im Rahmen der Evaluation verarbeiteten personenbezogenen Daten auch für weitergehende Fragestellungen zur Verfügung stehen, muss darauf explizit hingewiesen werden.
- Eine Evaluation verfolgt in erster Linie das Ziel der Qualitätsverbesserung. Je eher etwaige Konsequenzen innerhalb der Universität gezogen werden, desto unproblematischer ist dies. Eine Evaluation setzt jedoch ein wissenschaftsäquivalentes Verfahren (gleichrangige Gutachter, wissenschaftliche Redlichkeit etc.) voraus und räumt Betroffenen grundsätzlich das Recht zur Gegendarstellung ein.

Erheben

Universitäre Mitglieder und deren Angehörige sind zur Mitwirkung und Angabe notwendiger personenbezogener Daten verpflichtet.

Welche personenbezogenen Daten erhoben werden sollen, ist in einer universitären Satzung festzuschreiben.

Die Erhebung unter den universitären Mitgliedern darf nur durch die Universität selbst erfolgen.

Ist mit der externen Evaluation die Einwerbung von Fördermitteln verbunden, stellt der Antrag auf Einwerbung eine Einwilligungserklärung der Betroffenen dar.

Grundlagen: § 4a UG i.V.m. §§ 13 und 14 LDSG

Bearbeiten

Welche personenbezogenen Daten in welcher Form verarbeitet und bewertet werden sollen, ist in einer universitären Satzung festzuschreiben.

Im Regelfall ist die externe Einrichtung nur Empfänger der von der untersuchten Einrichtung übermittelten Daten.

Die Übermittlung von Evaluationsergebnissen ist unbedenklich, wenn die gesamte untersuchte Einheit betroffen ist und nicht nur ein Forscher alleine.

Die externe Einrichtung kann übermittelte personenbezogene Daten nur im Rahmen der Einwilligungserklärungen der Betroffenen verarbeiten.

Grundlagen: § 4a UG i.V.m. §§ 15 bis 25 LDSG

Veröffentlichen

Welche personenbezogenen Daten veröffentlicht werden sollen, ist in einer universitären Satzung festzuschreiben.

Von Professoren, Hochschul- und Privatdozenten, Mitarbeitern des wissenschaftlichen Dienstes, Lehrbeauftragten, Lehrkräften für besondere Aufgaben sowie sonstigen Mitarbeitern, die herausgehobene Funktionen in der Universität wahrnehmen, dürfen Name, Amts-, Dienst- und Funktionsbezeichnung, Telefon- und Telefaxnummern sowie E-Mail- und Internet-Adressen veröffentlicht werden, sofern die Betroffenen kein höher zu bewertendes schutzwürdiges Interesse geltend machen können.

Die Veröffentlichung von Evaluationsergebnissen ist unbedenklich, wenn die gesamte untersuchte Einheit betroffen ist und nicht nur ein Forscher alleine.

Es darf dargestellt werden, was geforscht wurde. Eine Bewertung der Forschungsleistungen Einzelner ist hingegen nur bei deren ausdrücklicher Einwil-

ligung oder in eingeschränkter Form bei nachweisbaren Verstößen gegen die wissenschaftliche Redlichkeit des Betroffenen erlaubt.

Grundlagen: §§ 4a und 125a Abs. 5 UG i.V.m. § 15 LDSG

Technische Hinweise:

- Bei einer Pseudonymisierung sind die identifizierenden Daten durch Zuordnungstabellen und Verschlüsselungsverfahren zu verändern und getrennt zu speichern. Dabei kann vorgesehen werden, dass der Betroffene selbst ein Pseudonym vergibt. Als automatisierte Verschlüsselungsverfahren bieten sich Hash-Funktionen nach ISO/IEC 10118 an.
- Verwendete Datenverarbeitungssysteme sind im Verfahrensverzeichnis zu dokumentieren, das vom zuständigen Datenschutzbeauftragten geführt wird (hier: der Landesdatenschutzbeauftragte). Hierbei ist darzulegen, welche personenbezogenen Daten (Art der Einzelmerkmale, Kreis der Betroffenen) in welchem Verfahren mit Hilfe welcher automatisierter Verfahren (welche Hard- und Software incl. der Vernetzung verwendet wird) auf welche Weise (und aufgrund welcher Rechtsgrundlage sowie zu welchem Zweck) verarbeitet werden und welche Datenschutzmaßnahmen (insbesondere zur Datensicherung) die verantwortliche Stelle dabei getroffen hat. Es ist außerdem aufzuführen, wer als Empfänger der Daten vorgesehen ist, welche Fristen für Löschung bzw. Sperrung vorgesehen sind und wer zugriffsberechtigt ist (siehe auch Datenschutzerklärungsmuster in der Anlage).

4.2 Beispiele aus der Lehre

4.2.1 Zulassung und Immatrikulation/Rückmeldung von Studierenden

Situationsbeschreibung:

Studienbewerbende wollen ein universitäres Studium aufnehmen bzw. fortsetzen.

Verantwortliche Stelle ist die Zulassungsstelle (für die Zulassung) und das Studiensekretariat für die Immatrikulation bzw. Rückmeldung.

Uneingeschränkt geltende Grundsätze zum datenschutzgerechten Umgang:

1. Grundsätze der Datenverarbeitung:
- Der Zweck, zu dem personenbezogene Daten verarbeitet werden sollen, ist konkret festzulegen.
- Die erhobenen Daten müssen für den Zweck geeignet und erforderlich sein.
- Bei der Datenverarbeitung ist darauf zu achten, dass möglichst wenig personenbezogene Daten verarbeitet werden.

2. Einfluss der Einwilligung:
- Ohne Einwilligung des Betroffenen dürfen personenbezogene Daten nur auf der Grundlage einer ausdrücklichen Rechtsvorschrift (Gesetz, Verordnung) verarbeitet werden.
- Mit Einwilligung des Betroffenen (siehe hierzu auch das entsprechende Formblatt in der Anlage) dürfen personenbezogene Daten nur im Rahmen der getroffenen Vereinbarungen (und natürlich unter Einhaltung gesetzlicher Vorschriften) verwendet werden.
- Eine Einwilligung von Betroffenen erfordert, dass der Betroffene über die beabsichtigte Datenverarbeitung (incl. der Benennung der verantwortlichen Stelle, Art und Weise der Datenverarbeitung, dem Kreis der Zugangsberechtigten und dem Zeitpunkt der Löschung), deren Zweck und etwaige Empfänger der Daten aufgeklärt wird. Außerdem ist er über seine Rechte auf Auskunft über gespeicherte Daten, auf Berichtigung, Löschung bzw. Sperrung unrichtiger oder unzulässiger bzw. nicht mehr erforderlicher Daten und auf sein Recht zur Anrufung des zuständigen Datenschutzbeauftragten hinzuweisen. Die Einwilligung muss schriftlich erklärt werden, um wirksam werden zu können.

Fallspezifische Grundsätze zum datenschutzgerechten Umgang:

- Personenbezogene Daten von Studierenden, die auf der Grundlage einer Rechtsvorschrift angegeben werden müssen, können sowohl für Verwaltungszwecke als auch für andere Zwecke verarbeitet werden. 40 Jahre lang ab der Exmatrikulation bzw. Abschluss des Prüfungsverfahrens liegen in diesem Sinne vor: Name, Geschlecht, Geburtsdatum und -ort des Studierenden, dessen Studiengang und Matrikelnummer, Ergebnisse und Daten der Diplomvorprüfung sowie der Abschlussprüfung (letztere incl. Einzelnoten), etwaige Studienunterbrechungen (z.B. durch Urlaubssemester) und das Datum der Immatrikulation sowie der Exmatrikula-

tion. Allerdings sind diese Daten unverzüglich nach Abschluss des Prüfungsverfahrens zu sperren.
- Sollen die im Rahmen der Zulassung und Immatrikulation verarbeiteten personenbezogenen Daten auch für weitergehende Fragestellungen zur Verfügung stehen, muss darauf explizit hingewiesen werden.

Erheben

Über Studienbewerbende dürfen folgende personenbezogenen Daten zur Zulassung erhoben werden: Namen, Geburtsdatum, Geschlecht, Heimat- und Semesteranschrift, Staatsangehörigkeit, Angaben zur Hochschulzugangsberechtigung (i.d.R. Abi-Zeugnis), über frühere Zulassungen, bereits abgelegte Prüfungen und besondere Zulassungsvoraussetzungen (z.B. eine ggf. vorliegende Berufsausbildung für den Studiengang Medieninformatik an der Universität Ulm). Bei Ausländern kommt hier noch ein Nachweis über deutsche Sprachkenntnisse hinzu.

Über Studienbewerbende dürfen (neben der Bestätigung über den Eingang des Semesterbeitrags) zusätzlich folgende personenbezogenen Daten zur Erstimmatrikulation erhoben werden: Frühere Namen, Geburtsort, etwaige vorangegangene Studienunterbrechungen und Prüfungsergebnisse, Einberufungsbescheide zum Wehr- oder Zivildienst, Passbilder sowie der Krankenversicherungsnachweis (bei Ausländern auch eine Aufenthaltsgenehmigung).

Im Rahmen der Rückmeldung ist zusätzlich die Matrikelnummer anzugeben und ggf. im Rahmen von Beurlaubungen Nachweise zu erbringen. Diese Nachweise sind nach einem Semester zu löschen.

Im Verlauf des Studiums sind außerdem insbesondere das Aufnehmen eines Dienstverhältnisses (etwa als hilfswissenschaftliche Kraft) anzugeben.

Grundlagen: § 125a UG (sowie §§ 90 und 96 Abs. 4 UG) und §§ 1 bis 4 und 8 bzw. 12 Hochschul-Datenschutzverordnung i.V.m. §§ 13 und 14 LDSG; sowie §§ 6 und 13 Zulassungs- und Immatrikulationsordnung der Universität Ulm und § 11a HVVO

Bearbeiten

Sofern die Studienbewerbenden auch an der Universität eingeschrieben wurden, können die erhobenen Daten auch für andere Verwaltungszwecke und sonstige Zwecke verarbeiten, solange der Betroffene eingeschrieben ist.

Wurden Studienbewerbende nicht an der Universität eingeschrieben, müssen deren personenbezogene Daten (vorbehaltlich anhängiger Gerichtsverfahren) nach einem Semester gelöscht werden.

Grundlagen: § 125a UG und § 12 Hochschul-Datenschutzverordnung i.V.m. §§ 15 bis 25 LDSG

Veröffentlichen

Ein Veröffentlichen der Daten ist nur in anonymisierter Form im Zuge des Lehrberichts oder mit Einwilligung der Betroffenen erlaubt.

Grundlagen: § 125a UG und § 11 Hochschul-Datenschutzverordnung

Technische Hinweise:

- Ist eine Rückmeldung mithilfe einer Chipkarte oder über Internet bzw. Intranet vorgesehen, muss sichergestellt sein, dass die Verbindung sichergestellt ist und sich der Studierende wirklich selbst zurück gemeldet hat. Für die notwendige elektronische Signatur kommen insbesondere elliptische Kurven bzw. El Gamal-Verfahren (ISO/IEC 9796) sowie DAS (ISO/IEC 14888) in Frage.
- Verwendete Datenverarbeitungssysteme sind im Verfahrensverzeichnis zu dokumentieren, das vom zuständigen Datenschutzbeauftragten geführt wird (hier: der Landesdatenschutzbeauftragte). Hierbei ist darzulegen, welche personenbezogenen Daten (Art der Einzelmerkmale, Kreis der Betroffenen) in welchem Verfahren mit Hilfe welcher automatisierter Verfahren (welche Hard- und Software incl. der Vernetzung verwendet wird) auf welche Weise (und aufgrund welcher Rechtsgrundlage sowie zu welchem Zweck) verarbeitet werden und welche Datenschutzmaßnahmen (insbesondere zur Datensicherung) die verantwortliche Stelle dabei getroffen hat. Es ist außerdem aufzuführen, wer als Empfänger der Daten vorgesehen ist, welche Fristen für Löschung bzw. Sperrung vorgesehen sind und wer zugriffsberechtigt ist (siehe auch Datenschutzerklärungsmuster in der Anlage).

4.2.2 Prüfungsverfahren von Studierenden

Situationsbeschreibung:

Studierende wollen bzw. sollten Prüfungen ablegen.

Verantwortliche Stelle ist die zuständige Prüfungsbehörde (Prüfungsamt bzw. der entsprechende Prüfungsausschuss).

Uneingeschränkt geltende Grundsätze zum datenschutzgerechten Umgang:

1. Grundsätze der Datenverarbeitung:
- Der Zweck, zu dem personenbezogene Daten verarbeitet werden sollen, ist konkret festzulegen.
- Die erhobenen Daten müssen für den Zweck geeignet und erforderlich sein.
- Bei der Datenverarbeitung ist darauf zu achten, dass möglichst wenig personenbezogene Daten verarbeitet werden.

2. Einfluss der Einwilligung:
- Ohne Einwilligung des Betroffenen dürfen personenbezogene Daten nur auf der Grundlage einer ausdrücklichen Rechtsvorschrift (Gesetz, Verordnung) verarbeitet werden.
- Mit Einwilligung des Betroffenen (siehe hierzu auch das entsprechende Formblatt in der Anlage) dürfen personenbezogene Daten nur im Rahmen der getroffenen Vereinbarungen (und natürlich unter Einhaltung gesetzlicher Vorschriften) verwendet werden.
- Eine Einwilligung von Betroffenen erfordert, dass der Betroffene über die beabsichtigte Datenverarbeitung (incl. der Benennung der verantwortlichen Stelle, Art und Weise der Datenverarbeitung, dem Kreis der Zugangsberechtigten und dem Zeitpunkt der Löschung), deren Zweck und etwaige Empfänger der Daten aufgeklärt wird. Außerdem ist er über seine Rechte auf Auskunft über gespeicherte Daten, auf Berichtigung, Löschung bzw. Sperrung unrichtiger oder unzulässiger bzw. nicht mehr erforderlicher Daten und auf sein Recht zur Anrufung des zuständigen Datenschutzbeauftragten hinzuweisen. Die Einwilligung muss schriftlich erklärt werden, um wirksam werden zu können.

Fallspezifische Grundsätze zum datenschutzgerechten Umgang:

- Personenbezogene Daten von Studierenden, die auf der Grundlage einer Rechtsvorschrift angegeben werden müssen, können sowohl für Verwaltungszwecke als auch für andere Zwecke verarbeitet werden. 40 Jahre lang ab der Exmatrikulation bzw. Abschluss des Prüfungsverfahrens liegen in diesem Sinne vor: Name, Geschlecht, Geburtsdatum und -ort des Studierenden, dessen Studiengang und Matrikelnummer, Ergebnisse und Daten der Diplomvorprüfung sowie der Abschlussprüfung (letztere incl. Einzelnoten), etwaige Studienunterbrechungen (z.B. durch Urlaubssemester) und das Datum der Immatrikulation sowie der Exmatrikula-

tion. Allerdings sind diese Daten unverzüglich nach Abschluss des Prüfungsverfahrens zu sperren.
- Sollen die im Rahmen des Prüfungsverfahrens verarbeiteten personenbezogenen Daten auch für weitergehende Fragestellungen zur Verfügung stehen, muss darauf explizit hingewiesen werden.

Erheben

Zusätzlich zu den Erhebungen im Rahmen der Zulassung, Immatrikulation und Rückmeldung darf insbesondere das Vorliegen der Zulassungsvoraussetzungen (also nur die Existenz der Hochschulzugangsberechtigung und der jeweils vorgeschriebenen Pflicht-Leistungsnachweise sowie ggf. von Zwischenprüfungen) erhoben werden.

Im Rahmen eines Prüfungsverfahrens können außerdem fristverlängernde Gründe (Kindeserziehung, Krankheit, Behinderung) und anerkannte Studienleistungen erhoben werden.

Grundlagen: § 125a UG und §§ 9 und 12 Hochschul-Datenschutzverordnung i.V.m. §§ 13 und 14 LDSG; sowie §§ 47 und 50 Studien- und Prüfungsordnung für die Informatikstudiengänge (Diplom) in der Fakultät für Informatik

Bearbeiten

Personenbezogene Daten, die im Rahmen etwaiger Sonderfälle erhoben wurden (wie ärztliche Atteste oder Härtefallbegründungen), sind nach einem Semester zu löschen.

Einem Prüfling ist innerhalb eines Jahres nach Abschluss des Prüfungsverfahrens auf formlosen Antrag gegenüber dem Prüfungsamt Einsicht in die ihn betreffenden Prüfungsakten zu gewähren. Danach sind sie zu sperren.

Grundlagen: § 125a UG und § 12 Hochschul-Datenschutzverordnung i.V.m. §§ 15 bis 25 LDSG; sowie § 37 Studien- und Prüfungsordnung für die Informatikstudiengänge (Diplom) in der Fakultät für Informatik

Veröffentlichen

Ein Veröffentlichen der Daten ist nur in anonymisierter Form im Zuge des Lehrberichts oder mit Einwilligung der Betroffenen erlaubt.

Bei der Dokumentation von Prüfungsleistungen ist darauf zu achten, dass die Studierenden nur ihre persönlichen Leistungen einsehen können.

Grundlagen: § 125a UG und § 11 Hochschul-Datenschutzverordnung sowie § 9 Abs. 4 LDSG

Technische Hinweise:

- Ist eine Prüfungsanmeldung mithilfe einer Chipkarte oder über Internet bzw. Intranet vorgesehen, muss sichergestellt sein, dass die Verbindung sichergestellt ist und sich der Studierende wirklich selbst angemeldet hat. Für die notwendige elektronische Signatur kommen insbesondere elliptische Kurven bzw. El Gamal-Verfahren (ISO/IEC 9796) sowie DAS (ISO/IEC 14888) in Frage.
- Verwendete Datenverarbeitungssysteme sind im Verfahrensverzeichnis zu dokumentieren, das vom zuständigen Datenschutzbeauftragten geführt wird (hier: der Landesdatenschutzbeauftragte). Hierbei ist darzulegen, welche personenbezogenen Daten (Art der Einzelmerkmale, Kreis der Betroffenen) in welchem Verfahren mit Hilfe welcher automatisierter Verfahren (welche Hard- und Software incl. der Vernetzung verwendet wird) auf welche Weise (und aufgrund welcher Rechtsgrundlage sowie zu welchem Zweck) verarbeitet werden und welche Datenschutzmaßnahmen (insbesondere zur Datensicherung) die verantwortliche Stelle dabei getroffen hat. Es ist außerdem aufzuführen, wer als Empfänger der Daten vorgesehen ist, welche Fristen für Löschung bzw. Sperrung vorgesehen sind und wer zugriffsberechtigt ist (siehe auch Datenschutzerklärungsmuster in der Anlage).

4.2.3 Durchführung einer internen Evaluation der Lehre

Situationsbeschreibung:

Eine Fakultät bzw. ein Fachbereich soll innerhalb der Universität bewertet werden und fertigt hierzu einen Lehrbericht an.

Verantwortliche Stelle ist die Fakultät bzw. der Fachbereich.

Uneingeschränkt geltende Grundsätze zum datenschutzgerechten Umgang:

1. Grundsätze der Datenverarbeitung:

- Der Zweck, zu dem personenbezogene Daten verarbeitet werden sollen, ist konkret festzulegen.
- Die erhobenen Daten müssen für den Zweck geeignet und erforderlich sein.
- Bei der Datenverarbeitung ist darauf zu achten, dass möglichst wenig personenbezogene Daten verarbeitet werden.

2. Einfluss der Einwilligung:
- Ohne Einwilligung des Betroffenen dürfen personenbezogene Daten nur auf der Grundlage einer ausdrücklichen Rechtsvorschrift (Gesetz, Verordnung) verarbeitet werden.
- Mit Einwilligung des Betroffenen (siehe hierzu auch das entsprechende Formblatt in der Anlage) dürfen personenbezogene Daten nur im Rahmen der getroffenen Vereinbarungen (und natürlich unter Einhaltung gesetzlicher Vorschriften) verwendet werden.
- Eine Einwilligung von Betroffenen erfordert, dass der Betroffene über die beabsichtigte Datenverarbeitung (incl. der Benennung der verantwortlichen Stelle, Art und Weise der Datenverarbeitung, dem Kreis der Zugangsberechtigten und dem Zeitpunkt der Löschung), deren Zweck und etwaige Empfänger der Daten aufgeklärt wird. Außerdem ist er über seine Rechte auf Auskunft über gespeicherte Daten, auf Berichtigung, Löschung bzw. Sperrung unrichtiger oder unzulässiger bzw. nicht mehr erforderlicher Daten und auf sein Recht zur Anrufung des zuständigen Datenschutzbeauftragten hinzuweisen. Die Einwilligung muss schriftlich erklärt werden, um wirksam werden zu können.

Fallspezifische Grundsätze zum datenschutzgerechten Umgang:

- Wenn für die Evaluation personenbezogene Daten an sich nicht wichtig sind, so sollten diese entweder anonymisiert erhoben oder so früh wie möglich anonymisiert werden. Ein erster Zwischenschritt hierzu ist die Pseudonymisierung (siehe auch unter technische Hinweise). Je eher die Daten (faktisch) anonymisiert sind, desto weniger Restriktionen unterliegt die Datenverarbeitung.
- Öffentlich zugängliche Daten dürfen jederzeit verarbeitet werden.
- Personenbezogene Daten von Studierenden, die auf der Grundlage einer Rechtsvorschrift angegeben werden müssen, können sowohl für Verwaltungszwecke als auch für andere Zwecke verarbeitet werden. 40 Jahre lang ab der Exmatrikulation bzw. Abschluss des Prüfungsverfahrens liegen in diesem Sinne vor: Name, Geschlecht, Geburtsdatum und -ort des Studierenden, dessen Studiengang und Matrikelnummer, Ergebnisse und Daten der Diplomvorprüfung sowie der Abschlussprüfung (letztere incl. Einzelnoten), etwaige Studienunterbrechungen (z.B. durch Urlaubssemester) und das Datum der Immatrikulation sowie der Exmatrikula-

tion. Allerdings sind diese Daten unverzüglich nach Abschluss des Prüfungsverfahrens zu sperren.
- Sollen die im Rahmen der Evaluation verarbeiteten personenbezogenen Daten auch für weitergehende Fragestellungen zur Verfügung stehen, muss darauf explizit hingewiesen werden.
- Eine Evaluation verfolgt in erster Linie das Ziel der Qualitätsverbesserung. Je eher etwaige Konsequenzen innerhalb der Universität gezogen werden, desto unproblematischer ist dies. Eine Evaluation setzt jedoch ein wissenschaftsäquivalentes Verfahren (gleichrangige Gutachter, wissenschaftliche Redlichkeit etc.) voraus und räumt Betroffenen grundsätzlich das Recht zur Gegendarstellung ein. Bei einer Lehrbewertung sind die Studierenden zu beteiligen.

Erheben

Universitäre Mitglieder sind zur Mitwirkung und Angabe notwendiger personenbezogener Daten verpflichtet.

Welche personenbezogenen Daten erhoben werden sollen, ist in einer universitären Satzung festzuschreiben.

Grundlagen: § 4a UG i.V.m. §§ 13 und 14 LDSG

Bearbeiten

Welche personenbezogenen Daten in welcher Form verarbeitet und bewertet werden sollen, ist in einer universitären Satzung festzuschreiben.

Ergebnisse von Lehrevaluationen sollen in anonymisierter Form den zuständigen Universitätsgremien übermittelt werden.

Aus den existierenden Datenbeständen dürfen in anonymisierter Form die notwendigen Strukturdaten (Fachstudiendauern, Schwund- und Erfolgsquoten, Absolventenquoten, Prüfungsnotenverteilungen, Entwicklung der Studierendenzahlen, Betreuungsrelationen zwischen Lehrenden und Lernenden, verfügbare Lehr- und Lernflächen bzw. Geräteausstattungen) weiterverarbeitet werden.

Umfragen bzw. Befragungen sind nur in anonymisierter Form weiter zu verarbeiten, es sei denn, die Betroffenen (hier: sowohl die Evaluierten wie auch die Evaluierenden) haben ausdrücklich ihr Einverständnis erklärt.

Grundlagen: § 4a UG i.V.m. § 11 Hochschul-Datenschutzverordnung und §§ 15 bis 25 LDSG

Veröffentlichen

Welche personenbezogenen Daten veröffentlicht werden sollen, ist in einer universitären Satzung festzuschreiben.

Ergebnisse von Lehrevaluationen sollen in anonymisierter Form Lehrenden und Studierenden bekanntgegeben werden.

Von Professoren, Hochschul- und Privatdozenten, Mitarbeitern des wissenschaftlichen Dienstes, Lehrbeauftragten, Lehrkräften für besondere Aufgaben sowie sonstigen Mitarbeitern, die herausgehobene Funktionen in der Universität wahrnehmen, dürfen Name, Amts-, Dienst- und Funktionsbezeichnung, Telefon- und Telefaxnummern sowie E-Mail- und Internet-Adressen veröffentlicht werden, sofern die Betroffenen kein höher zu bewertendes schutzwürdiges Interesse geltend machen können.

Die Veröffentlichung von Evaluationsergebnissen ist unbedenklich, wenn die gesamte untersuchte Einheit betroffen ist und nicht nur ein Lehrender alleine.

Es darf dargestellt werden, welche Lehrveranstaltungen abgehalten wurden. Eine Veröffentlichung der Bewertung von Lehrleistungen Einzelner ist hingegen nur bei deren ausdrücklicher Einwilligung erlaubt.

Grundlagen: §§ 4a und 125a Abs. 5 UG i.V.m. § 11 Hochschul-Datenschutzverordnung und § 15 LDSG

Technische Hinweise:

- Bei einer Pseudonymisierung sind die identifizierenden Daten durch Zuordnungstabellen und Verschlüsselungsverfahren zu verändern und getrennt zu speichern. Dabei kann vorgesehen werden, dass der Betroffene selbst ein Pseudonym vergibt. Als automatisierte Verschlüsselungsverfahren bieten sich Hash-Funktionen nach ISO/IEC 10118 an.
- Verwendete Datenverarbeitungssysteme sind im Verfahrensverzeichnis zu dokumentieren, das vom zuständigen Datenschutzbeauftragten geführt wird (hier: der Landesdatenschutzbeauftragte). Hierbei ist darzulegen, welche personenbezogenen Daten (Art der Einzelmerkmale, Kreis der Betroffenen) in welchem Verfahren mit Hilfe welcher automatisierter Verfahren (welche Hard- und Software incl. der Vernetzung verwendet wird) auf welche Weise (und aufgrund welcher Rechtsgrundlage sowie zu welchem Zweck) verarbeitet werden und welche Datenschutzmaßnahmen (insbesondere zur Datensicherung) die verantwortliche Stelle dabei getroffen hat. Es ist außerdem aufzuführen, wer als Empfänger der Daten vorgesehen ist, welche Fristen für Lö-

schung bzw. Sperrung vorgesehen sind und wer zugriffsberechtigt ist (siehe auch Datenschutzerklärungsmuster in der Anlage).

4.2.4 Durchführung einer externen Evaluation der Lehre

Situationsbeschreibung:

Eine Fakultät bzw. ein Fachbereich soll durch Dritte, z.B. der Evaluationsagentur Baden-Württemberg, bewertet werden.

Verantwortliche Stelle ist die Evaluationsagentur, die die Fakultät bzw. den Fachbereich (als übermittelnde Stelle) zur Einhaltung der Datenschutzbestimmungen zu verpflichten hat.

Uneingeschränkt geltende Grundsätze zum datenschutzgerechten Umgang:

1. Grundsätze der Datenverarbeitung:
- Der Zweck, zu dem personenbezogene Daten verarbeitet werden sollen, ist konkret festzulegen.
- Die erhobenen Daten müssen für den Zweck geeignet und erforderlich sein.
- Bei der Datenverarbeitung ist darauf zu achten, dass möglichst wenig personenbezogene Daten verarbeitet werden.

2. Einfluss der Einwilligung:
- Ohne Einwilligung des Betroffenen dürfen personenbezogene Daten nur auf der Grundlage einer ausdrücklichen Rechtsvorschrift (Gesetz, Verordnung) verarbeitet werden.
- Mit Einwilligung des Betroffenen (siehe hierzu auch das entsprechende Formblatt in der Anlage) dürfen personenbezogene Daten nur im Rahmen der getroffenen Vereinbarungen (und natürlich unter Einhaltung gesetzlicher Vorschriften) verwendet werden.
- Eine Einwilligung von Betroffenen erfordert, dass der Betroffene über die beabsichtigte Datenverarbeitung (incl. der Benennung der verantwortlichen Stelle, Art und Weise der Datenverarbeitung, dem Kreis der Zugangsberechtigten und dem Zeitpunkt der Löschung), deren Zweck und etwaige Empfänger der Daten aufgeklärt wird. Außerdem ist er über seine Rechte auf Auskunft über gespeicherte Daten, auf Berichtigung, Löschung bzw. Sperrung unrichtiger oder unzulässiger bzw. nicht mehr erforderlicher Daten und auf sein Recht zur Anrufung des zuständigen Datenschutzbeauftragten hinzuweisen. Die Einwilligung muss schriftlich erklärt werden, um wirksam werden zu können.

Fallspezifische Grundsätze zum datenschutzgerechten Umgang:

- Wenn für die Evaluation personenbezogene Daten an sich nicht wichtig sind, so sollten diese entweder anonymisiert erhoben oder so früh wie möglich anonymisiert werden. Ein erster Zwischenschritt hierzu ist die Pseudonymisierung (siehe auch unter technische Hinweise). Je eher die Daten (faktisch) anonymisiert sind, desto weniger Restriktionen unterliegt die Datenverarbeitung.
- Öffentlich zugängliche Daten dürfen jederzeit verarbeitet werden.
- Personenbezogene Daten von Studierenden, die auf der Grundlage einer Rechtsvorschrift angegeben werden müssen, können sowohl für Verwaltungszwecke als auch für andere Zwecke verarbeitet werden. 40 Jahre lang ab der Exmatrikulation bzw. Abschluss des Prüfungsverfahrens liegen in diesem Sinne vor: Name, Geschlecht, Geburtsdatum und -ort des Studierenden, dessen Studiengang und Matrikelnummer, Ergebnisse und Daten der Diplomvorprüfung sowie der Abschlussprüfung (letztere incl. Einzelnoten), etwaige Studienunterbrechungen (z.B. durch Urlaubssemester) und das Datum der Immatrikulation sowie der Exmatrikulation. Allerdings sind diese Daten unverzüglich nach Abschluss des Prüfungsverfahrens zu sperren.
- Sollen die im Rahmen der Evaluation verarbeiteten personenbezogenen Daten auch für weitergehende Fragestellungen zur Verfügung stehen, muss darauf explizit hingewiesen werden.
- Eine Evaluation verfolgt in erster Linie das Ziel der Qualitätsverbesserung. Je eher etwaige Konsequenzen innerhalb der Universität gezogen werden, desto unproblematischer ist dies. Eine Evaluation setzt jedoch ein wissenschaftsäquivalentes Verfahren (gleichrangige Gutachter, wissenschaftliche Redlichkeit etc.) voraus und räumt Betroffenen grundsätzlich das Recht zur Gegendarstellung ein. Bei einer Lehrbewertung sind die Studierenden zu beteiligen.

Erheben

Universitäre Mitglieder sind zur Mitwirkung und Angabe notwendiger personenbezogener Daten verpflichtet.

Welche personenbezogenen Daten erhoben werden sollen, ist in einer universitären Satzung festzuschreiben.

Die Erhebung unter den universitären Mitgliedern darf nur durch die Universität selbst erfolgen.

Ist mit der externen Evaluation die Einwerbung von Fördermitteln verbunden, stellt der Antrag auf Einwerbung eine Einwilligungserklärung der Betroffenen dar.

Grundlagen: § 4a UG i.V.m. §§ 13 und 14 LDSG

Bearbeiten

Welche personenbezogenen Daten in welcher Form verarbeitet und bewertet werden sollen, ist in einer universitären Satzung festzuschreiben.

Ergebnisse von Lehrevaluationen sollen in anonymisierter Form den zuständigen Universitätsgremien übermittelt werden.

Im Regelfall ist die externe Einrichtung nur Empfänger der von der untersuchten Einrichtung übermittelten Daten.

Die Übermittlung von Evaluationsergebnissen ist unbedenklich, wenn die gesamte untersuchte Einheit betroffen ist und nicht nur ein Lehrender alleine.

Die externe Einrichtung kann übermittelte personenbezogene Daten nur im Rahmen der Einwilligungserklärungen der Betroffenen verarbeiten.

Aus den existierenden Datenbeständen dürfen in anonymisierter Form die notwendigen Strukturdaten (Fachstudiendauern, Schwund- und Erfolgsquoten, Absolventenquoten, Prüfungsnotenverteilungen, Entwicklung der Studierendenzahlen, Betreuungsrelationen zwischen Lehrenden und Lernenden, verfügbare Lehr- und Lernflächen bzw. Geräteausstattungen) übermittelt werden.

Umfragen bzw. Befragungen sind nur in anonymisierter Form weiter zu verarbeiten, es sei denn, die Betroffenen (hier: sowohl die Evaluierten wie auch die Evaluierenden) haben ausdrücklich ihr Einverständnis erklärt.

Grundlagen: § 4a UG i.V.m. §§ 15 bis 25 LDSG

Veröffentlichen

Welche personenbezogenen Daten veröffentlicht werden sollen, ist in einer universitären Satzung festzuschreiben.

Ergebnisse von Lehrevaluationen sollen in anonymisierter Form Lehrenden und Studierenden bekannt gegeben werden.

Von Professoren, Hochschul- und Privatdozenten, Mitarbeitern des wissenschaftlichen Dienstes, Lehrbeauftragten, Lehrkräften für besondere Aufgaben sowie sonstigen Mitarbeitern, die herausgehobene Funktionen in der Universität wahrnehmen, dürfen Name, Amts-, Dienst- und Funktionsbezeichnung, Telefon- und Telefaxnummern sowie E-Mail- und Internet-Adressen veröffentlicht werden, sofern die Betroffenen kein höher zu bewertendes schutzwürdiges Interesse geltend machen können.

Die Veröffentlichung von Evaluationsergebnissen ist unbedenklich, wenn die gesamte untersuchte Einheit betroffen ist und nicht nur ein Lehrender alleine.

Es darf dargestellt werden, welche Lehrveranstaltungen abgehalten wurden. Eine Veröffentlichung der Bewertung von Lehrleistungen Einzelner ist hingegen nur bei deren ausdrücklicher Einwilligung erlaubt.

Grundlagen: §§ 4a und 125a Abs. 5 UG i.V.m. § 15 LDSG

Technische Hinweise:

- Bei einer Pseudonymisierung sind die identifizierenden Daten durch Zuordnungstabellen und Verschlüsselungsverfahren zu verändern und getrennt zu speichern. Dabei kann vorgesehen werden, dass der Betroffene selbst ein Pseudonym vergibt. Als automatisierte Verschlüsselungsverfahren bieten sich Hash-Funktionen nach ISO/IEC 10118 an.
- Verwendete Datenverarbeitungssysteme sind im Verfahrensverzeichnis zu dokumentieren, das vom zuständigen Datenschutzbeauftragten geführt wird (hier: der Landesdatenschutzbeauftragte). Hierbei ist darzulegen, welche personenbezogenen Daten (Art der Einzelmerkmale, Kreis der Betroffenen) in welchem Verfahren mit Hilfe welcher automatisierter Verfahren (welche Hard- und Software incl. der Vernetzung verwendet wird) auf welche Weise (und aufgrund welcher Rechtsgrundlage sowie zu welchem Zweck) verarbeitet werden und welche Datenschutzmaßnahmen (insbesondere zur Datensicherung) die verantwortliche Stelle dabei getroffen hat. Es ist außerdem aufzuführen, wer als Empfänger der Daten vorgesehen ist, welche Fristen für Löschung bzw. Sperrung vorgesehen sind und wer zugriffsberechtigt ist (siehe auch Datenschutzerklärungsmuster in der Anlage).

4.2.5 Einführung und Nutzung einer Chipkarte

Situationsbeschreibung:

Studierende erhalten eine kontaktlose Multifunktionskarte, die den Semesterausweis ersetzt, zur Rückmeldung und zum Erwerb des Semestertickets berechtigt, Zugang zu Rechnerpools und pre-paid-Zahlungen für Mensa, Cafeterien, Automaten und Uni-Bibliothek ermöglicht.

Verantwortliche Stelle ist das Studiensekretariat (hinsichtlich Semesterausweis und Rückmeldung sowie in Zusammenarbeit mit dem entsprechenden Aufsteller bei Automaten), das Studentenwerk (hinsichtlich Mensa und Cafeterien sowie an der Universität Ulm in Zusammenarbeit mit dem Nahverkehrsverbund DING beim Semesterticket) und das Rechenzentrum (an der Universität Ulm als Teil des Kommunikations- und Informationszentrums) bzw. (für die Informatik-Fakultät) die Service-Gruppe Informatik (hinsichtlich des Zugangs zu Rechnerpools).

Uneingeschränkt geltende Grundsätze zum datenschutzgerechten Umgang:

1. Grundsätze der Datenverarbeitung:
- Der Zweck, zu dem personenbezogene Daten verarbeitet werden sollen, ist konkret festzulegen.
- Die erhobenen Daten müssen für den Zweck geeignet und erforderlich sein.
- Bei der Datenverarbeitung ist darauf zu achten, dass möglichst wenig personenbezogene Daten verarbeitet werden.

2. Einfluss der Einwilligung:
- Ohne Einwilligung des Betroffenen dürfen personenbezogene Daten nur auf der Grundlage einer ausdrücklichen Rechtsvorschrift (Gesetz, Verordnung) verarbeitet werden.
- Mit Einwilligung des Betroffenen (siehe hierzu auch das entsprechende Formblatt in der Anlage) dürfen personenbezogene Daten nur im Rahmen der getroffenen Vereinbarungen (und natürlich unter Einhaltung gesetzlicher Vorschriften) verwendet werden.
- Eine Einwilligung von Betroffenen erfordert, dass der Betroffene über die beabsichtigte Datenverarbeitung (incl. der Benennung der verantwortlichen Stelle, Art und Weise der Datenverarbeitung, dem Kreis der Zugangsberechtigten und dem Zeitpunkt der Löschung), deren Zweck und etwaige Empfänger der Daten aufgeklärt wird. Außerdem ist er über seine Rechte auf Auskunft über gespeicherte Daten, auf Berichtigung, Löschung bzw. Sperrung unrichtiger oder unzulässiger bzw. nicht mehr erforderlicher Daten und auf sein

Recht zur Anrufung des zuständigen Datenschutzbeauftragten hinzuweisen. Die Einwilligung muss schriftlich erklärt werden, um wirksam werden zu können.

Fallspezifische Grundsätze zum datenschutzgerechten Umgang:

- Personenbezogene Daten von Studierenden, die auf der Grundlage einer Rechtsvorschrift angegeben werden müssen, können sowohl für Verwaltungszwecke als auch für andere Zwecke verarbeitet werden. 40 Jahre lang ab der Exmatrikulation bzw. Abschluss des Prüfungsverfahrens liegen in diesem Sinne vor: Name, Geschlecht, Geburtsdatum und -ort des Studierenden, dessen Studiengang und Matrikelnummer, Ergebnisse und Daten der Diplomvorprüfung sowie der Abschlussprüfung (letztere incl. Einzelnoten), etwaige Studienunterbrechungen (z.B. durch Urlaubssemester) und das Datum der Immatrikulation sowie der Exmatrikulation. Allerdings sind diese Daten unverzüglich nach Abschluss des Prüfungsverfahrens zu sperren.
- Betroffene, an die Chipkarten ausgegeben werden sollen, sind auf ihre Rechte (siehe unter Einfluss der Einwilligung) ausdrücklich hinzuweisen, über Maßnahmen und Folgen des Verlustes der Chipkarte aufzuklären und müssen erkennen können, wann Daten von der Chipkarte gelesen und verarbeitet werden (hierzu ist es notwendig, die Funktionsweise der Chipkarte möglichst allgemeinverständlich und die Art der zu verarbeitenden personenbezogenen Daten mitzuteilen).

Erheben

Im Rahmen der Zulassung und Immatrikulation wurden die notwendigen Daten bereits erhoben und dürfen für die Chipkarte genutzt werden.

Außerdem werden personenbezogene (Protokollierungs-) Daten im Rahmen der Nutzung der Chipkarte erhoben.

Grundlagen: § 125a UG (sowie § 96 Abs. 4 UG) und § 7 HochschulDatenschutzverordnung i.V.m. § 5 LDSG und §§ 13 und 14 LDSG

Bearbeiten

Jede verantwortliche Stelle darf nur die Daten einsehen können, für die sie zuständig und zu der sie rechtlich befugt ist. Eine Verarbeitung anderer Daten der Chipkarte ist nicht erlaubt.

Ein Bewegungsprofil darf nicht erstellt werden.

Protokolldaten sind nach einem Semester zu löschen.

Zu den Einschränkungen bei der Verarbeitung der Daten siehe auch unter technische Hinweise.

Grundlagen: § 125a UG und § 7 Hochschul-Datenschutzverordnung i.V.m. § 5 LDSG und §§ 15 bis 25 LDSG

Veröffentlichen

Ein Veröffentlichen der Daten ist nur in anonymisierter Form oder mit Einwilligung der Betroffenen erlaubt.

Grundlagen: § 125a UG und § 7 Hochschul-Datenschutzverordnung

Technische Hinweise:

- Vor Einführung der Chipkarte ist der zuständige Datenschutzbeauftragte (hier: der Landesdatenschutzbeauftragte) zu informieren und eine Vorabkontrolle durchzuführen. Dabei ist sicherzustellen, dass durch das zum Einsatz kommende Chipkarten-System keine besonderen Gefahren für das Persönlichkeitsrecht bestehen. In diesem Zusammenhang ist eine fristgerechte Löschung der gespeicherten Daten sowie von Protokolldaten, die durch die Chipkarte ausgelöst werden, sicherzustellen und zu verhindern, dass Unbefugte Daten lesen können.
- Die Chipkarte muss fälschungssichere Authentisierungsmerkmale (Unterschrift, Passbild, ggf. Hologramme) und Sicherheitsmechanismen gegen unbefugte Auswertungen ihrer Inhalte aufweisen. Zugriffs- und Nutzungsberechtigungen sind durch die Chipkarte selbst zu steuern. Die Kommunikation mit Nutzungsgeräten ist insbesondere durch kryptographische Maßnahmen und einer abhör- und fälschungssicheren Datenübertragung abzuschotten (siehe ISO/IEC 9798). Zur Verschlüsselung von Daten, Aufnahme von Signaturfunktionen auf der Chipkarte und Generierung von Zufallszahlen sind allgemein anerkannte und veröffentlichte Algorithmen zu verwenden (symmetrische Verschlüsselungsalgorithmen wie DES oder asymmetrische Verfahren wie RSA nach ISO/IEC 7816 bzw. elliptische Kurven oder El Gamal-Verfahren nach ISO/IEC 9796 oder DAS nach ISO/IEC 14888). Unterschiedliche Anwendungen dürfen sich nicht

gegenseitig beeinflussen und der Chipkartenhersteller darf nicht über ein Gesamtwissen verfügen.
- Verwendete Datenverarbeitungssysteme sind im Verfahrensverzeichnis zu dokumentieren, das vom zuständigen Datenschutzbeauftragten geführt wird (hier: der Landesdatenschutzbeauftragte). Hierbei ist darzulegen, welche personenbezogenen Daten (Art der Einzelmerkmale, Kreis der Betroffenen) in welchem Verfahren mit Hilfe welcher automatisierter Verfahren (welche Hard- und Software incl. der Vernetzung verwendet wird) auf welche Weise (und aufgrund welcher Rechtsgrundlage sowie zu welchem Zweck) verarbeitet werden und welche Datenschutzmaßnahmen (insbesondere zur Datensicherung) die verantwortliche Stelle dabei getroffen hat. Es ist außerdem aufzuführen, wer als Empfänger der Daten vorgesehen ist, welche Fristen für Löschung bzw. Sperrung vorgesehen sind und wer zugriffsberechtigt ist (siehe auch Datenschutzerklärungsmuster in der Anlage).

4.2.6 Alltag innerhalb einer Abteilung im Rahmen der Lehrverpflichtung

Situationsbeschreibung:

Eine Abteilung bietet Lehrveranstaltungen an, zu denen sie Leistungsnachweise ausgibt und Prüfungen durchführt.

Verantwortliche Stelle ist die Abteilung.

Uneingeschränkt geltende Grundsätze zum datenschutzgerechten Umgang:

1. Grundsätze der Datenverarbeitung:
- Der Zweck, zu dem personenbezogene Daten verarbeitet werden sollen, ist konkret festzulegen.
- Die erhobenen Daten müssen für den Zweck geeignet und erforderlich sein.
- Bei der Datenverarbeitung ist darauf zu achten, dass möglichst wenig personenbezogene Daten verarbeitet werden.

2. Einfluss der Einwilligung:
- Ohne Einwilligung des Betroffenen dürfen personenbezogene Daten nur auf der Grundlage einer ausdrücklichen Rechtsvorschrift (Gesetz, Verordnung) verarbeitet werden.
- Mit Einwilligung des Betroffenen (siehe hierzu auch das entsprechende Formblatt in der Anlage) dürfen personenbezogene Daten nur im Rahmen der getroffenen Vereinbarungen

(und natürlich unter Einhaltung gesetzlicher Vorschriften) verwendet werden.
- Eine Einwilligung von Betroffenen erfordert, dass der Betroffene über die beabsichtigte Datenverarbeitung (incl. der Benennung der verantwortlichen Stelle, Art und Weise der Datenverarbeitung, dem Kreis der Zugangsberechtigten und dem Zeitpunkt der Löschung), deren Zweck und etwaige Empfänger der Daten aufgeklärt wird. Außerdem ist er über seine Rechte auf Auskunft über gespeicherte Daten, auf Berichtigung, Löschung bzw. Sperrung unrichtiger oder unzulässiger bzw. nicht mehr erforderlicher Daten und auf sein Recht zur Anrufung des zuständigen Datenschutzbeauftragten hinzuweisen. Die Einwilligung muss schriftlich erklärt werden, um wirksam werden zu können.

Fallspezifische Grundsätze zum datenschutzgerechten Umgang:

- Personenbezogene Daten von Studierenden, die auf der Grundlage einer Rechtsvorschrift angegeben werden müssen, können sowohl für Verwaltungszwecke als auch für andere Zwecke verarbeitet werden. 40 Jahre lang ab der Exmatrikulation bzw. Abschluss des Prüfungsverfahrens liegen in diesem Sinne vor: Name, Geschlecht, Geburtsdatum und -ort des Studierenden, dessen Studiengang und Matrikelnummer, Ergebnisse und Daten der Diplomvorprüfung sowie der Abschlussprüfung (letztere incl. Einzelnoten), etwaige Studienunterbrechungen (z.B. durch Urlaubssemester) und das Datum der Immatrikulation sowie der Exmatrikulation. Allerdings sind diese Daten unverzüglich nach Abschluss des Prüfungsverfahrens zu sperren.
- Sollen die im Rahmen des Prüfungsverfahrens verarbeiteten personenbezogenen Daten auch für weitergehende Fragestellungen zur Verfügung stehen, muss darauf explizit hingewiesen werden.

Erheben

Um Leistungsnachweise ausstellen zu können, ist es für die Abteilung unerlässlich, personenbezogene Daten zu erheben. Hierbei ist sie berechtigt, Name, Matrikelnummer, Anschrift und die Zahl der bisherigen Fachsemester zu erfassen.

Grundlagen: § 125a UG und §§ 9 und 12 Hochschul-Datenschutzverordnung i.V.m. §§ 13 und 14 LDSG

Bearbeiten

Einem Prüfling ist innerhalb eines Jahres nach Abschluss des Prüfungsverfahrens auf Antrag Einsicht in die ihn betreffenden Prüfungsakten zu gewähren. Danach sind sie zu sperren.

Zur Teilnahme von Lehrveranstaltungen erforderliche Daten, Noten von Klausuren und Hausarbeiten sowie etwaige Gesamtnoten dürfen automatisiert verarbeitet werden.

Ein Semester nach Ausstellung von Leistungsnachweisen sind die dafür qualifizierenden Leistungen zu sperren.

Nach fünf Jahren ist beim Studiensekretariat nachzufragen, für wen die Klausurergebnisse, Praktikumsberichte, Softwaredokumentationen, Teilnehmerlisten zu löschen sind, aufgrund derer ein Leistungsnachweis ausgestellt wurde.

Ist es für den Betroffenen von Vorteil, Mitteilungen über den laufenden Lehrbetrieb zu erhalten (etwa über Verlegung oder Ausfall von Lehrveranstaltungen), kann die verantwortliche Stelle die entsprechenden Daten vom Studiensekretariat erhalten, muss diese aber unverzüglich löschen. Die Mitteilung kann aber auch über das Studiensekretariat im Rahmen eines Adressmitteilungsverfahrens (die Mitteilungen werden über das Studiensekretariat an die Betroffenen gesandt, die Adressen bleiben der Abteilung unbekannt) erfolgen.

Grundlagen: § 125a UG sowie §§ 9 und 12 Hochschul-Datenschutzverordnung i.V.m. §§ 15 bis 25 LDSG; sowie § 37 Studien- und Prüfungsordnung für die Informatikstudiengänge (Diplom) in der Fakultät für Informatik

Veröffentlichen

Ein Veröffentlichen der Daten ist nur in anonymisierter Form oder mit Einwilligung der Betroffenen erlaubt.

Bei der Dokumentation von Leistungen zum Erwerb von Scheinen sowie von Prüfungsleistungen ist darauf zu achten, dass die Studierenden nur ihre persönlichen Leistungen einsehen können. Insofern sind auch keine Aushänge sowie Internet-/Intranet-Veröffentlichung mit Namenslisten bzw. Matrikelnummern erlaubt.

Grundlagen: § 125a UG und § 9 Abs. 4 LDSG

Technische Hinweise:

- Ist eine Anmeldung zu einer Prüfung oder einer Lehrveranstaltung mithilfe einer Chipkarte oder über Internet bzw.

Intranet vorgesehen, muss sichergestellt sein, dass die Verbindung sichergestellt ist und sich der Studierende wirklich selbst angemeldet hat. Für die notwendige elektronische Signatur kommen insbesondere elliptische Kurven bzw. El Gamal-Verfahren (ISO/IEC 9796) sowie DAS (ISO/IEC 14888) in Frage.

- Verwendete Datenverarbeitungssysteme sind im Verfahrensverzeichnis zu dokumentieren, das vom zuständigen Datenschutzbeauftragten geführt wird (hier: der Landesdatenschutzbeauftragte). Hierbei ist darzulegen, welche personenbezogenen Daten (Art der Einzelmerkmale, Kreis der Betroffenen) in welchem Verfahren mit Hilfe welcher automatisierter Verfahren (welche Hard- und Software incl. der Vernetzung verwendet wird) auf welche Weise (und aufgrund welcher Rechtsgrundlage sowie zu welchem Zweck) verarbeitet werden und welche Datenschutzmaßnahmen (insbesondere zur Datensicherung) die verantwortliche Stelle dabei getroffen hat. Es ist außerdem aufzuführen, wer als Empfänger der Daten vorgesehen ist, welche Fristen für Löschung bzw. Sperrung vorgesehen sind und wer zugriffsberechtigt ist (siehe auch Datenschutzerklärungsmuster in der Anlage).

4.2.7 Durchführung der fachbezogenen Studienberatung

Situationsbeschreibung:

Eine Fakultät bzw. ein Fachbereich ist angehalten, ihren Studierenden eine fachbezogene Studienberatung anzubieten. Dies kann sowohl mündlich (im klassischen Verfahren) als auch DV-gestützt erfolgen, wie dies an der Fakultät für Informatik an der Universität Ulm mit dem Studien-Assistenz-System (SASy) geplant ist.

Verantwortliche Stelle ist die Studienberatungsstelle.

Uneingeschränkt geltende Grundsätze zum datenschutzgerechten Umgang:

1. Grundsätze der Datenverarbeitung:

- Der Zweck, zu dem personenbezogene Daten verarbeitet werden sollen, ist konkret festzulegen.
- Die erhobenen Daten müssen für den Zweck geeignet und erforderlich sein.
- Bei der Datenverarbeitung ist darauf zu achten, dass möglichst wenig personenbezogene Daten verarbeitet werden.

2. Einfluss der Einwilligung:
- Ohne Einwilligung des Betroffenen dürfen personenbezogene Daten nur auf der Grundlage einer ausdrücklichen Rechtsvorschrift (Gesetz, Verordnung) verarbeitet werden.
- Mit Einwilligung des Betroffenen (siehe hierzu auch das entsprechende Formblatt in der Anlage) dürfen personenbezogene Daten nur im Rahmen der getroffenen Vereinbarungen (und natürlich unter Einhaltung gesetzlicher Vorschriften) verwendet werden.
- Eine Einwilligung von Betroffenen erfordert, dass der Betroffene über die beabsichtigte Datenverarbeitung (incl. der Benennung der verantwortlichen Stelle, Art und Weise der Datenverarbeitung, dem Kreis der Zugangsberechtigten und dem Zeitpunkt der Löschung), deren Zweck und etwaige Empfänger der Daten aufgeklärt wird. Außerdem ist er über seine Rechte auf Auskunft über gespeicherte Daten, auf Berichtigung, Löschung bzw. Sperrung unrichtiger oder unzulässiger bzw. nicht mehr erforderlicher Daten und auf sein Recht zur Anrufung des zuständigen Datenschutzbeauftragten hinzuweisen. Die Einwilligung muss schriftlich erklärt werden, um wirksam werden zu können.

Fallspezifische Grundsätze zum datenschutzgerechten Umgang:

- Personenbezogene Daten von Studierenden, die auf der Grundlage einer Rechtsvorschrift angegeben werden müssen, können sowohl für Verwaltungszwecke als auch für andere Zwecke verarbeitet werden. 40 Jahre lang ab der Exmatrikulation bzw. Abschluss des Prüfungsverfahrens liegen in diesem Sinne vor: Name, Geschlecht, Geburtsdatum und -ort des Studierenden, dessen Studiengang und Matrikelnummer, Ergebnisse und Daten der Diplomvorprüfung sowie der Abschlussprüfung (letztere incl. Einzelnoten), etwaige Studienunterbrechungen (z.B. durch Urlaubssemester) und das Datum der Immatrikulation sowie der Exmatrikulation. Allerdings sind diese Daten unverzüglich nach Abschluss des Prüfungsverfahrens zu sperren.
- Sollen die im Rahmen der Studienberatung verarbeiteten personenbezogenen Daten auch für weitergehende Fragestellungen zur Verfügung stehen, muss darauf explizit hingewiesen werden.
- Wenn im Rahmen der Studienberatung keine personenbezogenen Daten verarbeitet werden, erübrigt sich jeglicher Datenschutz. Grundsätzlich dürfen personenbezogene Da-

ten, die im Rahmen der Studienberatung anfallen, nicht weiterverarbeitet werden – es sei denn, der Betroffene hat dies ausdrücklich genehmigt. Wohl aber dürfen hierzu Daten aus dem Prüfungsverfahren hinzugezogen werden.

Erheben

Soweit für die Studienberatung relevante personenbezogene Daten nicht durch Zulassung, Immatrikulation oder Rückmeldung bereits vorliegen und für Verwaltungszwecke bzw. sonstige Zwecke und damit auch der Studienberatung verarbeitet werden dürfen, ist es nur erlaubt, Daten mit Einwilligung des Betroffenen zu erheben.

Grundlagen: §§ 13 und 14 LDSG

Bearbeiten

Für die Studienberatung können anhand der Prüfungsverfahren folgende personenbezogene Daten weiterverarbeitet werden: Matrikelnummer, Art der Prüfung, Zulassungsvoraussetzungen (Existenz der Hochschulzugangsberechtigung, i.d.R. das Abitur, und vorgeschriebener Leistungsnachweise sowie bei Abschlussprüfungen auch von Zwischenprüfungen) und die Anzahl bisheriger Prüfungsversuche.

Im Rahmen einer Studienberatung zusätzlich erfasste Daten dürfen nur mit Zustimmung des Betroffenen übermittelt werden.

Sofern mit den Betroffenen keine längere Frist vereinbart wurde, sind speziell für die Studienberatung erhobene Daten nach einem Semester zu löschen.

Grundlagen: §§ 49 Abs. 4 und 125a UG sowie §§ 9 und 12 Hochschul-Datenschutzverordnung i.V.m. §§ 9 und 15 bis 20 LDSG

Veröffentlichen

Ein Veröffentlichen der Daten ist nur in anonymisierter Form oder mit Einwilligung der Betroffenen erlaubt.

Grundlagen: § 49 Abs. 4 UG i.V.m. § 15 LDSG

Technische Hinweise:

- Vor Einführung eines automatisierten Abrufverfahrens (Kennzeichen ist die programmgesteuerte Datenverarbeitung) zum Zweck der Studienberatung ist der zuständige Datenschutzbeauftragte (hier: der Landesdatenschutzbeauftragte) zu informieren und eine Vorabkontrolle durchzuführen. Dabei ist sicherzustellen, dass durch das zum Einsatz

kommende System keine besonderen Gefahren für das Persönlichkeitsrecht bestehen. In diesem Zusammenhang ist eine fristgerechte Löschung der gespeicherten Daten sicherzustellen und zu verhindern, dass Unbefugte Daten lesen können.

- Ist eine Studienberatung über Internet bzw. Intranet vorgesehen, muss sichergestellt sein, dass die Verbindung sichergestellt ist und sich der Studierende wirklich selbst angemeldet hat. Für die notwendige elektronische Signatur kommen insbesondere elliptische Kurven bzw. El Gamal-Verfahren (ISO/IEC 9796) sowie DAS (ISO/IEC 14888) in Frage.
- Verwendete Datenverarbeitungssysteme sind im Verfahrensverzeichnis zu dokumentieren, das vom zuständigen Datenschutzbeauftragten geführt wird (hier: der Landesdatenschutzbeauftragte). Hierbei ist darzulegen, welche personenbezogenen Daten (Art der Einzelmerkmale, Kreis der Betroffenen) in welchem Verfahren mit Hilfe welcher automatisierter Verfahren (welche Hard- und Software incl. der Vernetzung verwendet wird) auf welche Weise (und aufgrund welcher Rechtsgrundlage sowie zu welchem Zweck) verarbeitet werden und welche Datenschutzmaßnahmen (insbesondere zur Datensicherung) die verantwortliche Stelle dabei getroffen hat. Es ist außerdem aufzuführen, wer als Empfänger der Daten vorgesehen ist, welche Fristen für Löschung bzw. Sperrung vorgesehen sind und wer zugriffsberechtigt ist (siehe auch Datenschutzerklärungsmuster in der Anlage).

4.2.8 Anfragen über Studierendendaten

Situationsbeschreibung:

Durch Dritte wird an die Universität die Bitte herangetragen, mit Studierenden in Kontakt treten zu können bzw. deren Meldedaten übermittelt oder überprüft zu bekommen.

Verantwortliche Stelle ist das Studiensekretariat.

Uneingeschränkt geltende Grundsätze zum datenschutzgerechten Umgang:

1. Grundsätze der Datenverarbeitung:

- Der Zweck, zu dem personenbezogene Daten verarbeitet werden sollen, ist konkret festzulegen.
- Die erhobenen Daten müssen für den Zweck geeignet und erforderlich sein.

- Bei der Datenverarbeitung ist darauf zu achten, dass möglichst wenig personenbezogene Daten verarbeitet werden.

2. Einfluss der Einwilligung:
- Ohne Einwilligung des Betroffenen dürfen personenbezogene Daten nur auf der Grundlage einer ausdrücklichen Rechtsvorschrift (Gesetz, Verordnung) verarbeitet werden.
- Mit Einwilligung des Betroffenen (siehe hierzu auch das entsprechende Formblatt in der Anlage) dürfen personenbezogene Daten nur im Rahmen der getroffenen Vereinbarungen (und natürlich unter Einhaltung gesetzlicher Vorschriften) verwendet werden.
- Eine Einwilligung von Betroffenen erfordert, dass der Betroffene über die beabsichtigte Datenverarbeitung (incl. der Benennung der verantwortlichen Stelle, Art und Weise der Datenverarbeitung, dem Kreis der Zugangsberechtigten und dem Zeitpunkt der Löschung), deren Zweck und etwaige Empfänger der Daten aufgeklärt wird. Außerdem ist er über seine Rechte auf Auskunft über gespeicherte Daten, auf Berichtigung, Löschung bzw. Sperrung unrichtiger oder unzulässiger bzw. nicht mehr erforderlicher Daten und auf sein Recht zur Anrufung des zuständigen Datenschutzbeauftragten hinzuweisen. Die Einwilligung muss schriftlich erklärt werden, um wirksam werden zu können.

Fallspezifische Grundsätze zum datenschutzgerechten Umgang:

- Personenbezogene Daten von Studierenden, die auf der Grundlage einer Rechtsvorschrift angegeben werden müssen, können sowohl für Verwaltungszwecke als auch für andere Zwecke verarbeitet werden. 40 Jahre lang ab der Exmatrikulation bzw. Abschluss des Prüfungsverfahrens liegen in diesem Sinne vor: Name, Geschlecht, Geburtsdatum und -ort des Studierenden, dessen Studiengang und Matrikelnummer, Ergebnisse und Daten der Diplomvorprüfung sowie der Abschlussprüfung (letztere incl. Einzelnoten), etwaige Studienunterbrechungen (z.B. durch Urlaubssemester) und das Datum der Immatrikulation sowie der Exmatrikulation. Allerdings sind diese Daten unverzüglich nach Abschluss des Prüfungsverfahrens zu sperren.

Erheben

Eine gesonderte Erhebung von Daten findet in diesem Falle nicht statt.

Grundlagen: §§ 13 und 14 LDSG

Bearbeiten

Für einzelne Fälle existiert eine gesetzliche Grundlage für die Übermittlung von Studierendendaten (Beschäftigung als hilfswissenschaftliche Kraft, Anfragen von Polizeibehörden, Staatsanwaltschaften, Gerichten, Behörden der Gefahrenabwehr, Justiz-Vollzugs-Anstalten, zur Durchsetzung öffentlich-rechtlicher Ansprüche und bei Auskunftspflichten im Rahmen der Sozialgesetzgebung).

Grundsätzlich ist vor einer Übermittlung stets zu prüfen, ob der Empfänger der zu übermittelnden Daten berechtigt ist, diese abzufragen.

Bei externen Anfragen zu Umfragezwecken ist ein Adressmittlungsverfahren (die Mitteilungen/Fragebögen werden über das Studiensekretariat an die Betroffenen gesandt, die Adressen bleiben der anfragenden Stelle unbekannt) zweckmäßig.

Gegen eine universitätsinterne Abfrage durch eine Einrichtung, ob bestimmte Studierende noch eingeschrieben sind, ist nichts einzuwenden, da diese Daten auch für sonstige Zwecke verwendet werden dürfen. Es dürfen auch Adressdaten zur Übermittlung von Mitteilungen zum laufenden Lehrbetrieb übermittelt werden, jedoch ist hierfür ein Adressmittlungsverfahren (siehe oben) vorzuziehen. Weitergegebene Daten sind unverzüglich vom Empfänger zu löschen.

Grundlagen: § 125a UG sowie § 12 Hochschul-Datenschutzverordnung i.V.m. §§ 15 bis 20 LDSG

Veröffentlichen

Ein Veröffentlichen der Daten ist nur in anonymisierter Form oder mit Einwilligung der Betroffenen erlaubt.

Grundlagen: § 15 LDSG

Technische Hinweise:

- Verwendete Datenverarbeitungssysteme sind im Verfahrensverzeichnis zu dokumentieren, das vom zuständigen Datenschutzbeauftragten geführt wird (hier: der Landesdatenschutzbeauftragte). Hierbei ist darzulegen, welche personenbezogenen Daten (Art der Einzelmerkmale, Kreis

der Betroffenen) in welchem Verfahren mit Hilfe welcher automatisierter Verfahren (welche Hard- und Software incl. der Vernetzung verwendet wird) auf welche Weise (und aufgrund welcher Rechtsgrundlage sowie zu welchem Zweck) verarbeitet werden und welche Datenschutzmaßnahmen (insbesondere zur Datensicherung) die verantwortliche Stelle dabei getroffen hat. Es ist außerdem aufzuführen, wer als Empfänger der Daten vorgesehen ist, welche Fristen für Löschung bzw. Sperrung vorgesehen sind und wer zugriffsberechtigt ist (siehe auch Datenschutzerklärungsmuster in der Anlage).

4.3 Beispiele aus Technik und Verwaltung

4.3.1 Einrichtung neuer bzw. Änderung vorhandener Hard- und Software

Situationsbeschreibung:

In einer Abteilung soll neue Hard- oder Software eingerichtet werden, mit der personenbezogene Daten automatisiert verarbeitet werden sollen, bzw. wird vorhandene Hard- und Software hierzu geändert.

Verantwortliche Stelle ist die Abteilung.

Uneingeschränkt geltende Grundsätze zum datenschutzgerechten Umgang:

1. Grundsätze der Datenverarbeitung:
- Der Zweck, zu dem personenbezogene Daten verarbeitet werden sollen, ist konkret festzulegen.
- Die erhobenen Daten müssen für den Zweck geeignet und erforderlich sein.
- Bei der Datenverarbeitung ist darauf zu achten, dass möglichst wenig personenbezogene Daten verarbeitet werden.

2. Einfluss der Einwilligung:
- Ohne Einwilligung des Betroffenen dürfen personenbezogene Daten nur auf der Grundlage einer ausdrücklichen Rechtsvorschrift (Gesetz, Verordnung) verarbeitet werden.
- Mit Einwilligung des Betroffenen (siehe hierzu auch das entsprechende Formblatt in der Anlage) dürfen personenbezogene Daten nur im Rahmen der getroffenen Vereinbarungen (und natürlich unter Einhaltung gesetzlicher Vorschriften) verwendet werden.
- Eine Einwilligung von Betroffenen erfordert, dass der Betroffene über die beabsichtigte Datenverarbeitung (incl. der Benennung der verantwortlichen Stelle, Art und Weise der

Datenverarbeitung, dem Kreis der Zugangsberechtigten und dem Zeitpunkt der Löschung), deren Zweck und etwaige Empfänger der Daten aufgeklärt wird. Außerdem ist er über seine Rechte auf Auskunft über gespeicherte Daten, auf Berichtigung, Löschung bzw. Sperrung unrichtiger oder unzulässiger bzw. nicht mehr erforderlicher Daten und auf sein Recht zur Anrufung des zuständigen Datenschutzbeauftragten hinzuweisen. Die Einwilligung muss schriftlich erklärt werden, um wirksam werden zu können.

Fallspezifische Grundsätze zum datenschutzgerechten Umgang:

- entfallen für dieses Beispiel.

Erheben

Eine gesonderte Erhebung von Daten findet in diesem Falle nicht statt.

Grundlagen: §§ 13 und 14 LDSG

Bearbeiten

Eine gesonderte Verarbeitung von Daten findet in diesem Falle höchstens im Rahmen eines Funktionstests statt. Danach gelten die jeweiligen spezifischen Regelungen.

Grundlagen: §§ 15 bis 25 LDSG

Veröffentlichen

Eine gesonderte Veröffentlichung von Daten findet in diesem Falle nicht statt.

Grundlagen: § 15 LDSG

Technische Hinweise:

- Vor Einführung eines automatisierten Abrufverfahrens (Kennzeichen ist die programmgesteuerte Datenverarbeitung) ist der zuständige Datenschutzbeauftragte (hier: der Landesdatenschutzbeauftragte) zu informieren und eine Vorabkontrolle durchzuführen. Dabei ist sicherzustellen, dass durch das zum Einsatz kommende System keine besonderen Gefahren für das Persönlichkeitsrecht bestehen. In diesem Zusammenhang ist eine fristgerechte Löschung der gespeicherten Daten sicherzustellen und zu verhindern, dass Unbefugte Daten lesen können.
- Verwendete Datenverarbeitungssysteme sind im Verfahrensverzeichnis zu dokumentieren, das vom zuständigen Daten-

schutzbeauftragten geführt wird (hier: der Landesdatenschutzbeauftragte). Hierbei ist darzulegen, welche personenbezogenen Daten (Art der Einzelmerkmale, Kreis der Betroffenen) in welchem Verfahren mit Hilfe welcher automatisierter Verfahren (welche Hard- und Software incl. der Vernetzung verwendet wird) auf welche Weise (und aufgrund welcher Rechtsgrundlage sowie zu welchem Zweck) verarbeitet werden und welche Datenschutzmaßnahmen (insbesondere zur Datensicherung) die verantwortliche Stelle dabei getroffen hat. Es ist außerdem aufzuführen, wer als Empfänger der Daten vorgesehen ist, welche Fristen für Löschung bzw. Sperrung vorgesehen sind und wer zugriffsberechtigt ist (siehe auch Datenschutzerklärungsmuster in der Anlage).

- Es ist darauf zu achten, dass nur geeignete Systemkomponenten zum Einsatz kommen, mit denen insbesondere die nötigten Datensicherungsmaßnahmen ergriffen werden können, und nur die zur konkreten Aufgabenerfüllung erforderliche Hard- und Software installiert wird. Ferner ist sicherzustellen, dass in Ein- und Ausgabemasken nur solche Daten eingegeben bzw. ausgegeben werden können, die für die konkrete Aufgabe benötigt werden, und praxisgerechte Löschungsfunktionen eingebaut sind. Es sollte zumindest angezeigt werden können, welche Benutzer Zugriffsrechte haben, und eine vollständige und aussagekräftige Dokumentation der miteinander interagierenden Komponenten geben.

4.3.2 Umgang mit Personaldaten

Situationsbeschreibung

In einer Abteilung werden zahlreiche Personen beschäftigt.

Verantwortliche Stelle ist die Abteilung in Zusammenarbeit mit der Abteilung für Personalangelegenheiten.

Uneingeschränkt geltende Grundsätze zum datenschutzgerechten Umgang:

1. Grundsätze der Datenverarbeitung:

- Der Zweck, zu dem personenbezogene Daten verarbeitet werden sollen, ist konkret festzulegen.
- Die erhobenen Daten müssen für den Zweck geeignet und erforderlich sein.
- Bei der Datenverarbeitung ist darauf zu achten, dass möglichst wenig personenbezogene Daten verarbeitet werden.

2. Einfluss der Einwilligung:
- Ohne Einwilligung des Betroffenen dürfen personenbezogene Daten nur auf der Grundlage einer ausdrücklichen Rechtsvorschrift (Gesetz, Verordnung) verarbeitet werden.
- Mit Einwilligung des Betroffenen (siehe hierzu auch das entsprechende Formblatt in der Anlage) dürfen personenbezogene Daten nur im Rahmen der getroffenen Vereinbarungen (und natürlich unter Einhaltung gesetzlicher Vorschriften) verwendet werden.
- Eine Einwilligung von Betroffenen erfordert, dass der Betroffene über die beabsichtigte Datenverarbeitung (incl. der Benennung der verantwortlichen Stelle, Art und Weise der Datenverarbeitung, dem Kreis der Zugangsberechtigten und dem Zeitpunkt der Löschung), deren Zweck und etwaige Empfänger der Daten aufgeklärt wird. Außerdem ist er über seine Rechte auf Auskunft über gespeicherte Daten, auf Berichtigung, Löschung bzw. Sperrung unrichtiger oder unzulässiger bzw. nicht mehr erforderlicher Daten und auf sein Recht zur Anrufung des zuständigen Datenschutzbeauftragten hinzuweisen. Die Einwilligung muss schriftlich erklärt werden, um wirksam werden zu können.

Fallspezifische Grundsätze zum datenschutzgerechten Umgang:

- Beschäftigte sind bei der erstmaligen Speicherung ihrer personenbezogenen Daten umfassend darüber zu informieren, welche Daten gespeichert wurden (Datenspiegel).
- Verarbeitungsformen automatisierter Personalverwaltungsverfahren sind zu dokumentieren und einschließlich des jeweiligen Verwendungszweckes sowie der regelmäßigen Empfänger (incl. des Inhalts automatisierter Datenübermittlung) allgemein bekannt zu geben.

Erheben

Personenbezogene Daten über Bewerber, Beschäftigte, ehemalige Beschäftigte und Hinterbliebene dürfen nur erhoben werden, soweit dies für das Dienstverhältnis oder Zwecken der Personalplanung bzw. Personalwirtschaft erforderlich ist oder eine Rechtsvorschrift dies ausdrücklich erlaubt.

Fragebögen zur Erhebung personenbezogener Daten bedürfen der Genehmigung durch die oberste Dienstbehörde, sofern diese nicht durch eine Verwaltungsvorschrift des Ministeriums bereits festgelegt sind.

In Personalakten dürfen nur Unterlagen aufgenommen werden, die mit dem Dienstverhältnis des Betroffenen in einem unmittelbaren inneren Zusammen-

hang stehen.

Grundlagen: §§ 113 bis 113f LBG i.V.m. § 36 LDSG sowie §§ 13 und 14 LDSG

Bearbeiten

Personaldaten dürfen nur für Zwecke der Personalverwaltung bzw. Personalwirtschaft verarbeitet werden, es sei denn, der Betroffene willigt in eine anderweitige Verwendung ein.

Beschäftigungsdaten sind regelmäßig an die Sozialträger zu übermitteln. Die Beschäftigten sind einmal pro Jahr über diese Übermittlung zu unterrichten.

Bewerbungsunterlagen von nicht beschäftigten Personen sind den Betroffenen unverzüglich zurückzusenden und innerhalb eines Jahres zu löschen, sofern der Betroffene nicht einer weiteren Verarbeitung zugestimmt hatte oder ein anhängiger Rechtsstreit noch nicht abgeschlossen ist.

Personalakten sind fünf Jahre nach ihrem Abschluss (Emeritierung, Pension, Rente, Tod, Entfallen von Versorgungsverpflichtungen) aufzubewahren.

Versorgungsakten sind zehn Jahre nach der letzten Versorgungszahlung aufzubewahren, sofern nicht die Möglichkeit des Wiederauflebens des Anspruchs besteht.

Werden Personalakten nicht vom zuständigen Archiv übernommen, sind sie zu vernichten.

Grundlagen: §§ 113 bis 113f LBG i.V.m. § 36 LDSG sowie §§ 15 bis 25 LDSG und § 3 DEÜV

Veröffentlichen

Von Professoren, Hochschul- und Privatdozenten, Mitarbeitern des wissenschaftlichen Dienstes, Lehrbeauftragten, Lehrkräften für besondere Aufgaben sowie sonstigen Mitarbeitern, die herausgehobene Funktionen in der Universität wahrnehmen, dürfen Name, Amts-, Dienst- und Funktionsbezeichnung, Telefon- und Telefaxnummern sowie E-Mail- und Internet-Adressen veröffentlicht werden, sofern die Betroffenen kein höher zu bewertendes schutzwürdiges Interesse geltend machen können.

Grundlagen: § 125a UG i.V.m. § 15 LDSG

Technische Hinweise:

- Verwendete Datenverarbeitungssysteme sind im Verfahrensverzeichnis zu dokumentieren, das vom zuständigen Datenschutzbeauftragten geführt wird (hier: der Landesdatenschutzbeauftragte). Hierbei ist darzulegen, welche personenbezogenen Daten (Art der Einzelmerkmale, Kreis der Betroffenen) in welchem Verfahren mit Hilfe welcher automatisierter Verfahren (welche Hard- und Software incl. der Vernetzung verwendet wird) auf welche Weise (und aufgrund welcher Rechtsgrundlage sowie zu welchem Zweck) verarbeitet werden und welche Datenschutzmaßnahmen (insbesondere zur Datensicherung) die verantwortliche Stelle dabei getroffen hat. Es ist außerdem aufzuführen, wer als Empfänger der Daten vorgesehen ist, welche Fristen für Löschung bzw. Sperrung vorgesehen sind und wer zugriffsberechtigt ist (siehe auch Datenschutzerklärungsmuster in der Anlage).

5. Zusammenfassung

Das zentrale Thema für die Informatik ist der Umgang mit Informationen. Sofern es sich dabei um personenbezogene Daten handelt, müssen die Vorschriften des Datenschutzes beachtet werden. Die vorliegende Arbeit liefert einen Überblick darüber, welche Datenschutz-Vorschriften unter welchen Voraussetzungen an den baden-württembergischen Universitäten einzuhalten sind.

Ausgehend vom für diesen Bereich grundlegenden Volkszählungsurteil des Bundesverfassungsgerichts werden die Grundsätze des Datenschutzrechts herausgearbeitet: Jede Person darf grundsätzlich selbst über die Preisgabe und Verwendung ihrer persönlichen Daten bestimmen. Ein Eingriff in dieses Grundrecht auf informationelle Selbstbestimmung erfordert eine gesetzliche Grundlage, wobei der Verwendungszweck bereichsspezifisch und präzise zu bestimmen ist (Normenklarheit), die Angaben personenbezogener Daten für den Zweck geeignet und erforderlich sein müssen (Verhältnismäßigkeit) und nur so viele Daten zu erheben und zu speichern sind, wie unbedingt benötigt werden (Datensparsamkeit).

Anzuwenden ist stets nach dem Sitzprinzip das für die verantwortliche Stelle geltende Recht. Dabei hat bereichsspezifisches Recht Vorrang vor dem Landesdatenschutzgesetz, das für die Landes-Universitäten im Regelfall anzuwenden ist, und dieses wiederum vor dem Bundesdatenschutzgesetz bzw. der EG-Datenschutz-Richtlinie.

Personenbezogene Daten sind in erster Linie beim Betroffenen selbst zu erheben und zur Verarbeitung von diesen ist dessen ausdrückliche Einwilligung erforderlich. Dabei ist das persönliche Auskunftsrecht des Betroffenen zu beachten. Auch die Veröffentlichung personenbezogener Daten stellt ein besonders schwerer Eingriff in das Grundrecht der Betroffenen dar, da bereits veröffentlichte Daten auch ohne Einwilligungserklärung weiterverarbeitet werden dürfen.

Die Grundrechte auf informationelle Selbstbestimmung und Wissenschaftsfreiheit und ihre Interaktion werden ausgehend vom Hochschulurteil des Bundesverfassungsgerichts beschrieben. Auf dieser Grundlage wurden vom Gesetzgeber Bereichsregelungen (wie Forschungsklauseln, Bestimmungen zur Erhebung von Studierendendaten und zur Evaluation) beschlossen.

In den zentralen Gebieten des universitären Alltags wie Forschung, Lehre, Technik und Verwaltung werden die entsprechenden Datenschutzbestimmungen aufgeführt und anhand der relevanten Datenflüsse beschrieben, welche Umgangsweisen kritische Bereiche jeweils erfordern.

Für Daten zu wissenschaftlichen Zwecken existieren eine Reihe Sonderregelungen, die einem Forscher (im Gegensatz zu anderen Nutzern) mehr Möglichkeiten

zur Verarbeitung einräumen. Bei den Studierendendaten hat die Verwaltung weitgehende Rechte, bei einer Veröffentlichung sind jedoch enge Grenzen gesetzt. Bei der Evaluation ist die Erhebung weit reichend, doch auch hier dürfen nur im Ausnahmefall mehr als anonyme Daten veröffentlicht werden. Bei technischen Anwendungen stehen Maßnahmen zur Datensicherheit im Vordergrund. Die Verarbeitung und Veröffentlichung von Personaldaten unterliegt im Bereich der Universitäten den stärksten Restriktionen.

Für diese Bereiche wird anhand ausgewählter Fallbeispiele ausgeführt, wie sich die verantwortliche Stelle jeweils datenschutz-konform zu verhalten hat.

Anhang

1. Glossar

Adressmittlungsverfahren: Verfahren zur Datenerhebung, bei dem die Erhebungsunterlagen an die Betroffenen über einen Dritten verschickt werden, der alleine über den Zugang zu den nötigen personenbezogenen Daten verfügt

Akte: Unterlage zu amtlichen oder dienstlichen Zwecken, die keine Datei und nicht Bestandteil eines offiziellen Vorgangs ist

Amtsgeheimnis: Mit der Ausübung der Tätigkeit in einem Amt verbundene Verschwiegenheitsverpflichtung (z.B. Statistikgeheimnis, Sozialgeheimnis, Steuergeheimnis)

Anonymisierung: Verändern personenbezogener Daten derart, dass ein Personenbezug nicht mehr herstellbar ist

Auftragsdatenverarbeitung: Datenverarbeitung einer Stelle, die Daten im Auftrag einer anderen Stelle, der verantwortlichen Stelle, und zu deren Bestimmungen verarbeitet

Automatisiertes Abrufverfahren: Übermittlung von Daten durch automatisierte Abfrage

Automatisierte Datenverarbeitung: Programmgesteuerte Durchführung einer elektronischen Datenverarbeitung

Bereichsrecht: Recht, das für einen bestimmten Bereich gilt (und, sofern darin Datenschutzbestimmungen enthalten sind, Vorrang vor dem LDSG hat); siehe auch Auflistung in [Bergmann2002], S. 1 – 53 im Teil I, Ziffer 4.2 und 4.3

Berufsgeheimnis: Mit der Ausübung eines Berufes verbundene Verschwiegenheitsverpflichtung (z.B. für Ärzte, Notare, Sozialarbeiter)

Betroffene: Natürliche Person, deren personenbezogene Daten verarbeitet werden

Chipkarte: Mobiler Datenträger, der zum Erkennen einer Person, dem Erhalt einer Leistung oder für einen anderen Zweck verwendet wird und auf dem Daten gespeichert sind, die automatisiert verarbeitet werden können

Datei: Sammlung von Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden können oder gleichartig aufgebaut sind und

nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden können

Datengeheimnis: Mit der Ausübung einer Beschäftigung verbundene Verschwiegenheitsverpflichtung, im Rahmen der Beschäftigung angesammelte Kenntnisse über Daten zu keiner Zeit unbefugt zu verarbeiten

Datenschutz: Schutz vor unzulässiger Verarbeitung personenbezogener Daten

Datenschutzaudit: Überprüfung der Darstellung des Datenschutzkonzepts einer verantwortlichen Stelle durch unabhängige und dafür zugelassene Gutachter

Datenschutzbeauftragter: Person, die mit der Kontrolle der Einhaltung des Datenschutzes beauftragt wurde

Datenschutzerklärung: Freiwillige Selbstverpflichtung einer verantwortlichen Stelle, wie mit personenbezogenen Daten umgegangen wird

Datensicherheit: Maßnahmen zum Schutz der Daten vor Fehlern, Missbrauch und höherer Gewalt

Datensparsamkeit: Grundsatz, nur so viele Daten zu erheben, wie unbedingt benötigt werden

Datentreuhänder: Mit einer besonderen Schweigepflicht ausgestattete Stelle (siehe z.B. unter Berufsgeheimnis), die eine Auswertung von personenbezogenen Daten im Auftrag einer anderen Stelle vornimmt

Digitale Signatur: Elektronisches Pendant zur Unterschrift und der zweifelsfreien Authentifizierung

Einwilligungserklärung: Freiwillig und schriftlich abgegebene Erklärung des Betroffenen, mit der Verarbeitung seiner Daten einverstanden zu sein

Elektronische Signatur: siehe Digitale Signatur

Empfänger von Daten: Nicht betroffene Person oder Stelle, die Daten übermittelt bekommt

Erheben von Daten: Beschaffen von Daten über Betroffene

Evaluation: Bewertung eines Ist-Zustandes anhand vordefinierter Kriterien

Faktische Anonymisierung: Verändern personenbezogener Daten derart, dass ein Personenbezug nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft herstellbar ist

Forschungsklausel: Gesetzliche Regelung zur Forschung, die Vorrang vor Datenschutzbestimmungen hat

Gesetzesvorbehalt: Notwendigkeit einer gesetzlichen Regelung zum Eingriff in Rechte von Betroffenen

Hochschulautonomie: Recht einer Hochschule, sich selbst verwalten und hierzu Satzungen erlassen zu dürfen

Informationelle Selbstbestimmung: Recht einer Person, grundsätzlich selbst über die Preisgabe und Verwendung ihrer persönlichen Daten zu bestimmen

Internet: Weltweit miteinander verbundenes Informationsnetz

Intranet: Das in der Regel durch eine Firewall geschützte, nur lokal miteinander verbundene Informationsnetz

Kryptographie: Wissenschaft der Ver- und Entschlüsselung von Daten

Leistungsnachweis: Studienfortschrittsnachweis eines Studierenden, eine Lehrveranstaltung erfolgreich bestanden zu haben

Löschen von Daten: Unkenntlichmachen bzw. Vernichten gespeicherter Daten

Normenklarheit: Grundsatz der präzisen Bestimmung der Anwendung von Normen (Rechtsvorschriften); beim Datenschutz: Präzise und bereichsspezifische Bestimmung des Verwendungszwecks

Nutzen von Daten: Verwendung von Daten innerhalb der verarbeitenden Stelle

Öffentliche Verwaltung: Staatliche Verwaltung des Bundes, Landes, der Gemeinden oder Gemeindeverbände

Personenbezogene Daten: Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person

Primärdaten: Unmittelbar gewonnene Daten durch Beobachtung oder Befragung

Protokolldaten: Daten, die anfallen, wenn ein bestimmter elektronischer Dienst in Anspruch genommen wird, und aus Gründen der Nachvollziehbarkeit gespeichert werden

Prüfungsleistung: Studienfortschrittsnachweis eines Studierenden, den Inhalt einer Lehreinheit unter Prüfungsbedingungen darstellen zu können

Pseudonymisierung: Ersetzen des Namens und anderer eindeutigen Identifikationsmerkmale durch ein Kennzeichen

Rechtsvorschrift: Gesetz, Verordnung, Erlass bzw. Verfügung öffentlich-rechtlicher Institutionen auf der Grundlage eines Gesetzes

Speichern von Daten: Erfassen, Aufnehmen oder Aufbewahren von Daten auf Datenträgern

Sperren von Daten: Einschränken der weiteren Verarbeitung von Daten auf ausdrücklich erlaubte Nutzungsvorschriften

Übermitteln von Daten: Weitergabe von Daten an Dritte bzw. Ermöglichen der Einsichtnahme oder des Abrufs der Daten durch Dritte

Verantwortliche Stelle: Stelle, die Daten für sich selbst verarbeitet oder durch andere im Auftrag verarbeiten lässt und für die Verarbeitung datenschutzrechtlich verantwortlich ist

Verarbeiten von Daten: Sammelbezeichnung für Erheben, Speichern, Verändern, Übermitteln, Nutzen, Sperren und Löschen von Daten

Verändern von Daten: Inhaltliches Umgestalten gespeicherter Daten

Verfahrensverzeichnis: Verzeichnis, in dem alle automatisierten Verfahren ausführlich dokumentiert sind

Verhältnismäßigkeit: Grundsatz der zielkonformen und auf das Erforderliche beschränkten Vorgehensweise; beim Datenschutz: für den Zweck geeignete und erforderliche Angabe personenbezogener Daten

Veröffentlichen von Daten: Das der Allgemeinheit zugänglich machende Nutzen von Daten

Verordnung: Auf gesetzlicher Grundlage erlaubte Rechtsvorschrift eines Ministeriums zur näheren Ausführung gesetzlicher Vorschriften

Verschlüsselung: Verbergen des Originals durch Anwendung datenverändernder Algorithmen

Vorabkontrolle: Überprüfung der Übereinstimmung des Datenschutzkonzepts mit Datenschutzbestimmungen bei besonders sensiblen Eingriffen in das informationelle Selbstbestimmungsrecht

Wissenschaftlicher Zweck: Eindeutige Festlegung des Zwecks für Forschungsvorhaben, um mit den Daten flexibler umgehen zu können

Wissenschaftsfreiheit: im Grundgesetz verankerte Gewährleistung der unabhängigen Ausübung von Wissenschaft

Zweck: Grund zur und Ziel der Datenverarbeitung

2. Akronym- und Abkürzungsverzeichnis

BAföG: Bundesausbildungsförderungsgesetz

BDSG: Bundesdatenschutzgesetz

BfD: Bundesbeauftragter für den Datenschutz

BGB: Bürgerliches Gesetzbuch

BKGG: Bundeskindergeldgesetz

BSHG: Bundessozialhilfegesetz

BVerfG: Bundesverfassungsgericht

DEÜV: Datenerfassungs- und -übermittelungsverordnung

DES: Data Encryption Standard (offengelegter symmetrischer Verschlüsselungsstandard)

DAS: Digital Signature Algorithm (Public-Key-basierter Signaturmechanismus)

GG: Grundgesetz

EDV: Elektronische Datenverarbeitung

EG: Europäische Gemeinschaft; inzwischen: Europäische Union

i.d.F.: in der Fassung

i.V.m.: in Verbindung mit; Verknüpfung mehrerer Rechtsnormen

HISCOB: Programmpaket der Hochschul-Informations-System GmbH: Controlling-Baustein (zur Kosten- und Leistungsrechnung)

HISMBS: Programmpaket der Hochschul-Informations-System GmbH: Mittel-Bewirtschaftungs-System

HISPOS: Programmpaket der Hochschul-Informations-System GmbH: Prüfungs-Operations-System

HISSOS: Programmpaket der Hochschul-Informations-System GmbH: Studenten-Operations-System

HISQIS: Programmpaket der Hochschul-Informations-System GmbH: für Qualitätssteigerung der Hochschulverwaltung im Internet durch Selbstbedienung

HISSVA: Programmpaket der Hochschul-Informations-System GmbH: Stellenverwaltungsabwicklungssystem

HISZUL: Programmpaket der Hochschul-Informations-System GmbH: Zulassungssystem

HRG: Hochschulrahmengesetz

HVVO: Hochschulvergabeverordnung

HZG: Hochschulzulassungsgesetz

ISO/IEC: International Organisation for Standardization / International Electrotechnical Commission; internationaler Sicherheitsstandard für Informationstechnologien

LAN: Local Area Network (Lokales Netzwerk)

LBG: Landesbeamtengesetz

LDSG: Landesdatenschutzgesetz

LfD: Landesbeauftragter für den Datenschutz

NC: Numerus Clausus (Zulassungsbeschränkung)

PolG: Polizeigesetz

Rn: Randnummer

RSA: asymmetrisches Public-Key-Kryptosystem nach Rivest, Shamir und Adleman

SGB: Sozialgesetzbuch

SigG: Signaturgesetz

UG: Universitätsgesetz

UrhG: Urheberrechtsgesetz

WLAN: Wireless LAN (Funknetzwerk)

WoGG: Wohngeldgesetz

ZVS: Zentralstelle für die Vergabe von Studienplätzen

3. Literaturverzeichnis

[AKT1998]: Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder: Datenschutzfreundliche Technologien, Schwerin, CLUB WIEN und cw Obotritendruck, 1998.

[Bergmann2002]: Lutz Bergmann, Roland Möhrle und Armin Herb: Datenschutzrecht – Kommentar, Loseblattsammlung in 3 Bänden, Stuttgart, Richard Boorberg Verlag, 2002, Stand: Februar 2002.

[Bethge2000]: Herbert Bethge: Wissenschaftsrecht, in: Norbert von Achterberg, Günter Püttner und Thomas Würtenberger (Hrsg.): Besonderes Verwaltungsrecht – ein Lehr- und Handbuch, 2. Auflage, Heidelberg, C. F. Müller Verlag, 2000, Band 1, S. 1042 – 1123.

[Bizer1992]: Johann Bizer: Forschungsfreiheit und Informationelle Selbstbestimmung, Nomos Universitätsschriften Recht Band 85, Baden-Baden, Nomos Verlagsgesellschaft, 1992.

[Bizer2001]: Johann Bizer: Datenschutzgerechte Gestaltung des technischen Urheberschutzes, in: Datenschutz und Datensicherheit 12/2001, S. 726 – 733.

[Blömer2002]: Wilhelm Marcus Blömer und Flemming Moos: Datenschutz und Datensicherheit, in: Bert Kaminski, Thomas Henßler, Helge F. Kolaschnik und Anastasia Papathoma-Baetge (Hrsg.): Rechtshandbuch E-Business, Neuwied, Hermann Luchterhand Verlag, 2002, S. 199 – 245.

[Bochnik1996]: Hans Joachim Bochnik: Bestehen Datenschützer auf Forschungsblockaden?, in: MedizinRecht 6/1996, S. 262 – 264.

[Böhringer2002]: Ingo Böhringer: Die Novellierung des „Hochschullehrerprivilegs“ (§ 42 ArbnErfG), in: Neue Juristische Wochenschrift 13/2002, S. 952 – 954.

[Brennecke2001]: Harald Brennecke und Peter Breschendorf: Datenschutzrecht – Eine Einführung in das Bundesdatenschutzrecht nach dem BDSG 05/2001, Karlsruhe, Brennecke & Lechler, 2001.

[DFG1998]: Internationale Kommission der Deutschen Forschungsgemeinschaft: Ehrenkodex für gutes wissenschaftliches Verhalten, Auszug aus der Pressemitteilung Nr. 31 der Deutschen Forschungsgemeinschaft vom 16.12.1997, in: Neue Juristische Wochenschrift 24/1998, S. 1764 – 1765.

[Dornseif2002]: Maximilian Dornseif, Kay H. Schumann und Christian Klein: Tatsächliche und rechtliche Risiken drahtloser Computernetzwerke, in: Datenschutz und Datensicherheit 4/2002, S. 226 – 230.

[Fumy2000]: Walter Fumy: Von Common Criteria bis zu elliptischen Kurven – Sicherheitsstandards von ISO/IEC JTC 1/SC27, in: Datenschutz und Datensicherheit 7/2000, S. 385 – 391.

[Gerling2001]: Rainer W. Gerling, Cordula Langer und Ray Roßmann: Rechtsgrundlagen zur Rasterfahndung, in: Datenschutz und Datensicherheit 12/2001, S. 746 – 749.

[Gola2002]: Peter Gola und Christoph Klug: Die Entwicklung des Datenschutzrechts in den Jahren 2001/2002, in: Neue Juristische Wochenschrift 34/2002, S. 2431 – 2441.

[Hage1996]: Natalija el Hage: Lehrevaluation und studentische Veranstaltungskritik, herausgegeben vom Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie, Bonn, Richard Thierbach Verlag, 1996.

[Hailbronner2002]: Kay Hailbronner und Max-Emanuel Geis (Hrsg.): Kommentar zum Hochschulrahmengesetz (HRG), Loseblattsammlung in 2 Bänden, Heidelberg, C. F. Müller Verlag, 2002, Stand: Juni 2002.

[Hamm1999]: Rainer Hamm und Klaus Peter Möller (Hrsg.): Datenschutz und Forschung, Forum Datenschutz Band 7, Baden-Baden, Nomos Verlagsgesellschaft, 1999.

[Haug2001]: Volker Haug: Die Rechtsstellung der Studierenden, in: Volker Haug (Hrsg.): Das Hochschulrecht in Baden-Württemberg, Heidelberg, C. F. Müller Verlag, 2001, S. 277 – 316.

[Herberger2001]: Klaus Herberger: Die neuen Steuerungsinstrumente, in: Volker Haug (Hrsg.): Das Hochschulrecht in Baden-Württemberg, Heidelberg, C. F. Müller Verlag, 2001, S. 190 – 203.

[Homma1996]: Birgit Homma und Hanns Ullrich: Urheber-, Patent- und Arbeitnehmererfindungsrecht, in: Christian Flämig et al. (Hrsg.): Handbuch des Wissenschaftsrechts, 2. Auflage, Berlin, Springer-Verlag, 1996, Band 2, S. 1559 – 1590.

[HRK2000]: Hochschulrektorenkonferenz: Wegweiser 2000 durch die Qualitätssicherung in Lehre und Studium, Dokumente & Informationen 2/2000, Bonn, 2000.

[Jendro2000]: Frank Jendro: Evaluation und Datenschutz, in: Hochschul rektorenkonferenz: Im Aufbruch – Evaluation an Hochschulen, Beiträge zur Hochschulpolitik 9/2000, Bonn, 2000, S. 27 – 29.

[Kilian1998]: Wolfgang Kilian: Medizinische Forschung und Datenschutzrecht, in: Neue Juristische Wochenschrift 12/1998, S. 787 – 791.

[Kilian2002]: Wolfgang Kilian und Benno Heussen (Hrsg): Computerrechts-Handbuch, Loseblattsammlung, München, Verlag C. H. Beck, 2002, Stand: März 2002.

[Kimminich1996a]: Otto Kimminich: Hochschule im Grundrechtssystem, in: Christian Flämig et al. (Hrsg.): Handbuch des Wissenschaftsrechts, 2. Auflage, Berlin, Springer-Verlag, 1996, Band 1, S. 121 – 156.

[Kimminich1996b]: Otto Kimminich: Die Rechtsgestalt der Hochschulen, in: Christian Flämig et al. (Hrsg.): Handbuch des Wissenschaftsrechts, 2. Auflage, Berlin, Springer-Verlag, 1996, Band 1, S. 227 – 235.

[Knemeyer1996]: Franz-Ludwig Knemeyer: Hochschulautonomie / Hochschulselbstverwaltung, in: Christian Flämig et al. (Hrsg.): Handbuch des Wissenschaftsrechts, 2. Auflage, Berlin, Springer-Verlag, 1996, Band 1, S. 237 – 257.

[Köstlin1996]: Thomas Köstlin: Wissenschaftsfördernde Stiftungen, in: Christian Flämig et al. (Hrsg.): Handbuch des Wissenschaftsrechts, 2. Auflage, Berlin, Springer-Verlag, 1996, Band 2, S. 1417 – 1440.

[Krüger1996a]: Hartmut Krüger: Hochschule in der bundesstaatlichen Verfassungsordnung, in: Christian Flämig et al. (Hrsg.): Handbuch des Wissenschaftsrechts, 2. Auflage, Berlin, Springer-Verlag, 1996, Band 1, S. 157 – 187.

[Krüger1996b]: Hartmut Krüger: Forschung, in: Christian Flämig et al. (Hrsg.): Handbuch des Wissenschaftsrechts, 2. Auflage, Berlin, Springer-Verlag, 1996, Band 1, S. 261 – 308.

[LDSB1994]: Dr. Ruth Leuze: 15. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz in Baden-Württemberg, Stuttgart, 1994.

[LDSB2000]: Werner Schneider: 21. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg, Stuttgart, 2000.

[LDSB2001]: Werner Schneider: 22. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg, Stuttgart, 2001.

[LfD2000]: Hinweise des Landesbeauftragten für den Datenschutz Baden-Württemberg zum neuen Landesdatenschutzgesetz, Stuttgart, 2000.

[Metschke2000]: Rainer Metschke und Rita Wellbrock: Datenschutz in Wissenschaft und Forschung, Materialien zum Datenschutz Nr. 28, 2. Auflage, Berlin, Verwaltungsdruckerei Berlin, 2000.

[Oppermann1996]: Thomas Oppermann: Selbstverwaltung und staatliche Verwaltung, in: Christian Flämig et al. (Hrsg.): Handbuch des Wissenschaftsrechts, 2. Auflage, Berlin, Springer-Verlag, 1996, Band 1, S. 1009 – 1038.

[Simitis1998]: Spiros Simitis: Datenschutz – Rückschritt oder Neubeginn?, in: Neue Juristische Wochenschrift 34/1998, S. 2473 – 2479.

[Sokol1997]: Bettina Sokol, Landesbeauftragte für den Datenschutz Nordrhein-Westfalen: Chipkarten für Studierende – bequeme Welt oder gläserne Studierende?, in: Datenschutz Nachrichten 4/1997, S. 14; Auszug aus dem 13. Datenschutzbericht 1995/96, Ziffer 15.1, Seite 102f.

[Tinnefeld1994]: Marie-Theres Tinnefeld und Eugen Ehmann: Einführung in das Datenschutzrecht, 2. Auflage, München, R. Oldenbourg Verlag, 1994.

[Tinnefeld2001]: Marie-Theres Tinnefeld: Evaluation der Lehrenden – eine Fata-Data Morgana?, in: Datenschutz und Datensicherheit 1/2001, S. 21 – 26.

[Rechnungshof1994]: Rechnungshof Baden-Württemberg: Untersuchung der Organisationsstrukturen der zentralen Verwaltungen der Universitäten in Baden-Württemberg – Abschlussbericht, Stuttgart, September 1994.

[Reuke2001]: Hermann Reuke: Zum Verhältnis von Evaluation und Akkreditierung im Rahmen der ZEvA, in: Hochschulrektorenkonferenz: Internationalisierung = Evaluation + Akkreditierung?, Beiträge zur Hochschulpolitik 8/2001, Bonn, 2001, S. 33 – 40.

[Roellecke1996]: Gerd Roellecke: Geschichte des deutschen Hochschulwesens, in: Christian Flämig et al. (Hrsg.): Handbuch des Wissenschaftsrechts, 2. Auflage, Berlin, Springer-Verlag, 1996, Band 1, S. 3 – 36.

[Ullmann2001]: Markus Ullmann, Frank Koob und Harald Kelter: Anonyme Online-Wahlen – Lösungsansätze für die Realisierung von Online-Wahlen, in: Datenschutz und Datensicherheit 11/2001, S. 643 – 647.

[Wagner1999]: Wissenschaft schützt die Öffentlichkeit vor schlechten statistischen Ergebnissen, in: Datenschutz und Datensicherheit 23/1999, S. 377 – 383.

[Weichert1996]: Thilo Weichert: Datenschutz und medizinische Forschung – Was nützt ein „medizinisches Forschungsgeheimnis“?, in: MedizinRecht 6/1996, S. 258 – 261.

[Weichert1997]: Thilo Weichert: Datenschutz behindert Forschung?, in: Datenschutz Nachrichten 4/1997, S. 4 – 8.

[Wesel1992]: Uwe Wesel: Fast alles, was Recht ist – Jura für Nichtjuristen, 4. Auflage, Frankfurt am Main, Eichborn Verlag, 1992.

[Wiedmann2001]: Thomas Wiedmann: Rechtsgrundlagen für die Hochschulen in Baden-Württemberg, in: Volker Haug (Hrsg.): Das Hochschulrecht in Baden-Württemberg, Heidelberg, C. F. Müller Verlag, 2001, S. 11 – 42.

4. Verzeichnis grundlegender Rechtsbestimmungen

4.1 Maßgebliche Verfassungen

- Grundgesetz für die Bundesrepublik Deutschland i.d.F. v. 26.11.2001
- Verfassung des Landes Baden-Württemberg i.d.F. v. 09.06.2000

4.2 Grundlegende Gesetze

- Bundesdatenschutzgesetz (BDSG) i.d.F. v. 03.12.2001
- Gesetz über die Universitäten im Lande Baden-Württemberg (Universitätsgesetz – UG) i.d.F. v. 01.02.2000
- Gesetz über die Zulassung zum Hochschulstudium in Baden-Württemberg (Hochschulzulassungsgesetz – HZG) i.d.F. v. 06.12.1999
- Gesetz zum Schutz personenbezogener Daten (Landesdatenschutzgesetz – LDSG) i.d.F. v. 18.09.2000
- Hochschulrahmengesetz (HRG) i.d.F. v. 08.08.2002
- Landesbeamtengesetz (LBG) i.d.F. v. 19.12.2000
- Polizeigesetz (PolG) i.d.F. v. 13.01.1992
- Staatsvertrag über die Vergabe von Studienplätzen (ZVS-StV) i.d.F. v. 24.06.1999 (Anlage zum HZG)
- Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz (SGB X) i.d.F. v. 21.08.2002

4.3 Grundlegende Verordnungen

- Verordnung des Kultusministeriums zur Durchführung der Wahlen an den Universitäten i.d.F. v. 14.12.1977
- Verordnung des Wissenschaftsministeriums über die Vergabe von Studienplätzen in zulassungsbeschränkten Studiengängen durch die Hochschulen (Hochschulvergabeverordnung – HVVO) i.d.F. v. 12.04.2000
- Verordnung des Wissenschaftsministeriums zur Erhebung und Verarbeitung personenbezogener Daten der Studienbewerber, Studierenden und Prüfungskandidaten für Verwaltungszwecke der Hochschulen (Hochschul-Datenschutzverordnung) i.d.F. v. 27.09.1999
- Verordnung über die Erfassung und Übermittlung von Daten für die Träger der Sozialversicherung (Datenerfassungs- und –übermittlungsverordnung – DEÜV) i.d.F. v. 10.02.1998

4.4 Zitierte Vereinbarungen

- Rahmen-Dienstvereinbarung über Einführung, Einsatz und Ausbau der Informations- und Kommunikationstechnik in den Universitäten des Landes Baden-Württemberg (IuKR-DV) i.d.F. v. 16.12.1999

5. Verzeichnis grundlegender Urteile

[Achelpöhler2002]: Beschluss des OLG Düsseldorf zur Rasterfahndung II vom 08.02.2002 (3 Wx 357/01), veröffentlicht in: Datenschutz und Datensicherheit 4/2002, S. 244 – 245.

BVerfGE 35, 79: Entscheidungen des Bundesverfassungsgerichts: Urteil vom 29.05.1973 zur Mitbestimmung an Hochschulen (1 BvR 424/71 und 325/72), in: Band 35, Nr. 10, S. 79 – 170.

BVerfGE 65, 1: Entscheidungen des Bundesverfassungsgerichts: Urteil vom 15.12.1983 zum Volkszählungsgesetz 1983 (1 BvR 209, 269, 362, 420, 440, 484/83), in: Band 65, Nr. 1, S. 1 – 71.

BVerwGE 102, 304: Entscheidungen des Bundesverwaltungsgerichts: Urteil vom 11.12.1996 über die Überprüfung von Forschungstätigkeiten von Hochschullehrern (6 C 5.95), in: Band 102, Nr. 43, S. 304 – 316.

[OLG-Hamm1998]: Beschluss des OLG Hamm über die Akteneinsicht für Habilitationsschrift vom 28.11.1995 (1 Vas 38/94), veröffentlicht in: Datenschutz und Datensicherheit 22/1998, S. 107 – 109.

[Wiese2000]: M. Wiese: Rückruf einer Dissertation nach Ablieferung der Pflichtexemplare, Urteil des OLG Celle vom 01.12.1999 (13 U 69/99), in: Neue Juristische Wochenschrift 21/2000, S. 1579 – 1580.

[Zimmerling1998]: W. Zimmerling: Anmeldung zur Diplomprüfung über das Internet, Beschluss des VG Saarlouis vom 23.07.1998 (1 F 73/98), in: Neue Juristische Wochenschrift 43/1998, S. 3221 – 3222.

6. Verzeichnis verwendeter Web-Quellen

(Stand: 10.12.2002)

http://www.baden-wuerttemberg.datenschutz.de/material-lfd/internet.html

http://www.baden-wuerttemberg.datenschutz.de/material-lfd/passwort.html

http://www.baden-wuerttemberg.datenschutz.de/material-lfd/pcln.html

http://www.baden-wuerttemberg.datenschutz.de/material-lfd/verfahrensverzeichnis.html

http://www.datenschutz.hessen.de/o-hilfen/chipkart.htm

http://www.datenschutz.hessen.de/o-hilfen/evaluation.htm

http://www.datenschutz.hessen.de/tb26/k16p2.htm

http://www.his.de/Abt1/HISQIS/einfstand.pdf

http://www.informatik.uni-ulm.de/JusoHSG/chipkarten.htm

http://www.informatik.uni-ulm.de/JusoHSG/evaluation.htm

7. Gesetzesauszüge zum Datenschutz

7.1 Landesdatenschutzgesetz (LDSG)

§ 1 Aufgabe des Gesetzes

Aufgabe dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch die Verarbeitung seiner personenbezogenen Daten durch öffentliche Stellen in seinem Persönlichkeitsrecht beeinträchtigt wird.

§ 2 Anwendungsbereich

(1) Die Vorschriften dieses Gesetzes – ausgenommen des Sechsten Abschnitts – gelten für die Verarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen des Landes, der Gemeinden und Gemeindeverbände sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts (öffentliche Stellen).

(5) Soweit besondere Rechtsvorschriften des Bundes oder des Landes auf personenbezogene Daten anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten und von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

§ 3 Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Verarbeiten ist das Erheben, Speichern, Verändern, Übermitteln, Nutzen, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Erheben das Beschaffen von personenbezogenen Daten über den Betroffenen,
2. Speichern das Erfassen, Aufnehmen oder Aufbewahren von personenbezogenen Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung,
3. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
4. Übermitteln das Bekanntgeben personenbezogener Daten an einen Dritten in der Weise, dass
   a) die Daten an den Dritten weitergegeben werden oder
   b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,
5. Nutzen jede sonstige Verwendung personenbezogener Daten innerhalb der Daten verarbeitenden Stelle,
6. Sperren die Einschränkung der weiteren Verarbeitung personenbezogener Daten,
7. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(3) Verantwortliche Stelle ist jede Stelle, die personenbezogene Daten für sich selbst verarbeitet oder durch andere im Auftrag verarbeiten lässt.

(4) Empfänger ist jede Person oder Stelle, die Daten erhält, mit Ausnahme des Betroffenen.

(5) Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle, ausgenommen der Betroffene sowie diejenige Person und Stelle, die in einem Mitgliedstaat der Europäischen Union personenbezogene Daten im Auftrag verarbeitet.

(6) Anonymisieren ist das Verändern personenbezogener Daten in der Weise, dass Einzelangaben über persönliche und 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.

(7) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

(8) Automatisiert ist eine Datenverarbeitung, wenn sie durch Einsatz eines elektronischen Datenverarbeitungssystems programmgesteuert durchgeführt wird.

(9) Eine Datei ist
1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei) oder
2. eine sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht-automatisierte Datei).

(10) Eine Akte ist jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage. Nicht hierunter fallen Entwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

§ 4 Zulässigkeit der Datenverarbeitung

(1) Die Verarbeitung personenbezogener Daten ist nur zulässig,
1. wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder
2. soweit der Betroffene eingewilligt hat.

(2) Wird die Einwilligung beim Betroffenen eingeholt, ist er über die beabsichtigte Datenverarbeitung und den Zweck der Verarbeitung aufzuklären. Die Aufklärungspflicht umfasst bei einer beabsichtigten Übermittlung auch den Empfänger der Daten. Über die Möglichkeit einer weitergehenden Datenverarbeitung auf Grund gesetzlicher Bestimmungen ist er zu unterrichten. Der Betroffene ist unter Darlegung der Folgen darauf hinzuweisen, dass er die Einwilligung verweigern kann und dass die Möglichkeit besteht, die Einwilligung zu widerrufen.

(3) Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.

(4) Die Einwilligung kann auch elektronisch erklärt werden, wenn die empfangende Stelle sicherstellt, dass

1. die Einwilligung nur durch eine eindeutige und bewusste Handlung des Einwilligenden erfolgen kann,
2. sie nicht unerkennbar verändert werden kann,
3. ihr Urheber eindeutig erkannt werden kann und
4. die Einwilligung (Tag, Uhrzeit, Inhalt) protokolliert wird.

(5) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 3 Satz 1 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 2, die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, und die Erteilung der Einwilligung schriftlich festzuhalten.

(6) Der Betroffene hat das Recht, gegenüber der Verarbeitung seiner Daten, auch wenn diese rechtmäßig ist, ein schutzwürdiges, in seiner persönlichen Situation begründetes Interesse einzuwenden (Einwendungsrecht). Die Verarbeitung ist in diesem Fall nur zulässig, wenn eine Abwägung ergeben hat, dass sein Interesse hinter dem öffentlichen Interesse an der Verarbeitung zurückzustehen hat. Das Ergebnis der Abwägung ist ihm unter Angabe der Gründe mitzuteilen. Sätze 1 bis 3 finden keine Anwendung in den in § 33 Abs. 3 genannten Fällen.

(7) Entscheidungen, die für den Betroffenen eine nachteilige rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht auf eine Bewertung seiner Persönlichkeitsmerkmale gestützt werden, die ausschließlich im Wege einer automatisierten Verarbeitung seiner personenbezogenen Daten zu Stande gekommen ist.

§ 5 Rechte des Betroffenen

(1) Der Betroffene hat nach Maßgabe dieses Gesetzes ein Recht auf
1. Auskunft über die zu seiner Person gespeicherten Daten (§ 21),
2. Berichtigung, Löschung und Sperrung der zu seiner Person gespeicherten Daten (§§ 22 bis 24),
3. Auskunft aus dem Verfahrensverzeichnis (§ 11 Abs. 4),
4. Einwendung eines schutzwürdigen, in seiner persönlichen Situation begründeten Interesses gegenüber der Verarbeitung seiner Daten (§ 4 Abs. 6),
5. Schadensersatz (§ 25),
6. Anrufung des Landesbeauftragten für den Datenschutz (§ 27).

Diese Rechte können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(2) Wird für den Erhalt einer Leistung, das Erkennen einer Person oder für einen anderen Zweck ein Datenträger herausgegeben, den der Inhaber mit sich führen kann und auf dem seine personenbezogenen Daten automatisiert verarbeitet werden, hat die verantwortliche Stelle sicherzustellen, dass er dies erkennen und seine ihm nach Absatz 1 Nr. 1 bis 6 zustehenden Rechte ohne unvertretbaren Aufwand geltend machen kann. Der Inhaber ist bei Ausgabe des Datenträgers über die ihm nach Absatz 1 zustehenden Rechte sowie über die von ihm bei Verlust des Datenträgers zu treffenden Maßnahmen und über die Folgen aufzuklären.

§ 6 Datengeheimnis

Den bei öffentlichen Stellen beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten oder sonst zu verwenden (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 7 Verarbeitung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag öffentlicher Stellen durch andere Personen oder Stellen verarbeitet, bleibt der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in § 5 Abs. 1 Satz 1 Nr. 1 bis 5 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftraggeber hat den Auftragnehmer sorgfältig auszuwählen. Dabei ist besonders zu berücksichtigen, ob der Auftragnehmer ausreichend Gewähr dafür bietet, dass er die für eine datenschutzgerechte Datenverarbeitung erforderlichen technischen und organisatorischen Maßnahmen zu treffen in der Lage ist. Der Auftrag ist schriftlich zu erteilen. Dabei sind insbesondere Gegenstand und Umfang der Datenverarbeitung, die notwendigen technischen und organisatorischen Maßnahmen, etwaige Unterauftragsverhältnisse sowie die Befugnis des Auftraggebers festzulegen, dass er hinsichtlich der Verarbeitung personenbezogener Daten dem Auftragnehmer Weisungen erteilen darf. Der Auftrag kann auch durch die Fachaufsichtsbehörde mit Wirkung für ihrer Aufsicht unterliegende Stellen des Landes erteilt werden; diese sind von der Auftragserteilung zu unterrichten. Der Auftraggeber hat sich von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen durch den Auftragnehmer zu überzeugen.

(3) Ist der Auftragnehmer eine öffentliche Stelle, gelten für ihn nur die §§ 6, 9, 10, 27 bis 31, 40 und 41. Die Verarbeitung personenbezogener Daten ist nur im Rahmen des Auftrags und der Weisungen zulässig. Ist der Auftragnehmer der Ansicht, dass der Auftrag, einzelne Bestimmungen des Auftrags oder eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstoßen, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(5) Werden Wartungsarbeiten und vergleichbare Hilfstätigkeiten bei der Datenverarbeitung durch Stellen oder Personen außerhalb der verantwortlichen Stelle erbracht, gilt dies als Datenverarbeitung im Auftrag.

§ 8 Automatisiertes Abrufverfahren

(1) Ein automatisiertes Verfahren, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, darf nur eingerichtet werden, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist.

(2) Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen

1. Anlass und Zweck des Abrufverfahrens,
2. Dritte, an die übermittelt wird,
3. Art der abzurufenden Daten,
4. nach § 9 erforderliche technische und organisatorische Maßnahmen.

Die erforderlichen Festlegungen können auch durch die Fachaufsichtsbehörde mit Wirkung für ihrer Aufsicht unterliegende Stellen des Landes getroffen werden.

(3) Die Zulässigkeit des einzelnen Abrufs beurteilt sich nach den für die Erhebung und Übermittlung geltenden Vorschriften. Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Dritte, an den übermittelt wird. Die speichernde Stelle prüft die Zulässigkeit des Abrufs nur, wenn dazu Anlass besteht. Die speichernde Stelle hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann.

(4) Für die Einrichtung oder wesentliche Änderung eines automatisierten Verfahrens, das den Abruf personenbezogener Daten nur innerhalb einer öffentlichen Stelle ermöglicht, gelten die Absätze 1 und 2 entsprechend, wenn die Daten für einen anderen Zweck als den, für den sie gespeichert worden sind, genutzt werden sollen; dabei ist eine angemessene Abrufkontrolle zu gewährleisten.

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf aus Datenbeständen, die jedermann ohne oder nach besonderer Zulassung zur Benutzung offen stehen oder deren Veröffentlichung zulässig wäre.

§ 9 Technische und organisatorische Maßnahmen

(1) Die Gestaltung und Auswahl der technischen Einrichtungen und der Verfahren zur automatisierten Verarbeitung personenbezogener Daten hat sich an dem Grundsatz auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu verarbeiten.

(2) Öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine den Vorschriften dieses Gesetzes entsprechende Datenverarbeitung zu gewährleisten. Erforderlich sind Maßnahmen, wenn ihr Aufwand, insbesondere unter Berücksichtigung der Art der zu schützenden personenbezogenen Daten, in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

(3) Werden personenbezogene Daten automatisiert verarbeitet, sind je nach Art und Verwendung der zu schützenden personenbezogenen Daten und unter Berücksichtigung des Standes der Technik Maßnahmen zu treffen, die geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),
3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten zu verhindern (Speicherkontrolle),
4. zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle),

5. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),
6. zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Übermittlungskontrolle),
7. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
8. zu gewährleisten, dass Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
9. zu gewährleisten, dass bei der Übertragung von Daten sowie beim Transport von Datenträgern die Daten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),
10. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle), und
11. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

(3) Die Landesregierung wird ermächtigt, die in Absatz 2 genannten Anforderungen nach dem jeweiligen Stand der Technik und Organisation durch Rechtsverordnung fortzuschreiben.

(4) Werden personenbezogene Daten in nicht-automatisierten Dateien oder in Akten verarbeitet, sind insbesondere Maßnahmen zu treffen, um zu verhindern, dass Unbefugte bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung auf die Daten zugreifen können.

§ 10 Behördlicher Datenschutzbeauftragter

(1) Öffentliche Stellen können einen behördlichen Datenschutzbeauftragten bestellen. Die Bestellung bedarf der Schriftform.

(2) Bestellt werden darf nur, wer die zur Erfüllung seiner Aufgaben erforderliche Sachkunde und Zuverlässigkeit besitzt und durch die Bestellung keinem Interessenkonflikt ausgesetzt wird. Die öffentliche Stelle kann einen Bediensteten ihrer Aufsichtsbehörde mit deren Zustimmung zum Beauftragten für den Datenschutz bestellen. Mehrere Stellen können gemeinsam einen Datenschutzbeauftragten bestellen.

(3) Der behördliche Datenschutzbeauftragte ist bei der Erfüllung seiner Aufgaben der Behördenleitung unmittelbar zu unterstellen. Er ist bei der Erfüllung seiner Aufgaben weisungsfrei und darf deswegen nicht benachteiligt werden.

(4) Der behördliche Datenschutzbeauftragte hat die Aufgabe, die öffentliche Stelle bei der Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu unterstützen. Zu seinen Aufgaben gehört es insbesondere,
1. auf die Einhaltung der Datenschutzvorschriften bei der Planung, Einführung und Anwendung von Verfahren, mit denen personenbezogene Daten automatisiert verarbeitet werden, hinzuwirken,

2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz und den besonderen Erfordernissen des Datenschutzes in ihrem Tätigkeitsbereich vertraut zu machen sowie
3. das Verfahrensverzeichnis (§ 11) zu führen.
Der behördliche Datenschutzbeauftragte ist vor dem Einsatz oder der wesentlichen Änderung eines automatisierten Verfahrens rechtzeitig zu unterrichten.

§ 11 Verfahrensverzeichnis

(1) Jede öffentliche Stelle führt ein Verzeichnis der automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden (Verfahrensverzeichnis). Das Verzeichnis kann auch von einer Stelle für andere Stellen geführt werden.

(2) In das Verfahrensverzeichnis sind einzutragen:
1. Name und Anschrift der verantwortlichen Stelle,
2. die Bezeichnung des Verfahrens,
3. die Zweckbestimmung und die Rechtsgrundlage der Verarbeitung,
4. die Art der gespeicherten Daten,
5. der Kreis der Betroffenen,
6. die Empfänger der Daten oder Gruppen von Empfängern sowie die jeweiligen Datenarten, wenn vorgesehen ist,
a) die Daten zu übermitteln,
b) sie innerhalb der öffentlichen Stelle für einen weiteren Zweck zu nutzen oder
c) sie im Auftrag verarbeiten zu lassen,
7. die Fristen für die Prüfung der Sperrung und Löschung der Daten oder für die Sperrung und Löschung,
8. die zugriffsberechtigten Personengruppen oder Personen, die allein zugriffsberechtigt sind,
9. eine allgemeine Beschreibung der eingesetzten Hardware, der Vernetzung und der Software und
10. die technischen und organisatorischen Maßnahmen nach § 9.

(3) Absatz 1 gilt nicht für Verfahren, deren einziger Zweck das Führen eines Registers ist, das zur Information der Öffentlichkeit bestimmt ist und allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, sowie für Verfahren, die allgemeinen Verwaltungszwecken dienen, insbesondere Verfahren der Textverarbeitung.

(4) Die öffentliche Stelle macht die Angaben nach Absatz 2 Nr. 1 bis 7 des Verfahrensverzeichnisses auf Antrag jedermann in geeigneter Weise verfügbar. Satz 1 findet keine Anwendung auf Verfahren des Landesamtes für Verfassungsschutz.

§ 12 Vorabkontrolle

Wer für den Einsatz oder die wesentliche Änderung eines automatisierten Verfahrens zur Verarbeitung personenbezogener Daten zuständig ist, das mit besonderen Gefahren für das Persönlichkeitsrecht verbunden sein kann, insbesondere auf Grund der Art oder der Zweckbestimmung der Verarbeitung, darf das Verfahren erst einsetzen, wenn sichergestellt ist, dass diese Gefahren nicht bestehen oder durch technische oder organisatorische Maßnahmen verhindert werden;

dies gilt insbesondere für die Einrichtung eines automatisierten Abrufverfahrens nach § 8, für automatisierte Verfahren, mit denen Daten nach § 33 verarbeitet werden, und für die Herausgabe von Datenträgern nach § 5 Abs. 2. Das Ergebnis der Untersuchung und dessen Begründung sind aufzuzeichnen und dem behördlichen Datenschutzbeauftragten oder, wenn ein solcher nicht bestellt ist, dem Landesbeauftragten für den Datenschutz zur Prüfung zuzuleiten. Der behördliche Datenschutzbeauftragte wendet sich in Zweifelsfällen an den Landesbeauftragten für den Datenschutz.

§ 13 Erhebung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist.

(2) Personenbezogene Daten, die nicht aus allgemein zugänglichen Quellen entnommen werden, sind beim Betroffenen mit seiner Kenntnis zu erheben. Werden Daten nicht über eine bestimmte Person, sondern über einen bestimmten Personenkreis, etwa durch Videoüberwachung, erhoben, muss der Betroffene die seinen schutzwürdigen Belangen angemessene Möglichkeit zur Kenntnisnahme erhalten.

(3) Personenbezogene Daten dürfen beim Betroffenen ohne seine Kenntnis nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
2. die zu erfüllende Aufgabe ihrer Art nach eine solche Erhebung erforderlich macht und keine Anhaltspunkte dafür vorliegen, dass ihr überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) Bei Dritten dürfen personenbezogene Daten nur erhoben werden, wenn

1. einer der in § 15 Abs. 2 Nr. 1 bis 6 genannten Fälle vorliegt oder
2. die zu erfüllende Aufgabe ihrer Art nach eine solche Erhebung erforderlich macht und keine Anhaltspunkte dafür vorliegen, dass ihr überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

§ 14 Unterrichtung bei der Erhebung

(1) Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, sind ihm gegenüber anzugeben:

1. die beabsichtigte Datenverarbeitung und der Zweck der Verarbeitung sowie
2. bei einer beabsichtigten Übermittlung auch die Empfänger der Daten oder Gruppen von Empfängern, soweit der Betroffene nach den Umständen des Einzelfalls nicht mit der Übermittlung an diese rechnen muss.

Werden die Daten auf Grund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Über die der Auskunftspflicht zu Grunde liegende Rechtsvorschrift und die Folgen der Verweigerung von Angaben ist der Betroffene bei Verwendung eines Erhebungsvordrucks stets, sonst nur auf Verlangen aufzuklären. Bei Verwendung eines Erhebungsvordrucks ist der Betroffene auch auf das Bestehen von Auskunfts- und Berichtigungsrechten hinzuweisen.

(2) Werden Daten beim Betroffenen ohne seine Kenntnis oder bei Dritten erhoben, ist der Betroffene entsprechend Absatz 1 Satz 1 zu benachrichtigen, wenn die Daten in einer Datei gespeichert werden. Bei schriftlicher Benachrichtigung ist der Betroffene auch auf das Bestehen von Auskunfts- und Berichtigungsrechten hinzuweisen. Die Benachrichtigung erfolgt zum Zeitpunkt der Speicherung oder im Fall einer beabsichtigten Übermittlung spätestens bei der ersten Übermittlung. Sätze 1 bis 3 finden keine Anwendung auf Verfahren des Landesamtes für Verfassungsschutz.

(3) Eine Pflicht zur Benachrichtigung besteht in den Fällen des Absatzes 2 nicht, wenn

1. die Verarbeitung der Daten durch Gesetz ausdrücklich vorgesehen ist,
2. der Betroffene auf andere Weise Kenntnis von der Verarbeitung seiner Daten erlangt,
3. die Benachrichtigung des Betroffenen einen unverhältnismäßigen Aufwand erfordern würde,
4. die Benachrichtigung die ordnungsgemäße Erfüllung von Aufgaben der Gefahrenabwehr oder von Aufgaben der Finanzverwaltung im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung oder die Verfolgung von Straftaten oder Ordnungswidrigkeiten gefährden würde,
5. die Benachrichtigung die Sicherheit des Bundes oder eines Landes gefährden würde,
6. die Daten oder die Tatsache ihrer Speicherung zum Schutze des Betroffenen oder zum Schutze der Rechte Dritter geheim gehalten werden müssen und deshalb das Interesse des Betroffenen an der Benachrichtigung zurücktreten muss oder
7. die Daten ausschließlich für Zwecke der wissenschaftlichen Forschung oder der Statistik verarbeitet werden.

(4) Werden personenbezogene Daten bei einem Dritten außerhalb des öffentlichen Bereichs erhoben, so ist er auf Verlangen auf den Erhebungszweck hinzuweisen, soweit dadurch schutzwürdige Interessen des Betroffenen nicht beeinträchtigt werden. Werden die Daten auf Grund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, so ist er auf die Auskunftspflicht, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Über die der Auskunftspflicht zu Grunde liegende Rechtsvorschrift und die Folgen der Verweigerung von Angaben ist er bei Verwendung eines Erhebungsvordrucks stets, sonst nur auf Verlangen aufzuklären.

§ 15 Speicherung, Veränderung und Nutzung

(1) Das Speichern, Verändern und Nutzen personenbezogener Daten ist zulässig, wenn es

1. zur Erfüllung der Aufgaben der öffentlichen Stelle erforderlich ist und
2. für Zwecke erfolgt, für die die Daten erhoben worden sind; ist keine Erhebung vorausgegangen, dürfen die Daten nur für Zwecke genutzt werden, für die sie erstmals gespeichert worden sind.

(2) Das Speichern, Verändern und Nutzen personenbezogener Daten für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. der Betroffene eingewilligt hat oder offensichtlich ist, dass dies im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er seine Einwilligung hierzu verweigern würde,
3. der Betroffene einer durch Rechtsvorschrift festgelegten Auskunftspflicht nicht nachgekommen und über die beabsichtigte Datenverarbeitung unterrichtet worden ist,
4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
5. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist,
6. die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, es sei denn, dass überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen,
7. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen, oder
8. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuches oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist.

(3) Eine Speicherung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung, der Durchführung von Organisationsuntersuchungen, der Prüfung und Wartung von automatisierten Verfahren der Datenverarbeitung sowie statistischen Zwecken oder Zwecken der Durchführung eigener wissenschaftlicher Forschung der speichernden Stelle dient. Dies gilt auch für die Speicherung und Nutzung zu Ausbildungs- und Prüfungszwecken, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) Personenbezogene Daten, die ausschließlich zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für Zweck und hiermit in Zusammenhang stehende Maßnahmen gegenüber Bediensteten genutzt werden.

(5) Sind mit personenbezogenen Daten, die nach Absatz 1 bis 3 gespeichert werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, so ist die Speicherung auch dieser Daten zulässig, soweit nicht schutzwürdige Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen. Unter denselben Voraussetzungen dürfen die für die Aufgabenerfüllung nicht erforderlichen Daten innerhalb der speichernden Stelle weitergegeben werden; eine darüber hinausgehende Nutzung dieser Daten ist unzulässig.

§ 16 Übermittlung an Stellen innerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an Stellen innerhalb des öffentlichen Bereichs ist zulässig, wenn
1. zur Erfüllung der Aufgaben der übermittelnden Stelle oder der Stelle, an die die Daten übermittelt werden, erforderlich ist und
2. für Zwecke erfolgt, für die eine Nutzung nach § 15 Abs. 1 bis 4 zulässig wäre.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen einer öffentlichen Stelle im Geltungsbereich des Grundgesetzes, trägt diese die Verantwortung. In diesem Fall prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben der ersuchenden Stelle liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht. § 8 Abs. 3 Satz 2 und 3 bleibt unberührt.

(3) Die Stelle, an die die Daten übermittelt werden, darf sie nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihr übermittelt worden sind. Eine Verarbeitung für andere Zwecke ist nur unter den Voraussetzungen des § 15 Abs. 2 zulässig.

(4) Auf die Übermittlung verbundener Daten findet § 15 Abs. 5 entsprechende Anwendung.

§ 18 Übermittlung an Stellen außerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs ist zulässig, wenn
1. sie zur Erfüllung der Aufgaben der übermittelnden Stelle erforderlich ist und für Zwecke erfolgt, für die eine Nutzung nach § 15 Abs. 1 bis 4 zulässig wäre, oder
2. der Dritte, an den die Daten übermittelt werden sollen, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse am Ausschluss der Übermittlung hat.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(3) In den Fällen der Übermittlung nach Absatz 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten, insbesondere über den Dritten, an den die Daten übermittelt werden, und den Zweck der Übermittlung. Dies gilt nicht, wenn die Unterrichtung einen unverhältnismäßigen Aufwand erfordern würde, der Betroffene von der Übermittlung auf andere Weise Kenntnis erlangt, die Unterrichtung wegen der Art der personenbezogenen Daten unter Berücksichtigung der schutzwürdigen Interessen des Betroffenen nicht geboten erscheint oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.

(4) Die Stelle, an die die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihr übermittelt worden sind. Die übermittelnde Stelle hat sie in den Fällen des Absatzes 1 Nr. 2 hierauf hinzuweisen. Eine Verarbeitung für andere Zwecke ist nur zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle eingewilligt hat.

(5) Die übermittelnde Stelle soll die Übermittlung mit Auflagen versehen, die den Datenschutz bei dem Dritten, an den die Daten übermittelt werden, sicherstellen, oder mit dem Dritten Vereinbarungen zur Gewährleistung des Datenschutzes treffen.

§ 19 Übermittlung für Zwecke der wissenschaftlichen Forschung

(1) Die Übermittlung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung an Stellen innerhalb des öffentlichen Bereichs ist zulässig, wenn dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen am Ausschluss der Übermittlung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Kann der Zweck der Forschung auch mit anonymisierten Daten erreicht werden und steht der verantwortlichen Stelle nicht ausreichend Personal für eine Anonymisierung der Daten zur Verfügung, können die mit der Durchführung des Forschungsvorhabens befassten Personen diese Aufgabe für die verantwortliche Stelle unter deren Aufsicht wahrnehmen. Die betreffenden Personen sind zuvor nach dem Verpflichtungsgesetz zu verpflichten.

(2) Für die Übermittlung personenbezogener Daten an Stellen außerhalb des öffentlichen Bereichs gilt Absatz 1 mit der Maßgabe, dass die Übermittlung nur zulässig ist, wenn sich die Stelle verpflichtet, die übermittelten Daten nicht für andere Zwecke zu verarbeiten und die Bestimmungen des § 35 Abs. 2 und 3 einzuhalten.

§ 20 Übermittlung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes

(1) Für die Übermittlung personenbezogener Daten in Mitgliedstaaten der Europäischen Union sowie für die Übermittlung an Organe und Einrichtungen der Europäischen Gemeinschaft gelten §§ 16, 18 und 19 entsprechend.

(2) Die Übermittlung personenbezogener Daten in Staaten außerhalb der Europäischen Union oder an über- oder zwischenstaatliche Stellen ist unter den Voraussetzungen der §§ 18 und 19 zulässig, soweit in den folgenden Absätzen nichts anderes bestimmt ist.

(3) Die Übermittlung unterbleibt, soweit

1. Grund zu der Annahme besteht, dass durch sie gegen den Zweck eines deutschen Gesetzes verstoßen würde, oder
2. der Betroffene ein überwiegendes schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn in dem Staat außerhalb der Europäischen Union oder bei der über- oder zwischenstaatlichen Stelle ein angemessenes Datenschutzniveau nicht gewährleistet ist.

Die Angemessenheit des Datenschutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die bei Datenübermittlungen von Bedeutung sind; insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den Empfänger geltenden Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden.

(4) Ist in dem Staat, in den die Daten übermittelt werden sollen, kein angemessenes Datenschutzniveau gewährleistet, ist die Übermittlung nur zulässig, wenn
1. der Betroffene eingewilligt hat,
2. die Übermittlung für die Wahrung eines überwiegenden öffentlichen Interesses oder zur Geltendmachung rechtlicher Ansprüche vor Gericht einschließlich eines Vorverfahrens erforderlich ist,
3. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder
4. die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist und allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

(5) Ist in dem Staat, in den die Daten übermittelt werden sollen, kein angemessenes Datenschutzniveau gewährleistet, ist unbeschadet des Absatzes 4 eine Übermittlung auch zulässig, wenn die Person oder Stelle, an die die Daten übermittelt werden sollen, ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist; diese Garantien können sich auch aus Vertragsklauseln ergeben.

§ 21 Auskunft

(1) Dem Betroffenen ist von der speichernden Stelle auf Antrag unentgeltlich Auskunft zu erteilen über
1. die zu seiner Person gespeicherten Daten,
2. den Zweck der Verarbeitung,
3. die Herkunft der Daten, soweit diese gespeichert oder sonst bekannt ist, und die Empfänger oder Gruppen von Empfängern, an die die Daten übermittelt werden sollen, sowie
4. den strukturierten Ablauf der automatisierten Verarbeitung der ihn betreffenden Daten in den Fällen des § 4 Abs. 7 und die dabei herangezogenen Entscheidungskriterien.

Dies gilt nicht für personenbezogene Daten, die ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind.

(2) In dem Antrag soll die Art der personenbezogenen Daten näher bezeichnet werden, über die Auskunft erteilt werden soll. Sind die personenbezogenen Daten in Akten gespeichert, wird Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht.

(3) Die speichernde Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen. Sind die Daten in Akten gespeichert, ist dem Betroffenen auf Verlangen Akteneinsicht zu gewähren; Absatz 2 Satz 2 findet entsprechende Anwendung. Ein Recht auf Akteneinsicht besteht nicht, wenn die Daten des Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich

ist. In diesem Fall ist dem Betroffenen Auskunft zu erteilen. Rechtsvorschriften über die Akteneinsicht im Verwaltungsverfahren bleiben unberührt.

(4) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Behörden der Staatsanwaltschaften, an Polizeidienststellen, Verfassungsschutzbehörden und Behörden der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, ist sie nur mit Zustimmung dieser oder der nach Absatz 7 zuständigen Stelle zulässig. Satz 1 findet auch Anwendung auf die Übermittlung personenbezogener Daten an den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministers der Verteidigung. Für die Versagung der Zustimmung gelten die Absätze 5 und 6 entsprechend.

(5) Die Auskunftserteilung unterbleibt, soweit
1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder
3. die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen überwiegender berechtigter Interessen eines Dritten, geheim gehalten werden müssen
und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(6) Die Ablehnung der Auskunftserteilung bedarf keiner Begründung, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er den Landesbeauftragten für den Datenschutz anrufen kann.

(7) Die fachlich zuständige oberste Landesbehörde kann durch Rechtsverordnung bestimmen, dass eine andere als die speichernde Stelle die Auskunft erteilt.

§ 22 Berichtigung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird bei personenbezogenen Daten in Akten festgestellt, dass sie unrichtig sind, oder wird ihre Richtigkeit vom Betroffenen bestritten, so ist dies in der Akte zu vermerken oder auf sonstige Weise festzuhalten.

(2) Von der Berichtigung unrichtiger Daten sind die Empfänger der Daten zu verständigen, soweit dies zur Wahrung schutzwürdiger Interessen des Betroffenen oder zur Erfüllung der Aufgaben der verantwortlichen Stelle oder des Empfängers erforderlich erscheint; dies gilt nicht, wenn dies einen unverhältnismäßigen Aufwand erfordern würde.

§ 23 Löschung

(1) Personenbezogene Daten in Dateien sind zu löschen, wenn
1. ihre Speicherung unzulässig ist oder

2. ihre Kenntnis für die speichernde Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist.

(2) Personenbezogene Daten in Akten sind zu löschen, wenn die speichernde Stelle im Einzelfall feststellt, dass die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist.

(3) Vor einer Löschung sind die Daten dem zuständigen Archiv nach Maßgabe der §§ 3, 7 und 8 des Landesarchivgesetzes zur Übernahme anzubieten.

(4) Die Löschung unterbleibt, wenn

1. Grund zu der Annahme besteht, dass durch sie schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder

2. sie wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(5) Von einer Löschung unzulässig gespeicherter Daten sind die Empfänger der Daten nach Maßgabe des § 22 Abs. 2 zu verständigen.

§ 24 Sperrung

(1) Personenbezogene Daten in Dateien sind zu sperren, wenn

1. ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt oder

2. in den Fällen des § 23 Abs. 4 eine Löschung unterbleibt.

(2) Personenbezogene Daten in Akten sind zu sperren, wenn die speichernde Stelle im Einzelfall feststellt, dass die Daten unzulässig gespeichert sind. Sie sind ferner zu sperren, wenn die speichernde Stelle im Einzelfall feststellt, dass die Daten zur Aufgabenerfüllung nicht mehr erforderlich sind, eine Löschung nach § 23 Abs. 2 nicht in Betracht kommt und ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden.

(3) Gesperrte personenbezogene Daten sind gesondert aufzubewahren; bei automatisierten Verfahren kann die Sperrung statt dessen auch durch zusätzliche technische Maßnahmen gewährleistet werden. Lassen sich auf Grund der Art der Verarbeitung Maßnahmen nach Satz 1 nicht oder nur mit unverhältnismäßig hohem Aufwand durchführen, sind die Daten mit einem Sperrvermerk zu versehen.

(4) Ohne Einwilligung des Betroffenen dürfen gesperrte personenbezogene Daten nur genutzt oder übermittelt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot, zu Aufsichts- und Kontrollzwecken, zur Rechnungsprüfung oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerlässlich ist und

2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

Personenbezogene Daten, die unzulässig in Akten gespeichert sind, dürfen ohne Einwilligung des Betroffenen nicht mehr genutzt oder übermittelt werden.

(5) Von einer Sperrung unzulässig gespeicherter Daten sind die Empfänger der Daten nach Maßgabe des § 22 Abs. 2 zu verständigen.

§ 25 Schadensersatz

(1) Fügt eine öffentliche Stelle dem Betroffenen durch eine nach den Vorschriften dieses Gesetzes oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Verarbeitung seiner personenbezogenen Daten in oder aus Dateien einen Schaden zu, ist sie dem Betroffenen zum Ersatz des daraus entstehenden Schadens verpflichtet. Dies gilt nicht, wenn die öffentliche Stelle nachweist, dass der Umstand, durch den der Schaden eingetreten ist, nicht von ihr zu vertreten ist.

(2) Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen.

(3) Die Ansprüche nach den Absätzen 1 und 2 sind insgesamt bis zu einem Betrag in Höhe von zweihundertfünfzigtausend Deutsche Mark begrenzt. Ist auf Grund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von zweihundertfünfzigtausend Deutsche Mark übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht.

(4) Sind bei einer Datei mehrere Stellen speicherungsberechtigt und ist der Geschädigte nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.

(5) Mehrere Ersatzpflichtige haften als Gesamtschuldner.

(6) Auf das Mitverschulden des Betroffenen und die Verjährung sind die §§ 254 und 852 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

(7) Vorschriften, nach denen ein Ersatzpflichtiger in weiterem Umfang als nach dieser Vorschrift haftet oder nach denen ein anderer für den Schaden verantwortlich ist, bleiben unberührt.

(8) Der Rechtsweg vor den ordentlichen Gerichten steht offen.

§ 27 Anrufung des Landesbeauftragten für den Datenschutz

(1) Jeder kann sich an den Landesbeauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch eine öffentliche Stelle in seinen Rechten verletzt worden zu sein. Niemand darf benachteiligt oder gemaßregelt werden, weil er von seinem Recht nach Satz 1 Gebrauch gemacht hat.

(2) Wendet sich ein Betroffener an den Landesbeauftragten für den Datenschutz, weil ihm nach § 21 Abs. 5 oder besonderen gesetzlichen Vorschriften keine Auskunft erteilt worden ist, darf die Mitteilung des Landesbeauftragten für den Datenschutz an den Betroffenen keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen, sofern diese oder die nach § 21 Abs. 7 zuständige Stelle nicht einer weitergehenden Auskunft zustimmt. Das Gleiche gilt, wenn ein Betroffener unmittelbar den Landesbeauftragten für den Datenschutz anruft, und die für die Erteilung der Auskunft zuständige Stelle diesem unter Angabe von Gründen darlegt, dass sie bei einem Auskunftsersuchen eine Auskunft nach den in Satz 1 genannten Vorschriften verweigern würde.

§ 28 Kontrolle durch den Landesbeauftragten für den Datenschutz

(1) Der Landesbeauftragte für den Datenschutz kontrolliert bei den öffentlichen Stellen die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz.

(2) Die Kontrolle des Landesbeauftragten für den Datenschutz erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Für personenbezogene Daten in Dateien oder Akten über die Sicherheitsüberprüfung gilt dies jedoch nur, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten nicht widersprochen hat. Die speichernde Stelle hat die Betroffenen im Einzelfall oder in allgemeiner Form auf das Widerspruchsrecht hinzuweisen. Der Widerspruch ist schriftlich gegenüber der speichernden Stelle oder dem Landesbeauftragten für den Datenschutz zu erklären.

(4) Stellt der Landesbeauftragte für den Datenschutz bei seiner Kontrolle einen Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz fest, so ist er befugt, diesen bei den für die Verfolgung oder Ahndung zuständigen Stellen anzuzeigen.

§ 30 Mitteilung des Ergebnisses der Kontrolle, Beanstandungen

(1) Der Landesbeauftragte für den Datenschutz teilt der verantwortlichen Stelle das Ergebnis seiner Kontrolle mit. Damit können Vorschläge zur Verbesserung des Datenschutzes verbunden werden, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung personenbezogener Daten.

(2) Stellt der Landesbeauftragte für den Datenschutz Verstöße gegen Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dies

1. bei den öffentlichen Stellen des Landes gegenüber der zuständigen obersten Landesbehörde,

2. bei den Gemeinden, Gemeindeverbänden und den sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts sowie bei den in § 2 Abs. 2 genannten Stellen gegenüber dem vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden angemessenen Frist auf. In den Fällen des Satzes 1 Nr. 2 unterrichtet der Landesbeauftragte für den Datenschutz gleichzeitig die zuständige Aufsichtsbehörde.

(3) Der Landesbeauftragte für den Datenschutz kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.

(4) Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Landesbeauftragten für den Datenschutz getroffen worden oder beabsichtigt sind. Die in Absatz 2 Satz 1 Nr. 2 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an den Landesbeauftragten für den Datenschutz zu.

§ 32 Meldung an den Landesbeauftragten für den Datenschutz

(1) Die öffentlichen Stellen, die keinen Datenschutzbeauftragten nach § 10 bestellt haben, melden dem Landesbeauftragten für den Datenschutz den Einsatz und die wesentliche Veränderung eines automatisierten Verfahrens. Ausgenommen sind die in § 11 Abs. 3 und 4 Satz 2 genannten Verfahren.

(2) Die meldepflichtigen Stellen haben spätestens gleichzeitig mit der ersten Einspeicherung die Angaben nach § 11 Abs. 2 mitzuteilen.

§ 33 Verarbeitung besonderer Arten personenbezogener Daten

(1) Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben hervorgehen, dürfen nur verarbeitet werden, wenn

1. eine besondere Rechtsvorschrift dies vorsieht,
2. der Betroffene ausdrücklich eingewilligt hat,
3. die Verarbeitung zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist und der Betroffene aus rechtlichen oder tatsächlichen Gründen nicht in der Lage ist, seine Einwilligung zu geben, oder
4. dies zur Geltendmachung rechtlicher Ansprüche vor Gericht einschließlich eines Vorverfahrens erforderlich ist.

(2) Absatz 1 findet keine Anwendung auf die Verarbeitung von Daten über religiöse oder weltanschauliche Überzeugungen nach § 17, von Daten für Zwecke der wissenschaftlichen Forschung nach §§ 19 und 35 und von Daten im Zusammenhang mit Dienst- und Arbeitsverhältnissen nach § 36.

(3) Absatz 1 findet ferner keine Anwendung auf die Verarbeitung personenbezogener Daten

1. zur Gefahrenabwehr,
2. zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuches oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen,
3. durch das Landesamt für Verfassungsschutz,
4. durch die Finanzverwaltung, soweit sie die Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung verarbeitet, und
5. bei einer Sicherheitsüberprüfung nach dem Landessicherheitsüberprüfungsgesetz.

§ 34 Zweckbindung bei der Verarbeitung personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen

(1) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Person oder Stelle in Ausübung ihrer Berufs- oder Amtspflicht zur Verfügung gestellt worden sind, dürfen von der speichernden Stelle nur für den Zweck verarbeitet werden, für den sie sie erhalten hat. § 33 bleibt unberührt. In die Übermittlung an einen

Dritten außerhalb des öffentlichen Bereichs muss die zur Verschwiegenheit verpflichtete Stelle einwilligen.

(2) Für einen anderen Zweck dürfen die Daten nur verarbeitet werden, wenn
1. die Änderung des Zwecks durch besonderes Gesetz zugelassen ist oder
2. die Voraussetzungen vorliegen, die eine Nutzung nach § 15 Abs. 1 bis 4 zulassen würden und die zur Verschwiegenheit verpflichtete Stelle eingewilligt hat.

§ 35 Verarbeitung personenbezogener Daten durch Forschungseinrichtungen

(1) Öffentliche Stellen mit der Aufgabe unabhängiger wissenschaftlicher Forschung dürfen die zur Durchführung wissenschaftlicher Forschung erforderlichen personenbezogenen Daten erheben. Ohne Kenntnis des Betroffenen dürfen die Daten nur erhoben werden, wenn der Zweck des Forschungsvorhabens auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet werden.

(2) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

(3) Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, soweit
1. der Betroffene eingewilligt hat oder
2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist und überwiegende schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(4) Bei der Meldung nach § 32 darf die Beschreibung der Zweckbestimmung der Verarbeitung, zu deren Erfüllung personenbezogene Daten verarbeitet werden, auf die Angabe „Forschungsvorhaben“ beschränkt werden.

§ 36 Datenverarbeitung bei Dienst- und Arbeitsverhältnissen

(1) Personenbezogene Daten von Beschäftigten dürfen nur verarbeitet werden, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher planerischer, organisatorischer, personeller, sozialer oder haushalts- und kostenrechnerischer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienst- oder Betriebsvereinbarung es vorsieht.

(2) Auf die Verarbeitung von Personalaktendaten von Angestellten und Arbeitern sowie Auszubildenden in einem privatrechtlichen Ausbildungsverhältnis finden die für Beamte geltenden Vorschriften der §§ 113 bis 113 g des Landesbeamtengesetzes entsprechende Anwendung, es sei denn, besondere Rechtsvorschriften oder tarifliche Vereinbarungen gehen vor.

(3) Im Zusammenhang mit der Begründung eines Dienst- oder Arbeitsverhältnisses ist die Erhebung personenbezogener Daten eines Bewerbers bei dem bisherigen

Dienstherrn oder Arbeitgeber nur zulässig, wenn der Betroffene eingewilligt hat. Satz 1 gilt entsprechend für die Übermittlung personenbezogener Daten an künftige Dienstherrn oder Arbeitgeber. Steht fest, dass ein Dienst- oder Arbeitsverhältnis nicht zu Stande kommt, sind dem Betroffenen die von ihm vorgelegten Unterlagen unverzüglich zurückzusenden und die zu ihm gespeicherten Daten spätestens nach Ablauf eines Jahres zu löschen, es sei denn, er hat in die weitere Verarbeitung eingewilligt oder diese ist wegen eines anhängigen Rechtsstreits erforderlich.

7.2 Universitätsgesetz (UG)

§ 4a Bewertung der Forschung, Lehre, Förderung des wissenschaftlichen Nachwuchses und der Gleichberechtigung von Frauen und Männern

(1) Die Universitäten berichten regelmäßig über ihre Tätigkeit in Forschung und Lehre. Sie unterrichten die Öffentlichkeit über die Erfüllung ihrer Aufgaben.

(2) Die Arbeit der Universitäten in Forschung und Lehre, bei der Förderung des wissenschaftlichen Nachwuchses sowie bei der Durchsetzung der Gleichberechtigung von Frauen und Männern soll durch Eigen- und Fremdevaluation regelmäßig bewertet werden. Die Studierenden sind bei der Bewertung der Qualität der Lehre zu beteiligen. Die Ergebnisse der Bewertungen sollen veröffentlicht werden. § 25 Abs. 4 Satz 6 bis 9 und § 125 a Abs. 4 bleiben unberührt.

(3) Zur Wahrnehmung ihrer Aufgaben nach Absatz 1 und 2 dürfen die Universitäten die erforderlichen Erhebungen vornehmen und Auskünfte einholen. Die betroffenen Mitglieder der Universität und ihre Angehörigen sind zur Mitwirkung und zur Angabe entsprechender personenbezogener Daten verpflichtet. Die Universitäten erlassen Satzungen, in denen das nähere Bewertungsverfahren geregelt und auch bestimmt wird, welche personenbezogenen Daten der Mitglieder der Universität und ihrer Angehörigen, die zur Bewertung notwendig sind, erhoben, verarbeitet und in welcher Form veröffentlicht werden.

§ 25 Fakultätsrat

(4) *[Satz 6 bis 9]*

Zu den Aufgaben der Studienkommission gehört es insbesondere, Empfehlungen zur Weiterentwicklung von Gegenständen und Formen des Studiums im Sinne von § 40 Abs. 1 und 2 sowie zur Verwendung der für Studium und Lehre vorgesehenen Mittel zu erarbeiten und die Evaluation der Lehre gemäß § 4 a unter Einbeziehung studentischer Veranstaltungskritik zu organisieren. Der Bericht enthält für den Berichtszeitraum auch Angaben über die Bewertung des Lehrangebotes in den einzelnen Studiengängen, insbesondere über Befragungen der Studierenden zur Qualität der Lehre und die Stellungnahme des Lehrkörpers zu den Ergebnissen der Befragung; der Bericht bezieht auch die Ergebnisse externer Bewertungen ein. Der Fakultätsrat gibt der Fachschaft Gelegenheit, zu dem Bericht Stellung zu nehmen. Der Fakultätsrat erörtert den Bericht der Studienkommission und ergreift geeignete Maßnahmen zur Verbesserung der Lehre.

§ 49 Beratung

(4) Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren Person, die um eine Beratung nachgesucht hat, dürfen nicht ohne deren Einverständnis an Dritte weitergegeben werden.

§ 112 Öffentlichkeit

(4) *[Satz 1 und 2]*
Die an einer Sitzung eines Gremiums Beteiligten sind zur Verschwiegenheit über alle in nichtöffentlicher Sitzung behandelten Angelegenheiten verpflichtet, soweit dies aus Gründen des öffentlichen Wohls geboten ist, Personal- oder Prüfungsangelegenheiten betroffen sind oder die Pflicht zur Verschwiegenheit besonders beschlossen worden ist. Die Pflicht zur Verschwiegenheit schließt auch die Geheimhaltung der Beratungsunterlagen ein.

§ 125a Verarbeitung personenbezogener Daten

(1) Die Studienbewerber, Studierenden und Prüfungskandidaten sowie die staatlichen und kirchlichen Prüfungsämter sind verpflichtet, für Verwaltungszwecke der Universität personenbezogene Daten zum Hochschulzugang, zum Studium, zum Studienverlauf und zu den Prüfungen anzugeben. Das Wissenschaftsministerium bestimmt durch Rechtsverordnung die anzugebenden Daten und die Zwecke, für die sie verarbeitet werden dürfen.

(2) Soweit den Universitäten soziale Betreuungsaufgaben nach § 59 b Abs. 2 zugewiesen worden sind, richtet sich die Verarbeitung personenbezogener Daten nach den Vorschriften des Landesdatenschutzgesetzes.

(3) Die Übermittlung der nach Absatz 1 erhobenen Daten und ihre Nutzung für andere Zwecke sind nur zulässig, wenn und soweit
1. eine Rechtsvorschrift dies erlaubt,
2. der Betroffene eingewilligt hat,
3. die Einwilligung des Betroffenen nicht eingeholt werden kann, jedoch offensichtlich ist, dass dies im Interesse des Betroffenen liegt und er in Kenntnis des anderen Zwecks einwilligen würde,
4. die Daten von der Universität für den anderen Zweck oder von der empfangenden Hochschule oder Berufsakademie auf Grund einer durch Rechtsvorschrift festgelegten Auskunftspflicht beim Betroffenen erhoben werden dürfen,
5. dies zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuches oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist und sich die ersuchende Stelle die Daten zur Verfolgung von Ordnungswidrigkeiten oder zur Vollstreckung von Bußgeldbescheiden nicht auf andere Weise beschaffen kann oder
6. dies zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person oder zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Abwehr einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist.

Eine Speicherung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung,

der Durchführung von Organisationsuntersuchungen, der Prüfung und Wartung von automatisierten Verfahren der Datenverarbeitung sowie statistischen Zwecken der speichernden Stelle dient. Dies gilt auch für die Speicherung und Nutzung zu Ausbildungs- und Prüfungszwecken, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) Die Universitäten dürfen zur Wahrnehmung ihrer Aufgaben in der Lehre die Teilnehmerinnen und Teilnehmer von Lehrveranstaltungen über Ablauf sowie Art und Weise der Darbietung des Lehrstoffs befragen und die Antworten auswerten. Eine Auskunftspflicht der Studierenden besteht nicht. Die Befragung und Auswertung darf nur so erfolgen, dass die Antworten und Auswertungen nicht oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft bestimmten oder bestimmbaren Teilnehmerinnen und Teilnehmern zugeordnet werden können. Die Ergebnisse der Befragung sollen in anonymisierter Form den Lehrenden und Studierenden bekanntgegeben und den zuständigen Gremien der Universität zur Erörterung übermittelt werden. Die Ergebnisse der Auswertung dürfen nur für Zwecke der Bewertung der Lehre verwendet werden.

(5) Die Universitäten dürfen in Veröffentlichungen bei Angaben über die dienstliche Erreichbarkeit von Professoren, Hochschul- und Privatdozenten, Mitarbeitern des wissenschaftlichen Dienstes, Lehrbeauftragten, Lehrkräften für besondere Aufgaben sowie sonstigen Mitarbeitern, die herausgehobene Funktionen in der Universität wahrnehmen, ohne deren Einwilligung nur Name, Amts-, Dienst- und Funktionsbezeichnung, Telefon- und Telefaxnummern sowie E-Mail- und Internet-Adressen aufnehmen. Der Betroffene kann der Veröffentlichung widersprechen, wenn sein schutzwürdiges Interesse wegen seiner besonderen persönlichen Situation das Interesse der Universität an der Veröffentlichung überwiegt. Andere als die in Satz 1 aufgeführten Angaben dürfen nur veröffentlicht werden, soweit der Betroffene eingewilligt hat.

7.3 Hochschul-Datenschutzverordnung

§ 1 Zulassung

Studienbewerber haben den Hochschulen für die Zulassung folgende personenbezogene Daten anzugeben:

1. Familienname,
2. Vorname,
3. Geburtsdatum,
4. Geschlecht,
5. Heimat- und Semesteranschrift,
6. Staatsangehörigkeit,
7. Hochschulzugangsberechtigung (Art, Jahr des Erwerbs, Noten, Ort der Ausstellung),
8. Studiengang, für den die Zulassung angestrebt wird sowie die angestrebte Abschlussprüfung, das gewünschte Studienfach oder die gewünschten Studienfächer und die gewünschte Gewichtung des Studienfachs (Haupt- und Nebenfach, Vertiefungsrichtung o. Ä.),

9. weitere Studiengänge, für welche die Zulassung hilfsweise beantragt wird,
10. frühere Zulassungen und abgelegte Prüfungen, sowie beantragte oder beabsichtigte gleichzeitige Zulassung zu einem anderen Studiengang,
11. Verlust des Prüfungsanspruchs in dem angestrebten oder einem verwandten Studiengang,
12. Dauer, Art und Umfang berufspraktischer Tätigkeiten vor Aufnahme des Studiums oder besondere Kenntnisse, Fähigkeiten und Vorbildungen soweit diese Zulassungsvoraussetzungen sind,
13. Dauer, Art und Umfang eines Arbeits-, Dienst- oder Ausbildungsverhältnisses oder einer sonstigen beruflichen Tätigkeit während des Studiums,
14. deutsche Sprachkenntnisse,
15. Konfessionszugehörigkeit bei Wahl eines theologischen Studienfaches,
16. Ergebnis einer erforderlichen künstlerischen Eingangsprüfung oder Sporteingangsprüfung.
Die Hochschulen können diese Daten für ihre Verwaltungszwecke verarbeiten oder sonst nutzen.

§ 2 Immatrikulation

Studienbewerber haben den Hochschulen zusätzlich zu den nach § 1 anzugebenden Daten für die Immatrikulation folgende weitere personenbezogene Daten anzugeben:
1. Frühere Namen, insbesondere Geburtsnamen, Geburtsort,
2. Hörerstatus, Art des Studiums, Hochschulsemester, Fachsemester, Praxissemester, Semester an Studienkollegs, Urlaubssemester, Studienunterbrechungen nach Art, Dauer und Grund,
3. Fakultäts- oder Fachbereichszugehörigkeit,
4. Bezeichnung der bisher besuchten Hochschulen sowie der gleichzeitig besuchten weiteren Hochschulen, die an diesen verbrachten Studienzeiten und jeweils gewählten Studiengänge,
5. Art, Fachrichtung, Monat, Jahr sowie Note und Ergebnis der bisher abgelegten Vor-, Zwischen- und Abschlussprüfungen,
6. Vorliegen eines Einberufungsbescheids zum Wehrdienst oder Zivildienst,
7. Umstände, die einer Immatrikulation entgegenstehen können, insbesondere
a) Mitgliedschaft in einer anderen Hochschule oder vorangegangener Ausschluss als Mitglied einer Hochschule,
b) Krankheit, durch die der Studienbewerber die Gesundheit anderer Studenten ernstlich gefährdet oder den ordnungsgemäßen Studienbetrieb zu beeinträchtigen droht oder ein Gesundheitszustand, der ein ordnungsgemäßes Studium ausschließt,
c) strafbare Handlungen in den zwei vorangegangenen Jahren, die bei bestehender Mitgliedschaft zur Exmatrikulation berechtigt hätten,
d) Verbüßung einer Freiheitsstrafe während des Studiums,
8. Versicherungsbescheinigung der zuständigen Krankenkasse nach der Studentenkrankenversicherungs-Meldeverordnung,
9. Entrichtung des Beitrags an das Studienwerk.

Die Hochschulen können diese Daten für ihre Verwaltungszwecke verarbeiten oder sonst nutzen.

§ 3 Unterlagen für die Zulassung und die Immatrikulation

(1) Zur Zulassung sind folgende Unterlagen vorzulegen:
1. Eine vollständige und amtlich beglaubigte Kopie oder Abschrift der Hochschulzugangsberechtigung, erforderlichenfalls auch der Hochschuleingangsprüfung und auf Anforderung der Hochschule die Originale,
2. Antrag auf Zulassung,
3. Nachweis, dass der Studienbewerber zeitlich in der Lage ist, sich dem Studium uneingeschränkt zu widmen, sofern ein Dienst-, Arbeits- oder Ausbildungsverhältnis während des Studiums (Vorlesungszeit) besteht; falls ein Parallelstudium beabsichtigt ist, ist ein Nachweis über die bisherigen Studienleistungen vorzulegen,
4. bei Ausländern der Nachweis, dass ausreichende deutsche Sprachkenntnisse bestehen,
5. zum Studium erforderlicher Nachweis der künstlerischen Begabung oder der sportlichen Leistungsfähigkeit.

(2) Zur Immatrikulation sind folgende Unterlagen vorzulegen:
1. Kopie des Zulassungsbescheides der Hochschule oder der Zentralstelle für die Vergabe von Studienplätzen,
2. Antrag auf Immatrikulation,
3. eine vollständige und amtlich beglaubigte Kopie oder Abschrift der Hochschulzugangsberechtigung und auf Anforderung der Hochschule das Original,
4. vollständige Nachweise über bereits erbrachte Studien- und Prüfungsleistungen und Zeugnisse über bereits abgelegte Vor-, Zwischen- und Abschlussprüfungen bzw. deren Anerkennung,
5. Abgangsbescheinigung der zuletzt besuchten Hochschule,
6. zum Studium erforderliche Praktikumsnachweise und Zeugnisse,
7. zum Studium erforderlicher Nachweis der künstlerischen Begabung, oder der sportlichen Leistungsfähigkeit, soweit bei der Zulassung nicht vorgelegt,
8. Versicherungsbescheinigung der zuständigen Krankenkasse nach der Studentenkrankenversicherungs-Meldeverordnung sowie den Nachweis über den entrichteten Beitrag für das Studentenwerk,
9. bei Ausländern eine Aufenthaltsgenehmigung, die zur Aufnahme eines Studiums berechtigt,
10. Geburtsurkunde, Personalausweis, oder Reisepass auf Verlangen der Hochschule.

§ 4 Rückmeldung

(1) Bei der Rückmeldung haben die Bewerber auf Verlangen der Hochschule folgende personenbezogenen Daten anzugeben:
1. Familienname, Vorname, Geburtsdatum, Geschlecht,
2. Heimat- und Semesteranschrift, Matrikelnummer,
3. Nachweis über die Entrichtung des Beitrags an das Studentenwerk.

(2) Beim Rückmeldeverfahren verarbeitet und nutzt die Hochschule die bisher gespeicherten sowie die nach Absatz 1 anzugebenden Daten für ihre Verwaltungszwecke.

§ 5 Beurlaubung

Studierende, die eine Beurlaubung beantragen, haben die für die Beurlaubung geltend gemachten Gründe anzugeben und nachzuweisen. Bei dem Verfahren zur Beurlaubung verarbeitet die Hochschule die bisher gespeicherten Daten. Darüber hinaus werden Urlaubsgrund, Semester und Dauer der Beurlaubung gespeichert und verarbeitet.

§ 6 Gasthörer

Der Antrag auf Zulassung als Gasthörer muss folgende Angaben enthalten:
1. Familienname,
2. Vorname,
3. Geburtsdatum,
4. Geschlecht,
5. Anschrift,
6. gewünschte Lehrveranstaltungen und Fachrichtung,
7. Staatsangehörigkeit.

Die Hochschulen können diese Daten für ihre Verwaltungszwecke verarbeiten oder sonst nutzen. Die Hochschulen sind berechtigt, Nachweise über die Vorbildung zu erheben.

§ 7 Studienausweis

Der Studienausweis enthält folgende Angaben:
1. Familienname,
2. Vorname,
3. Geburtsdatum,
4. Studiengang,
5. Matrikel-Nummer,
6. Gültigkeitsdauer,
7. Fakultäts- oder Fachbereichszugehörigkeit,
8. auf Verlangen der Hochschule ein mit dem Erscheinungsbild des Inhabers übereinstimmendes Lichtbild.

§ 8 Mitteilungspflichten

Die Studierenden haben der Hochschule unverzüglich mitzuteilen:
1. Änderung des Namens, der Anschrift und der Staatszugehörigkeit,
2. Aufnahme eines Dienst-, Arbeits- oder Ausbildungsverhältnisses, das während des Studiums ausgeübt wird und das Studium beeinträchtigt,
3. den Verlust des Studienbuches oder des Studienausweises,
4. die Verbüßung einer Freiheitsstrafe,
5. das Auftreten einer Krankheit gemäß § 2 Abs. 1 Nr. 7b.

Die Hochschulen können diese Daten für ihre Verwaltungszwecke verarbeiten oder sonst nutzen.

§ 9 Zulassung zu Hochschulprüfungen

(1) Im Prüfungsverfahren verarbeitet die Hochschule, das zuständige Prüfungsamt oder die Prüfungsstellen die bei Zulassung“ Immatrikulation, Rückmeldung, Beurlaubung und Exmatrikulation erhobenen und gespeicherten Daten. Bei der Meldung zur Prüfung sind zusätzlich folgende Daten anzugeben:
1. Matrikelnummer,
2. Art der Prüfung,
3. Zulassungsvoraussetzungen,
4. Angabe über etwaigen Verlust des Prüfungsanspruchs,
5. Anzahl der bisherigen Prüfungsversuche,
6. bei Abschlussprüfungen Angabe einer Ausbildungsförderung.
Die Hochschulen können diese Daten für ihre Verwaltungszwecke verarbeiten oder sonst nutzen.

(2) Bei der Meldung zur Prüfung sind folgende Unterlagen vorzulegen:
1. Der Nachweis über die Erfüllung der Zulassungsvoraussetzungen über die abgelegte Zwischenprüfung, Diplom-Vorprüfung (Art, Fach, Zeitpunkt und Ergebnis),
2. Nachweis über Fristenverlängerung zur Ablegung der Zwischenprüfung/Diplom-Vorprüfung,
3. bei Promotionsprüfung zusätzlich der Nachweis über die zuletzt besuchte Hochschule und die abgelegte Abschlussprüfung (Art, Fach, Zeitpunkt und Ergebnis).

(3) Die Hochschule kann von den Teilnehmern einer Lehrveranstaltung, deren erfolgreiches Bestehen zu bescheinigen ist, folgende Daten erheben und verarbeiten:
1. Familienname,
2. Vorname,
3. Matrikelnummer,
4. Anschrift,
5. Zahl der bisherigen Fachsemester.

§ 10 Exmatrikulation

Für die Exmatrikulation verarbeitet die Hochschule die bisher gespeicherten Daten des Antragstellers und erhebt und verarbeitet darüber hinaus den Grund, das Datum und den Zeitpunkt des Wirksamwerdens der Exmatrikulation.

§ 11 Lehrberichte

Die Hochschule darf die gespeicherten Daten auch verarbeiten und nutzen, soweit dies zur Erstellung von fachspezifischen anonymisierten Lehrberichten durch ihre hierfür zuständigen Stellen erforderlich ist.
Die Lehrberichte geben insbesondere Auskunft über:
– die Fachstudiendauer bis zur Vor- oder Zwischen- und bis zur Abschlussprüfung,
– die Schwundquote bis zur Vor- oder Zwischenprüfung,
– die Erfolgsquote bei der Vor- oder Zwischenprüfung,
– die Absolventenquote,

– die Notenverteilung bei den Prüfungen.

§ 12 Verarbeitung der Daten

(1) Die Hochschule darf folgende Daten von Studierenden 40 Jahre – vom Zeitpunkt der Exmatrikulation ab gerechnet – verarbeiten:
1. Familienname, Vorname, Geburtsname, Geburtsdatum, Geburtsort, Geschlecht,
2. Studiengang, Matrikelnummer,
3. Praxissemester, Urlaubssemester oder sonstige Studienunterbrechungen,
4. Ergebnis und Datum der Diplom-Vorprüfung oder Zwischenprüfung,
5. Ergebnis und Datum der Abschlussprüfung mit Gesamtnote und den die Gesamtnote tragenden Einzelnoten,
6. Datum der Immatrikulation und Exmatrikulation sowie Exmatrikulationsgrund.
Diese Daten sind nach der Exmatrikulation gemäß § 20 Abs. 3 des Landesdatenschutzgesetzes unverzüglich zu sperren, es sei denn, das Prüfungsverfahren ist noch nicht abgeschlossen; in diesem Falle sind diese Daten unverzüglich nach Abschluss des Prüfungsverfahrens zu sperren. Alle sonstigen Daten sind nach der Exmatrikulation unverzüglich zu löschen, es sei denn, das Prüfungsverfahren ist noch nicht abgeschlossen; in diesem Falle sind die Daten nach Abschluss des Prüfungsverfahrens unverzüglich zu löschen.

(2) Die Daten von Personen, die nicht immatrikuliert werden, sind nach der rechtskräftigen Entscheidung hierüber, die Daten von Gasthörern nach Beendigung der Zulassung unverzüglich zu löschen.

7.4 Landesbeamtengesetz (LBG)

§ 113 Personalakte

(1) Über jeden Beamten ist eine Personalakte zu führen; sie ist vertraulich zu behandeln und vor unbefugter Einsicht zu schützen. Zur Personalakte gehören alle Unterlagen einschließlich der in Dateien gespeicherten Informationen, die den Beamten betreffen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten); andere Unterlagen dürfen in die Personalakte nicht aufgenommen werden. Personalaktendaten dürfen nur für Zwecke der Personalverwaltung oder Personalwirtschaft verwendet werden, es sei denn, der Beamte willigt in die anderweitige Verwendung ein. Nicht Bestandteil der Personalakte sind Unterlagen, die besonderen, von der Person und dem Dienstverhältnis sachlich zu trennenden Zwecken dienen, insbesondere Prüfungs-, Sicherheits- und Kindergeldakten. Kindergeldakten können mit Besoldungs- und Versorgungsakten verbunden geführt werden, wenn diese von der übrigen Personalakte getrennt sind und von einer von der Personalverwaltung getrennten Organisationseinheit bearbeitet werden; § 35 des Ersten Buches Sozialgesetzbuch und die §§ 67 bis 78 des Zehnten Buches Sozialgesetzbuch bleiben unberührt.

(2) Die Personalakte kann nach sachlichen Gesichtspunkten in Grundakte und Teilakten gegliedert werden; Unterlagen über Disziplinarverfahren sind stets als

Teilakte zu führen. Teilakten können bei der für den betreffenden Aufgabenbereich zuständigen Behörde geführt werden. Nebenakten (Unterlagen, die sich auch in der Grundakte oder in Teilakten befinden) dürfen nur geführt werden, wenn die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist oder wenn mehrere personalverwaltende Behörden für den Beamten zuständig sind; sie dürfen nur solche Unterlagen enthalten, deren Kenntnis zur rechtmäßigen Aufgabenerledigung der betreffenden Behörde erforderlich ist. In die Grundakte ist ein vollständiges Verzeichnis aller Teil- und Nebenakten aufzunehmen.

(3) Zugang zur Personalakte dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist; dies gilt auch für den Zugang im automatisierten Abrufverfahren

(4) Der Dienstherr darf personenbezogene Daten über Bewerber, Beamte, frühere Beamte und ihre Hinterbliebenen nur erheben, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes erforderlich ist oder eine Rechtsvorschrift dies erlaubt. Fragebogen, mit denen solche personenbezogenen Daten erhoben werden, bedürfen der Genehmigung durch die zuständige oberste Dienstbehörde; der Genehmigung bedarf es nicht für Fragebogen, die durch eine Verwaltungsvorschrift eines Ministeriums für die Verwendung in der Landesverwaltung festgelegt sind.

(5) Die oberste Dienstbehörde bestimmt, bei welcher Behörde oder Dienststelle die Personalakten, im Falle der Gliederung die Grund- und Teilakten, zu führen sind.

§ 113c Einsichtsrecht

(1) Der Beamte hat, auch nach Beendigung des Beamtenverhältnisses, ein Recht auf Einsicht in seine vollständige Personalakte.

(2) Einem Bevollmächtigten des Beamten ist Einsicht zu gewähren, soweit dienstliche Gründe nicht entgegenstehen. Dies gilt auch für Hinterbliebene, wenn ein berechtigtes Interesse glaubhaft gemacht wird, und deren Bevollmächtigte. Für Auskünfte aus der Personalakte gelten die Sätze 1 und 2 entsprechend.

(3) Die personalaktenführende Behörde bestimmt, wo die Einsicht gewährt wird. Soweit dienstliche Gründe nicht entgegenstehen, können Auszüge, Abschriften, Ablichtungen oder Ausdrucke gefertigt werden; dem Beamten ist auf Verlangen ein Ausdruck der zu seiner Person automatisiert gespeicherten Personalaktendaten zu überlassen.

(4) Der Beamte hat ein Recht auf Einsicht auch in andere Akten, die personenbezogene Daten über ihn enthalten und für sein Dienstverhältnis verarbeitet werden, soweit gesetzlich nichts anderes bestimmt ist; dies gilt nicht für Sicherheitsakten. Die Einsichtnahme ist unzulässig, wenn die Daten des Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart

verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist dem Beamten Auskunft zu erteilen.

§ 113d Vorlage und Auskunft

(1) Ohne Einwilligung des Beamten ist es zulässig, die Personalakte für Zwecke der Personalverwaltung oder Personalwirtschaft der obersten Dienstbehörde oder einer im Rahmen der Dienstaufsicht weisungsbefugten Behörde vorzulegen. Das gleiche gilt für Behörden desselben Geschäftsbereichs, soweit die Vorlage zur Vorbereitung oder Durchführung einer Personalentscheidung notwendig ist, sowie für Behörden eines anderen Geschäftsbereichs desselben Dienstherrn, soweit diese an einer Personalentscheidung mitzuwirken haben. Ärzten, die im Auftrag der personalverwaltenden Behörde ein medizinisches Gutachten erstellen, darf die Personalakte ebenfalls ohne Einwilligung vorgelegt werden. Die Vorlage der Personalakte an andere Dienstherren ist nur mit Einwilligung des Beamten zulässig, es sei denn, sie dient der Vorbereitung personeller Maßnahmen, die nicht der Zustimmung des Beamten bedürfen. Für Auskünfte aus der Personalakte gelten die Sätze 1 bis 4 entsprechend. Soweit eine Auskunft ausreicht, ist von einer Vorlage abzusehen.

(2) Auskünfte an sonstige Dritte dürfen nur mit Einwilligung des Beamten erteilt werden, es sei denn, dass die Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder der Schutz rechtlicher, höherrangiger Interessen des Dritten die Auskunftserteilung erfordert. Inhalt und Empfänger der Auskunft sind dem Beamten schriftlich mitzuteilen.

(3) Vorlage und Auskunft sind auf den jeweils erforderlichen Umfang zu beschränken.

(4) § 113 a bleibt unberührt.

§ 113f Aufbewahrung, Vernichtung

(1) Personalakten sind nach ihrem Abschluss von der personalaktenführenden Behörde fünf Jahre aufzubewahren. Personalakten sind abgeschlossen,

1. wenn der Beamte ohne Versorgungsansprüche aus dem öffentlichen Dienst ausgeschieden ist, mit Ablauf des Jahres der Vollendung des 65. Lebensjahres, in den Fällen des § 66 dieses Gesetzes und des § 11 der Landesdisziplinarordnung jedoch erst, wenn mögliche Versorgungsempfänger nicht mehr vorhanden sind,
2. wenn der Beamte ohne versorgungsberechtigte Hinterbliebene verstorben ist, mit Ablauf des Todesjahres,
3. wenn nach dem verstorbenen Beamten versorgungsberechtigte Hinterbliebene vorhanden sind, mit Ablauf des Jahres, in dem die letzte Versorgungsverpflichtung entfallen ist.

(2) Unterlagen über Beihilfen, Heilfürsorge, Heilverfahren, Unterstützungen, Urlaub, Erkrankungen, Umzugs- und Reisekosten sind drei Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, aufzubewahren.

(3) Versorgungsakten sind zehn Jahre nach Ablauf des Jahres, in dem die letzte Versorgungszahlung geleistet worden ist, aufzubewahren; besteht die Möglichkeit eines Wiederauflebens des Anspruchs, sind die Akten 30 Jahre aufzubewahren.

(4) Nebenakten, die von einer Beschäftigungsbehörde geführt werden, die nicht zugleich personalverwaltende Behörde ist, sind, soweit sie bei der Beschäftigungsbehörde verbleiben, ein Jahr nach Ablauf des Jahres, in dem der Beamte aus dieser Beschäftigungsbehörde ausgeschieden ist, aufzubewahren.

(5) Die Personalakten werden nach Ablauf der Aufbewahrungsfrist vernichtet, sofern sie nicht vom zuständigen Archiv übernommen werden.

(6) Die für die Versorgung zuständige Behörde hat in den Fällen des Absatzes 1 Nr. 2 und 3 der personalaktenführenden Behörde den Zeitpunkt des Abschlusses der Personalakten mitzuteilen.

§ 113g Datenverarbeitung in Dateien

(1) Personalaktendaten dürfen in Dateien nur für Zwecke der Personalverwaltung oder der Personalwirtschaft verarbeitet werden. Ihre Übermittlung ist nur nach Maßgabe der § 113 a Abs. 2 und 3 und § 113 d zulässig. Ein automatisierter Datenabruf durch andere Behörden ist unzulässig, soweit durch besondere Rechtsvorschrift nichts anderes bestimmt ist.

(2) Personalaktendaten im Sinne des § 113 a dürfen automatisiert nur im Rahmen ihrer Zweckbestimmung und nur von den übrigen Personaldateien technisch und organisatorisch getrennt verarbeitet werden. Dies gilt nicht für Besoldungs- und Versorgungsdaten, die auch bei der Gewährung von Leistungen im Rahmen der Beihilfe und Heilfürsorge sowie des Heilverfahrens erforderlich sind.

(3) Von den Unterlagen über medizinische oder psychologische Untersuchungen und Tests dürfen im Rahmen der Personalverwaltung nur die Ergebnisse automatisiert verarbeitet werden, soweit sie die Eignung betreffen und ihre Verarbeitung dem Schutz des Beamten dient.

(4) Beamtenrechtliche Entscheidungen dürfen nicht ausschließlich auf Informationen und Erkenntnisse gestützt werden, die unmittelbar durch automatisierte Verarbeitung personenbezogener Daten gewonnen werden.

(5) Bei erstmaliger Speicherung in automatisierten Dateien ist dem Betroffenen die Art der über ihn gemäß Absatz 1 gespeicherten Daten mitzuteilen, bei wesentlichen Änderungen ist er zu benachrichtigen. Ferner sind die Verarbeitungsformen automatisierter Personalverwaltungsverfahren zu dokumentieren und einschließlich des jeweiligen Verwendungszweckes sowie der regelmäßigen Empfänger und des Inhalts automatisierter Datenübermittlung allgemein bekanntzugeben.

8. Muster

8.1 Muster für eine Einwilligungserklärung

Quelle: [Metschke2000], S. 56 – 63.

Will eine universitäre Abteilung im Rahmen eines Forschungsvorhabens eine Studie anfertigen, zu der personenbezogene Daten verarbeitet werden sollen, so sollte sie von den Befragten eine datenschutzrechtliche Einwilligungserklärung einholen. Diese Einwilligungserklärung hat folgende Angaben zu enthalten:

1. Angaben zur verantwortlichen Stelle:

Träger und Leiter des Forschungsvorhabens, zu dem die Einwilligungserklärung eingeholt werden soll, damit die verantwortliche Stelle eindeutig und mindestens für die Dauer des Forschungsvorhabens (und der damit verbundenen Verarbeitungszeiten) benannt ist.

Beispiel

> Die Abteilung Medieninformatik ist Teil der Fakultät für Informatik an der Universität Ulm und zugleich eine wissenschaftliche Lehr- und Forschungseinheit, die sich schwerpunktmäßig mit ... beschäftigt. Leiter der Abteilung ist Prof. Dr. Michael Weber.

2. Allgemeine Angaben zum Datenschutz:

Beispiel

> Unsere Arbeiten berücksichtigen stets die zugrunde liegenden Bestimmungen des Datenschutzes. Die Grundlage für unsere Datenverarbeitung bildet dabei diese Einverständniserklärung neben dem Landesdatenschutzgesetz.

3. Angaben zum konkreten Forschungsvorhaben:

- Zweck des Forschungsvorhabens
- Art der Daten, die hierzu von den Betroffenen erhoben werden sollen
- Art und Weise der Datenverarbeitung
- Maßnahmen zur Datensicherheit (insbesondere: wer ist zugriffsberechtigt, existieren Sicherheitsvorkehrungen wie Firewalls, Passwort-geschützte Datenverarbeitungssysteme,

Terminalbeschränkungen zur Verarbeitung, automatische Bildschirmsperren und Protokollierungsvorschriften)

4. Rechtsbelehrung:

Beispiel

Ihre personenbezogenen Daten werden nur für dieses Forschungsvorhaben und unmittelbar mit diesem Forschungsvorhaben in Verbindung stehende Forschungsvorhaben verwendet. Sie werden nicht an Dritte zu anderen Zwecken weitergegeben, es sei denn, Sie willigen erneut in einer späteren Einwilligungserklärung in eine solche Weiterübermittlung der Daten ein. Sobald der Forschungszweck dies erlaubt, werden die Informationen, mit denen ein Personenbezug hergestellt werden kann, aus Datensicherheitsgründen gesondert gespeichert. Sobald der Forschungszweck es zulässt, werden Ihre personenbezogenen Daten vernichtet bzw. gelöscht. Dies wird spätestens am ... sein. Ihre Einwilligung ist freiwillig. Durch eine Verweigerung der Einwilligung entstehen Ihnen keine Nachteile. Sie können Ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen und die Löschung bzw. Vernichtung Ihrer Daten verlangen. Sie haben das Recht, Auskunft über die von uns gespeicherten Daten zu erhalten und können den Landesdatenschutzbeauftragten anrufen.

5. Unterschrift des Betroffenen:

Beispiel

Ich habe die Information über das Forschungsvorhaben erhalten und bin mit der vorgesehenen Verarbeitung meiner Daten einverstanden.

Ort, Datum, Unterschrift

8.2 Muster für eine Datenschutzerklärung

Quelle: Existierende Datenschutzerklärungen einzelner Universitäten, zusammengetragen von Dr. Wolfram Gass

Im Rahmen ihrer Tätigkeit kann die universitäre Abteilung eine im Internet veröffentlichte Datenschutzerklärung über die angewandten Datenschutzmaßnahmen abrufbar machen, so dass sich Dritte vorab informieren können. Diese freiwillige Datenschutzerklärung sollte folgende Angaben enthalten:

1. Angaben zur verantwortlichen Stelle:

Die Einrichtung, welche die Datenschutzerklärung abgibt, muss unbedingt genau, d.h. mit Anschrift und der verantwortlichen Person bezeichnet werden.

Beispiel

> Die Abteilung Medieninformatik ist Teil der Fakultät für Informatik an der Universität Ulm und zugleich eine wissenschaftliche Lehr- und Forschungseinheit, die sich schwerpunktmäßig mit ... beschäftigt. Leiter der Abteilung ist Prof. Dr. Michael Weber.

2. Allgemeine Angaben zum Datenschutz:

Beispiel

> Unsere Arbeiten berücksichtigen stets die zugrunde liegenden Bestimmungen des Datenschutzes. Die Grundlage für unsere Datenverarbeitung bildet dabei diese Einverständniserklärung neben dem Landesdatenschutzgesetz.

3. Erhebung:

- Rechtsgrundlage für die Erhebung von personenbezogenen Daten (z.B. § 13 und 14 LDSG; § ... Hochschul-Datenschutzverordnung oder andere Bereichsregelungen)
- Hinweis auf datenschutzgerechten Umgang im Rahmen der Erhebung

Beispiel

> Ihre Daten werden von uns nur in der Weise verarbeitet, wie dies in den oben aufgeführten Rechtsvorschriften vorgesehen ist oder wie Sie das in Ihrer Einwilligung erklärt haben. Im Rahmen des Zugriffs auf unser Internetangebot wird aus Sicherheitsgründen in einer Protokolldatei vorübergehend die Adresse der aufgerufenen Daten, der Zeitpunkt des Zugriffs, die Mitteilung, ob der Zugriff erfolgreich verlief und die aufrufende IP-Adresse gespeichert. Eine

Auswertung erfolgt nur zu statistischen Zwecken.

4. Speicherung, Veränderung, Nutzung, Übermittlung:

- Rechtsgrundlage für das Bearbeiten der erhobenen personenbezogenen Daten
- Hinweis auf datenschutzgerechten Umgang im Rahmen des Bearbeitens (hier müssen Hinweise über Löschungsfristen, Anonymisierungsverfahren, Empfänger von Weiterleitungen z.B. zur technischen Wartung, die Freiwilligkeit des Nutzers beim Aufruf von Diensten, einen Ausschluss kommerzieller Nutzung, etc. aufgeführt werden)

5. Maßnahmen zur Datensicherheit:

- etwaige Risiken des Nutzers (z.B. Gefahr des Lesens bzw. der Verfälschung von Daten bei der Übertragung durch Dritte, Cookies...)
- ergriffene technische und organisatorische Maßnahmen (z.B. Firewalls, Passwortschutz, Protokollierungsvorschriften)

6. Haftungsausschluss:

Beispiel

Inhalte und Funktionalitäten unserer Internetangebote wurden unter größtmöglicher Sorgfalt implementiert und werden regelmäßig aktualisiert. Dennoch können wir nicht ausschließen, dass Fehler auftreten. Wir übernehmen daher keine Haftung für die Richtigkeit, Vollständigkeit und Aktualität unseres Internetangebots. Für eventuelle Schäden oder Konsequenzen, die durch die direkte oder indirekte Nutzung der angebotenen Inhalte entstehen, übernehmen wir keine Haftung. Ebenso wird keine Haftung übernommen für eventuelle Datenschutz- oder sonstige Rechtsverletzungen in anderen Angeboten, auf die wir einen Link gesetzt haben.

7. Datenschutzsiegel:

Ein Datenschutzsiegel wird nur aufgeführt, sofern die Datenschutzerklärung in einem Datenschutz-Audit-Verfahren von einem unabhängigen und dafür zugelassenen Gutachter überprüft und zertifiziert wurde.