Bernd Juraschko

Datenschutz in der Bibliothek 2.0

Einleitung

Sowohl die Gesprächsnotiz der Bibliothekarin mit einem Benutzer als auch eine E-Mail hinterlassen Spuren. Wie diese Daten zu behandeln sind, ist nicht nur eine technische Angelegenheit, sondern auch ein Thema des Datenschutzes. Je stärker der Datenaustausch vorgenommen wird, desto wichtiger ist ein wirksamer Schutz personenbezogener Daten. Eine Bibliothek 2.0, die besonders stark Interaktion fördert, hat sich daher mit dem Datenschutz aktiv auseinander zu setzen. Unter der Bibliothek 2.0 wird hier eine individuelle oder zumindest individualisierbare Bibliothek verstanden. Eine Bibliothek, die den jeweiligen Erwartungen des Kunden möglichst gerecht wird. Von einer solchen Bibliothek wird ein Höchstmaß an Flexibilität gefordert. Mitentscheidend für den Erfolg einer Serviceleistung ist das Vertrauen in den Schutz der persönlichen Integrität des einzelnen Nutzers. Dem Datenschutz kommt eine hervorgehobene Stellung zu und ist keinesfalls nur aus allgemeiner Gesetzesgehorsamspflicht umzusetzen.

Allgemeine Grundlagen

Grundanliegen des Datenschutzes

Grundanliegen des Datenschutzes ist die Wahrung des Rechtes auf informationelle Selbstbestimmung. Dies hat das Bundesverfassungsgericht ausdrücklich im sogenannten Volkszählungsurteil festgestellt.[1] Das Recht auf informationelle Selbstbestimmung steht jeder natürlichen Person zu. Es ist unabhängig von Staatsangehörigkeit oder Wohnsitz. Der Datenschutz umfasst jegliche personenbezogene Datenerhebung und Datenverarbeitung –somit die gesamte Existenzdauer der Daten. Dabei geht es um die Verfügungsbefugnis über individualisierte Daten, Eingriffsabwehr, Wissen über die Art der Verwendung, Gewährleistung der Kommunikations- und Handlungsfähigkeit des Einzelnen.[2] Personenbezogene

1 BVerfGE, NJW 1984, 419
2 Sokol in Gehrke, S. 94

Daten können sein: Name, Adresse, Geburtsdatum, Telefonnummer, Mail- und IP-Adresse, Logfiles und Verbindungsdaten, Rechnungen etc.

Der Datenschutz ist ausdrücklich nicht auf die elektronische Datenverarbeitung beschränkt. Die Verarbeitung personenbezogener Daten ist nur erlaubt, wenn eine gesetzliche Grundlage oder eine Einwilligung besteht. Dies gilt auch dann, wenn das Gesamtergebnis nützlich ist oder jedenfalls so erscheint. Ausgeschlossen ist daher ein Kompetenzerfindungsrecht der handelnden Person. Eine Einwilligung muss stets freiwillig abgegeben werden. Eine freie Willensbildung ist nur bei Vorliegen aller relevanten Informationen über den Zweck und die Art der Informationsverarbeitung möglich. Die erteilte Einwilligung ist zu protokollieren und für den Nutzer jederzeit zugänglich. Dem Nutzer muss es möglich sein, seine Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen. Soweit Daten verarbeitet werden, erfolgt dies für einen bestimmten und bekannten Zweck. Dieser Zweck darf ohne zusätzliche Zustimmung des Betroffenen weder einfach verändert oder gar ausgetauscht werden.

Weiterhin fordert der Datenschutz die Transparenz der Datenverarbeitung. Der Betroffene hat schnell und unkompliziert Kenntnis darüber erhalten, wo und in welchem Umfang Daten über seine Person gesammelt wurden.

Die große Bandbreite des Datenschutzes wird durch das einschränkende Merkmal der Personenbezogenheit begrenzt. Daher ist Datenschutz nur eine Teilmenge des Komplexes Datensicherheit. Anders formuliert ist Datenschutz ohne Datensicherheit nicht möglich.

Potentielle Gefahren

Durch Mängel im Sicherheitssystem der Datenverarbeitung können Menschen (natürliche Personen) massiv geschädigt werden. Besonders betroffen ist vor allem das allgemeine Persönlichkeitsrecht, das sich beispielsweise in der Würde und dem Ansehen eines Menschen äußert. Darüber hinaus können wirtschaftliche Schäden wie eine schlechtere Kreditwürdigkeit etc. eintreten.

Juristische Personen, z.B. ein eingetragener Verein oder eine GmbH, werden von einem Teil der Datenschutzgesetze ebenfalls geschützt.[3] Durch den Verlust geheimer Informationen können sie einen Wettbewerbsnachteil gegenüber Konkurrenten erleiden. Der Wettbewerbsnachteil entsteht durch den Verlust von Know-how und dem Ansehensverlust.

Lecks bei der Datensicherheit sind von besonderer Qualität. Einmal preisgegebene Informationen können nicht mehr zurückgeholt werden. Die Gründe für Lücken im Sicherheitssystem der Datenverarbeitung können vielfältig sein. Im Wesentlichen lassen sie sich unterteilen in:

3 Kein Schutz juristischer Personen besteht aber nach dem Bundesdatenschutzgesetz

Technisches Versagen (Ausfall von Hard- und Software)
Organisatorische Mängel (mangelhafte Wartung, fehlende oder fehlerhafte Dokumentation, menschliche Fehlhandlungen (Herumliegenlassen von Passwörtern, Löschen oder fehlerhaftes Verschieben von Daten)
Vorsätzliche Handlungen
Höhere Gewalt (Überschwemmung, Blitzeinschlag)
Unrechtmäßigkeit des Handelns

Mittel und Handlungsweisen

Ohne Datensicherheit ist ein wirksamer Datenschutz nicht möglich. Einem guten Datenschutz liegt ein klares Konzept zu Grunde. Er umfasst die organisatorische und technische Umsetzung. Ferner führt er zu einer Bewusstseinsbildung bei den Mitarbeiterinnen und Mitarbeitern. Bei aller Standfestigkeit ist das Datenschutzkonzept nicht fix, sondern ist regelmäßig zu überprüfen. Gegebenfalls findet eine Anpassung des Konzepts auf neue Situationen statt.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat für unterschiedliche Schutzbedürfnisse zwei verschiedene Wege zur Herstellung und Wahrung der Informationssicherheit und damit des Datenschutzes entwickelt:

1. Das analytische Vorgehen nach dem IT-Sicherheitshandbuch. Grundlage ist eine umfassende formelle Risikoanalyse. Dieses Verfahren durchzuführen ist sehr aufwändig.
2. Besitzen die zu schützenden Systeme höchstens einen mittleren Schützbedarf, so kann stattdessen auch der IT-Grundschutz des BSI angewendet werden. Im IT-Grundschutzhandbuch werden pauschalisierte Maßnahmen empfohlen. Das Handbuch ist modular aufgebaut. Die einzelnen Module können somit bedarfsgerecht angewendet werden. Auf Grund der sehr detaillierten Darstellung zu sehr vielen Aspekten der Informationstechnik ist es sehr umfangreich. Es enthält Maßnahmenlisten, wie technisch die Sicherheit erhöht und gewährleistet werden kann.

Ob der zweite Weg für den Schutz der jeweiligen personenbezogener Daten genügt, kann nur im Einzelfall entschieden werden. Notwendig sind alle erforderlichen Maßnahmen, um den Schutz herzustellen. Nicht notwendig ist die in jedem Fall denkbar beste und damit aufwändigste Maßnahme.

Das BSI hat Standards entwickelt, die eine wirkungsvollen technische und organisatorische Datensicherheit und damit den Datenschutz zum Inhalt haben.:

• BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)
• BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
• BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
• BSI-Standard 100-4: DRAFT: Notfallstandard

Neben den BSI-Standards sind weitere z.B. British Standard BS 7799, den es auch als ISO 17799 gibt, entwickelt worden.

Die Standards haben zunächst einmal den rechtlichen Charakter von Empfehlungen. Sie können aber durch die Aufnahme in ein gesetzliches Regelwerk z.B. durch eine Aufnahme in eine verwaltungsinterne Richtlinie[4], Rechtsverordnung[5] oder in die Satzung einer Universität verbindlich werden. Die BSI-Standards eigenen sich ferner als juristische Auslegungsrichtlinie für die Frage des anzulegenden Sorgfaltsmaßstabs bei einem Rechtsverstoß gegen das Datenschutzgesetz. Durch die Einhaltung dieser Standards ist es möglich, ein Zertifikat zu erlangen. Ein solches kann sich bei der Begründung eines Fördermittelantrages als Teilnachweis für die Leistungsfähigkeit der Einrichtung als nützlich erweisen.

Geht es um elektronisch verarbeitete Daten, so ist Ziel der Netzsicherheit ein möglichst umfassender Systemdatenschutz, d.h. auf eine Gefährdung wird automatisch reagiert. Wichtig dabei ist, dass das System zielgerecht erkennt, wann tatsächlich eine Gefährdung vorliegt und wann ein erlaubter Arbeitsvorgang. Ein System, dass die vorgesehenen Arbeiten blockiert, anstatt sich auf die relevanten Gefährdungen zu konzentrieren, ist wegen mangelnder Usability kein Sicherheitssystem, sondern ein unnötiges Ärgernis. Im Ergebnis hat die Netzsicherheit zu gewährleisten, dass ein Schutz durch Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle vorgenommen wird und Unberechtigte keinen Zutritt zum System haben.

Zu den Kerneinheiten eines Sicherheitskonzepts für eine System, dass aus einem Netzwerk besteht oder mit einem Netzwerk z.B. Internet verbunden ist, ist eine leistungsstarke und flexible Firewall. Wiederum zentraler Punkt hier ist die Definition der Filterregeln. Wie diese aussehen, hängt von verschiednen Faktoren wie notwendige Sicherheitsstufe, Art und Struktur der Daten, Arbeitsvorgängen bei der gestatteten Abfrage etc. ab.

Hauptgruppe	Personalisierungsgrade und Nutzungsrechte
Walk-in-user / Gast	Nutzer ohne persönliches Profil, eingeschränkte Rechte
Registrierter Benutzer	Nutzer hat ein persönliches Profil, erweiterte Nutzungsrechte
Administrator	Nutzer hat ein persönliches Profil und ist mit umfassenden Rechten ausgestattet, kann selber Rechte vergeben

4 Z.B. Leitlinie zur Gewährleistung der IT-Sicherheit in der Landesverwaltung Brandenburg (IT- Sicherheitsleitlinie) - Runderlass der Landesregierung, Az.: 653/07, vom 2. Oktober 2007

5 Z.B. § 3 Passdatenerfassungs- und Übermittlungsverordnung

Die Sicherheitsstandards richten sich nach dem Grad der möglichen Individualisierung der Daten. Hierfür kann die gleiche Einteilung wie für die Rechtevergabe verwendet werden. Das Grundgerüst besteht aus den drei Hauptgruppen: dem Walk-in-user/Gast, dem registrierten Benutzer und dem Administrator. In vielen Einrichtungen wird dieses Schema vor allem in der Hauptgruppe registrierte Benutzer weiter unterteilet.

Anforderung an eine gute Datenschutzerklärung und technische Dokumentation

Im vorliegenden Beitrag ist an mehreren Stellen von der Einhaltung des Transparenzgebots die Rede. Das Transparentsgebot wird durch eine hohe Usability der technischen Dokumentation und Datenschutzerklärung verwirklicht. Sie beinhalten Hinweise in benutzergerechter Sprache, die sachlich richtig, eindeutig und relevant sind. Die sachliche Korrektheit der Erklärung umfasst die Vollständigkeit als auch die technischen und die juristischen Komponenten. An den notwendigen Stellen weist sie die Quellen nach. Im Hinblick auf die Vollständigkeit gilt das Echtheitsgebot – d.h. es erfolgt keine „Bereinigung", um tatsächlich gesammelte Daten zu verheimlichen. Für die rechtlichen Bezüge werden Gesetzesangaben genannt. Werden technische Normen und Standards verwendet, so sind diese ebenfalls zu zitieren. Die Verwendung von Verweisen und Bezugnahmen, z.B. von Gesetzeszitaten ist sinnvoll und notwendig, denn auch eine epische, verwässernde Länge kann die Verständlichkeit trüben. Es ist auf eine Verständlichkeit des Textes zu achten. Die Qualität einer Datenschutzerklärung steigt nicht mit zunehmender Länge.[6] Die verwendeten Formulierungen entsprechen der Zielgruppe. So werden beispielsweise Fachbegriffe aufgelöst oder erläutert. Vorgänge können durch Grafiken veranschaulicht werden. Werden unterschiedliche Zielgruppen mit verschieden umfangreichen Datenverarbeitungskenntnissen angesprochen, so sind die Erläuterungen an der Gruppe mit den geringsten DV-Kenntnissen auszurichten. Ebenso ist eine Teilung der Erläuterungen in eine Kurzform und in zusätzliche Ausführungen denkbar.

Welches Gesetz gilt jetzt?

Um die Handlungsmöglichkeiten und Pflichten im Einzelnen kennen zu lernen, ist es notwendig, alle einschlägigen Rechtsquellen aufzufinden. Im Datenschutzrecht ist die diesbezügliche Lage relativ unübersichtlich. Grundlage des Datenschutzes sind in erster Linie erlassene Rechtsnormen. Daneben wirkt die Rechtsprechung,

6 Schuler in Gehrke; S. 45, S. 50

insbesondere die des Bundesverfassungsgerichts, in erheblichem Maße wegweisend mit.[7]

Zusammenspiel der Gesetze und Rechtsvorschriften

Bei den Rechtsvorschriften können zwei große Unterteilungen vorgenommen werden. Die erste betrifft die Unterscheidung von Datenschutzgesetzen des Bundes und der Länder. Das Bundesdatenschutzgesetz (BDSG) gilt für die öffentliche Hand und private Unternehmen. Dagegen gelten die Landesdatenschutzgesetze (LDSG) alleine für die Behörden der Länder. Die meisten Bibliotheken sind kommunale Einrichtungen oder Bestandteile von Einrichtungen der Länder. Für sie gelten die jeweiligen Landesdatenschutzgesetze. Die Landesdatenschutzgesetze sind in aller Regel inhaltlich stark an das Bundesdatenschutzgesetz angelehnt.

Die zweite große Unterscheidung ist zwischen den allgemeinen und den besonderen Datenschutzgesetzen. Zu den allgemeinen Datenschutzgesetzen gehören das Bundesdatenschutzgesetz und die Datenschutzgesetze der Länder. Die besonderen Datenschutzgesetze regeln den Datenschutz für einen spezifischen Bereich. Beispiele hierfür sind das Teledienstdatenschutzgesetz, der Mediendienststaatsvertrag und die hochschuldatenrechtlichen Bestimmungen. Letztere finden sich in den Hochschulgesetzen der Bundesländer. Es besteht ein Anwendungsvorrang der Fachgesetze, z.B. Hochschulgesetz. Das BDSG und die LDSG sind Auffanggesetze und kommen erst dann zum Zug, wenn keine Spezialregelung aus einem Fachgesetz einschlägig ist. Dies wird im Folgenden kurz skizziert:

Wegen den unterschiedlichen Schutzbereichen ist die Unterscheidung der einzelnen Gesetze von Bedeutung. So schützt das BDSG nur personenbezogene Daten natürlicher Personen, nicht hingegen die juristischer Personen. Dagegen umfasst das TKG auch den Schutz juristischer Personen, § 91 Abs. 1 S. 2 TKG.

Trotz seiner häufig nachrangigen Stellung in der Rechtsanwendung hat das BDSG durch seine Vorbildfunktion z.B. für die Landesdatenschutzgesetze eine besondere Bedeutung.

Von einigen wenigen Sondervorschriften abgesehen ist das BDSG inhaltlich sehr generalisierend abgefasst. Dadurch will der Gesetzgeber möglichst alle notwendigen Lebenssachverhalte im Umgang mit personenbezogenen Daten erfassen und vor allem eine unübersichtlichen Fallsammlung vermeiden. Das BDSG befasst sich nur mit der Nutzung personenbezogener Daten. Deren Begriffsbestimmung findet sich in § 3 Abs. 1 BDSB und § 3 Abs. 9 BDSG.

„§ 3 BDSG
(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)…

7 BVerfGE 65, 1 ff. (Volkszählung); BVerfG, NVwZ 2007, 688 (Videoüberwachung)

(9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben."

Das BDSG ist ein Verbotsgesetz mit Erlaubnisvorbehalt, d.h. es wird eine ausdrückliche Erlaubnis nach § 4 Abs. 1 BDSG für die Erhebung, Verarbeitung und Nutzung der Daten benötigt, ansonsten ist die Handlung verboten.

Gemäß § 1 Abs. 3 S. 1 BDSG ist das BDSG gegenüber anderen bundesrechtlichen Datenschutzgesetzen subsidiär. Vorrangig sind: §§ ab § 88 TKG, bestimmte Normen des TMG, Normen über die Einhaltung der Beruf- und Amtsgeheimnisse (§ 1 Abs. 3 BDSG).

Die zentrale Norm § 9 BDSG: umfasst technische und organisatorische Maßnahmen und führt damit den Datenschutz und die IT-Sicherheit zusammen.

Zu den für Bibliotheken besonders wichtigen Spezialvorschriften gehört § 40 BDSG, welcher die Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen zum Gegenstand hat. In Absatz 1 wird die Zweckbindung der Datenverarbeitung und Nutzung an die wissenschaftliche Forschung festgelegt. Unter Beachtung von Absatz 3 (Anonymisierung) ist die Übermittlung der Daten an eine zentrale Einheit im gleichen Hause wie eine Bibliothek möglich. Abgrenzungsfragen tauchen aber dann auf, wenn die Daten an eine nichtöffentliche Stelle (Legaldefinition in § 2 BDSG) übermittelt werden, wie dies bei Kooperationsprojekten der Fall sein kann. § 40 BDSG hat landesrechtliche Entsprechungen z.B. Art. 23 BayDSG.

Parallel zu den gesetzlichen Vorschriften können vertragsrechtlich begründete Vertraulichkeitsregeln vereinbart werden. Dies ist beispielsweise bei Auftragsrecherchen der Fall. Hier erfolgt die Mitteilung von personenbezogenen Daten durch den Kunden nicht zu Veröffentlichungszwecken, sondern nur als Mittel, um weiterforschen zu können. Trotz der Brisanz mancher Mitteilungen werden Bibliothekare damit nicht zu Berufsgeheimnisträgern, sie sind vielmehr vertraglich gebunden. Die vertragliche Bindung genügt nicht, um ein Zeugnisverweigerungsrecht zu begründen.

Anwendungsbeispiel E-Learning

Am Beispiel des E-Learning-Angebots einer Hochschulbibliothek werden im Folgenden die Wahl der einschlägigen Vorschriften und damit das Zusammenspiel der einzelnen Gesetze demonstriert.

Je nach Schwerpunkt der einzelnen Funktionalitäten werden E-Learning-Lernumgebungen als Lern-Management- oder als Content-Management-System bezeichnet. Mit Lern-Management-Systemen können Lerninhalte in einer Datenbank verwaltet und Lernenden zur Verfügung gestellt werden. Abhängig von der Ausgestaltung können verschiedene rechte- und rollenabhängige Zugangsmög-

lichkeiten bestehen, die von einem Administrator verwaltet werden.[8] Content-Management-Systeme sind komplexe Redaktionssysteme zum Erstellen und Administrieren von Onlineinhalten. Zentrales Merkmal ist dabei die strenge Trennung von Inhalt und Layout.[9] Viele E-Learning-Umgebungen sind sowohl Lern- als auch Content-Management-Systeme. Nach dem ausdrücklichen Willen des Gesetzgebers soll die Benutzung soweit möglich anonym oder zumindest pseudonym erfolgen.[10] Ist eine Datenerhebung nicht zu vermeiden, so hat der Anbieter seinen zahlreichen Unterrichtungspflichten nachzukommen.[11]

Die meisten Hochschulen sind als Einrichtungen der Länder mit der Rechtsform Körperschaften öffentlichen Rechts. Damit ist der generelle Anwendungsbereich für das allgemeine Landesdatenschutzgesetz eröffnet. Die Landesdatenschutzgesetze können auf Grund einer ausdrücklichen Nennung für bereichsspezifische Regelungen[12] des Bundes- oder Landesrechts subsidiär sein. Ein vorrangig zu berücksichtigendes Gesetz könnte das Teledienstedatenschutzgesetz (TDDSG) sein. Ziel einer E-Learning-Plattform in der Bibliothek 2.0 ist der interaktive Austausch. Damit liegt eine Individualkommunikation im Sinne von § 2 Abs. 2 Nr. 1 Teledienstegesetz (TDG) und damit ein Teledienst vor. Jedoch ist das E-Learning-Angebot der Hochschulbibliothek der Hochschule als Dienstleister zuzurechnen. Spätestens hier ist eine Trennung zwischen Angehörigen der Hochschule und Externen vorzunehmen. Zunächst sollen die Angehörigen der Hochschule betrachtet werden. Die Nutzung durch die Studierenden findet nicht auf Grund eines Vertrages, sondern im Rahmen ihrer Mitgliedschaftsrechte statt. Mangels Vertrages kommt das Teledienstedatenschutzgesetz daher nicht zur Anwendung. Als vorrangig zu berücksichtigende Norm kommen ferner Vorschriften des jeweiligen Hochschuldatenschutzrechts in Betracht. In diesen wird festgelegt, in welchem Umfang und zu welchem Zweck Daten an einer Hochschule auf Grund des Mitgliedschaftsverhältnisses erhoben werden können. Ohne eine entsprechende Rechtsgrundlage dürfen im Rahmen des Mitgliedschaftsverhältnisses keine Daten erhoben oder verarbeitet werden. In den Hochschulgesetzen der Länder wird festgelegt, welche Daten bei der Immatrikulation zu erheben sind. Zu prüfen ist, ob und wenn ja, inwieweit diese Daten einer Zweckbindung unterliegen. Besteht eine solche und wird eine Verarbeitung zum Zwecke der Teilnahme an E-Learning-Veranstaltungen nicht gedeckt, so dürfen die Daten auch nicht auf Grund des Mitgliedschaftsverhältnisses verwendet werden.[13] Als Ausweg bleibt eine vertragliche Vereinbarung mit den Angehörigen der Hochschule, wie sie auch mit Externen getroffen werden kann. In diesen Fällen richtet sich eine zulässige

8 Flisek, Christian: Datenschutzrechtliche Fragen des E-Learning an Hochschulen, CR 2004, 62, 63

9 Flisek, 2004, S. 62, 63

10 §§ 4 Abs. 6 TDDSG und 18 Abs. 6 MDStV; Flisek, 2004, S. 62, 63

11 §§ 4 Abs. 1 TDDSG und 18 Abs. 1 S. 1 MDStV

12 Z.B. Art. 2 Abs. 7 BayDSG

13 Beispielsweise wird in der Literatur Art. 58 Abs. 6 S. 2 BayHSchG aus verschiedenen Gründen nicht als hinreichende Ermächtigungsgrundlage gesehen: Flisek, 2004, S. 62, 67; wegen den Auslegungsproblemen siehe auch Kundenwünsche und Konfliktmanagement

Datenerhebung nach dem Teledienstedatenschutzgesetz. Welcher Weg für welche Dienstleistung rechtlich zulässig ist, ist vor der Aufnahme des Service zu prüfen und gegebenenfalls mit dem Datenschutzbeauftragten abzusprechen. Durch diese Absprachen können Klagen zwar nicht ausgeschlossen werden. Durch einen gemeinsamen Standpunkt können aber viele Fragen und Beschwerden bereits im Vorfeld erledigt werden, bevor sie sich zu öffentlichkeitswirksamen Schwierigkeiten entwickeln.

Darüber hinaus gibt es bei Pilot- oder Großprojekten gemeinsame Papiere oder Absprachen zwischen den einzelnen Datenschutzbeauftragten. Diese betreffen regelmäßig die Auslegung einer gesetzlichen Vorschrift für einen exemplarischen Fall. Die Bindungswirkung dieser Absprachen ist von der jeweiligen Ausgestaltung abhängig. Zumindest bieten sie aber ein gutes Argument bzw. Entscheidungshilfe. Da diese nicht immer oder häufig erst spät veröffentlicht werden, ist es ratsam sich bei dem jeweiligen Datenschutzbeauftragten nach dem Bestehen von einschlägigen gemeinsamen Standpunkten und Absprachen zu erkundigen.

Gesetzeskonkurrenz

Durch ein- und denselben Sachverhalt können mehrere Gesetze tatsächlich oder auch nur vermeintlich betroffen sein. Wichtig ist, dass bei der ersten Sammlung der einschlägigen Vorschriften alle in Betracht kommenden Normen erfasst werden. Das genauere (Aus-)Sortieren ist erst der nächste Schritt. Die verbleibenden Normen werden dann geordnet. Dabei stellt sich heraus, dass einige Normen nebeneinander bestehen können und sich andere gegenseitig ausschließen (Gesetzeskonkurrenz). Neben den Datenschutzgesetzen des Bundes und der Länder sind die einzelnen Durchführungsvorschriften, das Urheberrecht, das Telekommunikationsgesetz und vor allem das Grundgesetz zu beachten.

Fall: Hochschullehrer H will Auszüge aus einem urheberrechtlich geschützten Werk in seinen elektronischen Semesterapparat einstellen. Er möchte weder gegen das Datenschutzrecht (Grundsatz der Datensparsamkeit) noch gegen das Urheberrecht verstoßen.

Lösungsskizze: Die Schrankenregelung § 52a UrhG (Öffentliche Zugänglichmachung für Unterricht und Forschung) lässt das Einstellen von urheberrechtlich geschützten Materialien unter der Bedingung zu, dass das Angebot nur einem „bestimmt abgegrenzten Kreis von Unterrichtsteilnehmern öffentlich zugänglich" ist. Daher wird er mit der Zugangskontrolle personenbezogene Daten erheben und verarbeiten. Dies wird auch von § 4 Abs. 1 BDSG bzw. das betreffende LDSG ausdrücklich gestattet. Denn § 52a UrhG ist eine gesetzliche Anordnung zur Datenverarbeitung i.S.v. § 4 Abs. 1 BDSG. Aus datenschutzrechtlicher Sicht bestehen gegen das Vorhaben keine Bedenken.

Fall: Bibliothekarin B unterrichtet Informationskompetenz in einer blended-learning-Form. Die E-Learning-Strecke enthält auch elektronische Übungsaufgaben, deren Lösungsversuche gespeichert werden und von den jeweiligen Studie-

renden selbst oder durch die Kursleiterin eingesehen werden können. Ist B die Einsichtnahme zu Kontrollzwecken ohne weiteres gestattet? Die betreffenden Studien- und Prüfungsordnung machen keinerlei Aussagen zum Einsatz elektronischer Datensammlungen.

Lösungsskizze: Der Lehrenden steht es zu, den Leistungsstand der Lernenden zu überprüfen. Dies kann auch in einer elektronischen Form geschehen. Dem Lernenden ist aber zu erkennen zu geben, dass seine Leistungen gerade überprüft werden. Eine heimliche Leistungskontrolle stellt einen besonderen Eingriff dar, der besonders zu rechtfertigen ist. Daher ist in die Studien- und Prüfungsordnungen aufzunehmen, dass Prüfungen bzw. Leistungskontrollen auch in elektronischer Form stattfinden. Der Studierende soll die Möglichkeit haben, vor der Wahl des Kurses bzw. Faches wissen zu können, wann und wo von ihm personenbezogene Daten verarbeitet werden. Zur Ermittlung des Kenntnisstandes ist ein heimliches Vorgehen nicht erforderlich und verstößt daher gegen das Übermaßverbot. Die heimliche Datenauswertung ist rechtswidrig und zu unterlassen.

Internationaler Datenschutz

Internationale Kooperationen zwischen Informationseinrichtungen oder ein Wissenschaftler, der sich gerade im Ausland befindet, aber den Service seiner Bibliothek nutzen möchte, sind nur zwei von vielen Beispielen von grenzüberschreitenden Serviceleistungen einer modernen Bibliothek. Damit findet Datenaustausch nicht nur auf nationaler Ebene, sondern international statt. Der Datenschutz ist längst zu einem Thema in der EU geworden. Neben der bestehenden Datenschutzrichtlinie[14] sind künftig auch weitere gemeinschaftsrechtliche Regelungen zu erwarten.

Kommt es zu einem Datenaustausch über Staatsgrenzen hinweg, so ist darauf zu achten, welche Länder davon betroffen sind. In den meisten europäischen Staaten gilt das „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten“ und das „Zusatzprotokoll zum Europäischen Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitenden Datenverkehr“[15]. Bei einem Datenaustausch zwischen den Vertragsstaaten sind die Datenschutzgesetze des Staates anzuwenden, an dem die verarbeitende Stelle ihren Geschäftssitz hat.

14 Richtlinie (EG) Nr. 46/95 des Europäischen Parlaments und des Rates vom 24.10.1995, Abl. EG L 281/31 vom 23.11.1995. Dennoch ist das faktische Schutzniveau zwischen den einzelnen Mitgliedsstaaten nach wie vor von erheblichen Unterschieden geprägt. Zuletzt ist das Vereinigte Königreich (Regulation of Investigatory Powers Act 2000) massiv in die Kritik geraten. http://www.heise.de/newsticker/meldung/EU-Kommission-will-Datenschutz-in-Grossbritanniendurchsetzen-847192.html Zuletzt besucht am: 10.05.2010

15 Zusatzprotokoll vom 8.11.2001, BGBl. 2002 S. 1887, in Kraft getreten am 01.07.2004, auch für die Bundesrepublik Deutschland

Anders hingegen die Lage, wenn es sich um Datenschutzfragen handelt, bei denen ein Nichtvertragsstaat im obigen Sinne betroffen ist. Hier wird unterschieden, wo die Datenverarbeitung stattfindet. Liegen Geschäftssitz und Datenverarbeitung außerhalb des Vertragsgebietes, so wird auch nur das Datenschutzrecht des fremden Staates angewandt. Erfolgt hingegen die Datenverarbeitung über Rechner, die in Deutschland stehen, so wird auf den Standort des Rechners abgestellt. Mithin kommt deutsches Datenschutzrecht zur Anwendung. Ebenfalls kommt bundesdeutsches Datenschutzrecht zur Anwendung, wenn sich der Geschäftssitz in Deutschland befindet, die Datenverarbeitung aber außerhalb des Vertragsgebietes erfolgt.

Hinzuweisen ist ferner auf § 4b Abs. 3 BDSG. Danach dürfen Daten nur an Länder außerhalb der EU weitergegeben werden, wenn hier ein „angemessenes Schutzniveau“ sichergestellt ist.

Neuralgische Punkte in der Bibliothek 2.0

Kundenwünsche

Zentrum der Bibliothek 2.0 ist der Kunde mit seinen Informationswünschen. Der Service ist bestmöglich individualisiert. D.h. um eine Massenversorgung mit Informationen zu gewährleisten, sind die Angebote grundsätzlich gruppenbezogen angelegt. Tritt nun ein konkreter Kundenwunsch auf, so werden die einschlägigen vorhandenen Angebote - so weit möglich - individualisiert. Bei der Individualisierung der Serviceleistungen werden personenbezogene Daten erzeugt und verarbeitet. Die Bibliothek 2.0 achtet den Kunden und dessen Datenhoheit. Wenn der Kunde sein Nutzenmaximum in einem zwar nur durchschnittlichen Serviceangebot, aber in einem hohen Maß an Achtung seiner Privatsphäre sieht, besteht kein Grund, Serviceleistungen aufzudrängen. Ein solches Verhalten verringert den persönlichen Nutzen und ist organisatorisch eine Verschwendung. Es ist denkbar, dass ansonsten ein an sich wichtiger Aufsatz zu seinem Thema nicht gefunden würde. Jedoch liegt die Entscheidung der Auswahl eindeutig beim Kunden. Vorzugswürdig ist es daher, den Service an einer leicht erkennbaren Stelle, dennoch nicht aufdringlich, anzubieten. Ziel ist die Optimierung der Informationssuche des Kunden unter Beachtung seiner persönlichen Ziele und keine besserwisserische Belehrung. Es geht in erster Linie um die Kundenorientierung und nicht um eine Perfektionierung der Leistungsmöglichkeiten. Letztere können für die Erlangung des Hauptziels hilfreich sein, sind aber nicht dieses selbst.

Die Bibliothek 2.0 versteht sich als innovative Einrichtung. Werden neue Serviceleistungen entwickelt, die personenbezogene Daten verarbeiten, so werden sie unter Beachtung des Datenschutzes nach dem Maximalprinzip ausgerichtet. Aus-

gangslage ist der Stand des Rechts.[16] Juristische Vorhaben mit hoher Erfolgsaussicht können ebenfalls bereits angemessen berücksichtigt werden.[17] D.h. innerhalb der erlaubten Datenverarbeitung entsteht mit dem Schritt über die bisherigen Grenzen hinweg das maximal Mögliche – eine neue Dienstleistung. Mit einer definierten Datenmenge, deren Verwendung zugestimmt wurde, wird ein Höchstmaß an Dienstleistungen angeboten. Ist für weitergehende Dienstleistungen ein Mehr an Daten erforderlich, so erfolgt eine ausdrückliche Nachfrage. Der Kunde besitzt die Autonomie, die Löschung seiner Daten aus einer höheren Dienstleistungsstufe zu verlangen und dadurch wieder auf ein einfacheres und unpersönlicheres Serviceniveau zurückzukommen. Beispielsweise ist ihm datenschutzrechtlich jederzeit die Austragung aus einer Servicegruppe zu gestatten. Das spiegelbildliche Verfahren, das Vorgehen nach dem Minimalprinzip (Grundsatz der Datenvermeidung) ist bei der datenschutzrechtlichen Optimierung von bestehenden Serviceleistungen anzuwenden.

Um das Ziel eines kundenorientierten Servicebetriebs zu erreichen, sind die Kunden an der Umsetzung zu beteiligen. Die Partizipation von späteren Kunden ist mehr als nur eine vage Idee, um die Usability zu verbessern, sondern wird in DIN EN ISO 13407 (1999) bereits ausdrücklich gefordert. Die Einbeziehung späterer Kunden kann in verschiedener Art und Weise erfolgen. In jedem Fall bedeutet die Einbeziehung der Benutzer und die damit verbundene Personalisierung auch und gerade sowohl die Einbeziehung der Userdaten als auch der Interessen der User wie Datenschutz. Diese zum Teil gegensätzlichen Interessen gilt es mit denen der betroffenen Informationseinrichtung gesetzeskonform in Zielrichtung eines bestmöglichen Services in Einklang zu bringen.

Fragen zu Informationen, die über die notwendigen Bestandsdaten einer Dienstleistung hinausgehen, müssen eindeutig als freiwillig gekennzeichnet sein. Dabei ist der Dienstleistungszweck eng auszulegen. Eine Dienstleistung ist eine in sich abgeschlossene Einheit. Es widerspricht dem Datenschutz, wenn Dienstleistungsbündel von deutlich unterschiedlichem Bestandsdatenniveau geschnürt werden – vor allem, wenn sie den Zweck haben, durch einen einheitlichen Zugang den Datenschutz unnötig aufzuweichen. Eine fortschrittliche Servicearchitektur bündelt inhaltlich zusammengehörende Dienstleistungen, die dasselbe Niveau von personenbezogenen Bestandsdaten aufweisen, in einer ansprechenden Art und Weise.

16 Als Maßstab für die Auslegung bestehender Rechtsnormen ist die Auffassung des EuGH, des Bundesverfassungsgerichts, des Bundesgerichtshofs und die sonstige ständige Rechtsprechung zu wählen. Aus Verantwortung und Loyalität gegenüber dem Dienstherrn und dem Finanziers sowie dem Ansehen der Einrichtung, sollten auch angenehm erscheinenden Meinungen in der Literatur erst dann in der Praxis gefolgt werden, wenn diese abgesichert sind.

17 Bereits unsicherer, für langfristige Planungen gleichwohl interessant sind: Gesetzesvorhaben mit Erfolgsaussicht, offizielle Stellungnahmen von Ministerien, eindeutige Stellungnahmen von Personen, deren Einfluss auf wesentliche Gremien besteht (z.B. Generalanwalt am EuGH, Vors. Richter am BVerfG oder BGH, Bundesdatenschutzbeauftragter)

Anonymität

Zu den Kernthemen des Datenschutzes gehört die Frage, was ist anonym und was nicht. So können beim Erfassen von Daten über Handlungen einer Gruppe personenbezogene Daten vorliegen, wenn ein Personenbezug herstellbar ist. Die Frage, ab welcher genauen Gruppengröße ein Personenbezug möglich ist, kann nur im Einzelfall bestimmt werden. Die Rechtsprechung umfasst derzeit lediglich Einzelfallentscheidungen, durch die Kleingruppen von drei bis sieben Personen noch als personenbezogen eingestuft werden.[18]

Am Anfang dieses Kapitels wurde von einer individuellen Bibliothek und individualisierten Dienstleistungen gesprochen. Daher sieht eine Auseinandersetzung mit dem Thema Anonymität zunächst widersprüchlich aus. Jedoch unterfallen Daten zu Personengruppen, die nicht einer einzelnen Person zugerechnet werden können, nicht dem Datenschutzrecht. Entsprechende anonyme statistische Datenerhebungen sind daher ohne besondere datenschutzrechtliche Einwilligung möglich. Soweit keine besondere gesetzliche Erlaubnis für die Verwendung personenbezogener Daten besteht, bedeutet die Anonymisierung die einzige zulässige Nutzungsmöglichkeit. Ansonsten kommt die Bereitstellung dieser Informationen zur Nutzung nicht in Frage.

Daher lautet die Gretchenfrage, ob es sachlich wirklich erforderlich und nicht nur interessant oder „ganz praktisch" ist, dass der genaue Name des Benutzers und die damit verbundenen Daten bekannt sind. Für viele Serviceleistungen genügt es, wenn lediglich die aktuell vorhandene Nutzungsberechtigung bekannt ist.

Was rechtlich unter Anonymisieren als Vorgang zu verstehen ist, ist in § 3 Abs. 7 BDSG legal definiert. Danach ist „anonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können." Welche Methoden genau erforderlich sind, hängt sowohl vom Datenbestand als auch vom Umfang einer allgemeinen Kenntnis über den Dateninhalt ab.[19] Erwartet wird, dass bei der Anonymisierung der aktuelle Stand der Technik mindestens erreicht wird. Dagegen ist aber auch anerkannt, dass sich eine absolute Anonymisierung regelmäßig nicht erreichen lässt. Eine relative bzw. faktische Anonymisierung ist ausreichend.[20]

Im Gegensatz zur landläufigen Meinung gelten IP-Nummern insgesamt nicht als anonyme Daten, sondern im Sinne des Teledienstdatenschutzgesetzes (TDDSG) als „Pseudonyme".[21] Die generalisierende Begründung hierfür ist, dass

18 Speichert, Horst: Praxis des IT-Rechts, S. 124

19 Tinnefeld et. al., 2005: 3.1.2

20 BVerfG, NJW 1987, 2805, 2807; NJW 1988, 962, 963

21 Vgl. Vorlage der Hessischen Landesregierung für den 13. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz nicht öffentlichen Bereich in Hessen zuständigen Aufsichtsbehörden vom 30. August, Ders. 15/1539, 9.1: http://starweb.hessen.de/cache/DRS/15/pdf/9/1539.pdf zuletzt besucht am: 10.05.2010

statische IP-Nummern im Gegensatz zu dynamischen IP-Nummern einer natürlichen Person zugeordnet werden.

Datenschutz für Mitarbeiter

Geht es um eine Individualisierung des Services, so sind beide Seiten der Dienstleistung datenschutzrechtlich zu betrachten. Auf der anderen Seite des Dienstleistungskanals sitzt ein Mitarbeiter der Bibliothek mit eigenen datenschutzrechtlichen Interessen. Neben der Frage nach dem Umgang mit den Benutzerdaten ist daher der Schutz der Mitarbeiterdaten ein weiteres Kerngebiet des Datenschutzes innerhalb einer Bibliothek und Informationseinrichtung.

Der Schutz der persönlichen Daten des Arbeitnehmers wird zweifach abgesichert:

Zum einen durch den individualrechtlichen Schutz, der dem Arbeitnehmer zum Arbeitgeber beim Umgang mit personenbezogenen Daten durch das BDSG bzw. LDSG zusteht.

Zum anderen wird der Schutz mittels kollektivrechtliche Vereinbarungen zum Arbeitnehmerdatenschutz in Tarifverträgen, Betriebs- oder Dienstvereinbarungen (§ 4 Abs. 1 BDSG) gewährleistet. Grundlage hierfür sind die Beteiligungsrechte von Personal- bzw. Betriebsräten.

Die informationellen Beteiligungsrechte des Betriebsrates sind u. a. im Betriebsverfassungsgesetz, des Personalrates im Bundespersonalvertretungsgesetz bzw. in den Landespersonalvertretungsgesetzen geregelt. Bundespersonalvertretungsgesetz und Betriebsverfassungsgesetz weisen starke Parallelen im Hinblick auf den Datenschutz auf. So ist es nach § 68 Abs. 1 Nr. 2 BPVG Aufgabe des Personalrates, die Einhaltung des Datenschutzes bei der Verarbeitung personenbezogener Daten zu überwachen. Zur Durchführung dieser Aufgabe steht dem Personalrat ein Informationsrecht gem. § 68 Abs. 2 Nr. 1 BPVG zu. Mitbestimmungsrechte bestehen beispielsweise zu den Inhalten von Personalfragebögen (§§ 75 Abs. 3 Nr. 8, 76 Abs. 2 Nr. 1), bei Beurteilungsrichtlinien (§§ 75 Abs. 2 Nr. 3, 76 Abs. 2 Nr. 8), bei Erlass von Auswahlrichtlinien (§ 76 Abs. 2 Nr. 8) und bei der Einführung und Anwendung technischer Einrichtungen, welche geeignet und bestimmt sind, Verhalten oder Leistung der Beschäftigten im öffentlichen Dienst zu überwachen (§ 75 Abs. 3 Nr. 17).[22]

Bei einer Veröffentlichung von Mitarbeiterdaten, die über die reine dienstliche Tätigkeit hinausgehen, ist streng zwischen bibliotheksinternen Intranet und dem weltweitzugänglichen Internet zu unterscheiden. Dies gilt auch dann, wenn es zuvor gedruckte Briefbögen, Prospekte etc. gab. Wegen den besonderen datenschutzrechtlichen Risiken ist von einem generellen Verbot einer Veröffentlichung von Mitarbeiterdaten, die über die reine Diensterfüllung hinausreichen, auszuge-

22 BVerwG, NJW 1986, 526

hen.[23] Vor der Veröffentlichung von Mitarbeiterdaten im Internet ist daher deren Einverständnis gem. § 4 Abs. 1 BDSG einzuholen. Daneben können weitere Normen einschlägig sein. Beispielsweise ist eine Vorstellung des Mitarbeiters mit Bild im Internet[24] wegen § 23 KUrhG nur mit ausdrücklicher Zustimmung des Mitarbeiters möglich.

Nach Auffassung des Bundesdatenschutzbeauftragten ist eine Veröffentlichung von Mitarbeiterdaten ohne deren ausdrückliche Einwilligung nur soweit zulässig, als es zur Aufgabenerfüllung erforderlich ist.[25] Hierzu gehören die Benennung der zuständigen Ansprechperson sowie deren Erreichbarkeit. In den übrigen Fällen ist eine ausdrückliche und freiwillige Einwilligung erforderlich. Für die Einwilligung ist nach § 4 Abs. 2 S. 2 grundsätzlich Schriftform erforderlich.

Datenweitergabe innerhalb der gleichen öffentlichen Stelle

Werden Daten innerhalb einer öffentlichen Stelle z.B. von der Bibliothek zur Personalabteilung weitergegeben, so liegt darin keine Übermittlung (§ 15 Abs. 6 BDSG). Eine Übermittlung setzt eine Bekanntgabe der Daten an einen Dritten (§ 3 Abs. 5 S. 2 Nr. 3 BDSG) voraus. Die einfache Datenweitergabe unterliegt weniger Restriktionen als eine Datenübermittlung. Dies gilt aber nur für die unmittelbare Weitergabe. Wird hingegen eine externe Stelle z.B. ein privater Servicedienstleiter zwischengeschaltet, so liegt eine Datenübermittlung von der öffentlichen Stelle an ein Privatunternehmen und von diesem wiederum an eine öffentliche Stelle vor. Daher ist auch der Datenschutz ein Grund, das zeitweise[26] als modern gepriesene Outsourcing von Dienstleistungen im Bereich der Datenverarbeitung umfassend zu überdenken. Unter Umständen ist es dem externen Dienstleister nicht oder nur mit höherem Aufwand rechtlich möglich, die gleiche Leistung zu erbringen.

Logfiles und ihre Verwendung

Bei der Logfileanalyse wird eine Logdatei über einen bestimmten Zeitraum nach bestimmten Kriterien untersucht. Damit kann der allgemeine Erfolg einer Webseite ermittelt werden. Die Logfileanalyse erlaubt, festzustellen, mit welcher Häufig-

23 Beispiel für eine der eng umgrenzten Ausnahmen: LG München I, Urt. 10.09.2003, Az: O 13848/03, MMR 2004, 499 (Geschäftsführer-Adresse im Internet)

24 Im dienstinternen Intranet ist hingegen keine Einwilligung rechtlich erforderlich - gleichwohl sehr sinnvoll. Näher hierzu: Tinnefeld, MMR 2001, 797, 800

25 Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (1999/2000), Kap. 18.10, http://www.bfd.bund.de/informationen/tb9900/kap18/18_10.html. Zuletzt besucht am: 10.05.2010

26 Ein Blick in die Wirtschaftsgeschichte zeigt einen regen und regelmäßigen Wechsel von In- und Outsourcingtendenzen.

keit und in welcher Art und Weise ein Webangebot genutzt wird. Die Logfileanalyse wird sowohl für wissenschaftliche als auch für kommerzielle Zwecke eingesetzt. Die Logfileanalyse ist demnach ein Evaluationsinstrument. Mit ihr ist es möglich, zielgerichtet den Ressourceneinsatz für vielbesuchte Webseiten zu erhöhen und Änderungen von wenig besuchten Webseiten bis hin zu deren Löschungen zu betreiben. Sie ist damit generell geeignet, durch die Verwendung der erhaltenen Verlaufsdaten zur Steuerung und damit zur Verbesserung des Services beizutragen. Die Entscheidung, welche Daten des Kunden aufgezeichnet werden, liegt regelmäßig beim Webmaster. Diese Daten sind häufig: IP-Adresse, angefragte URL, Zugriffszeitpunkt und die übertragene Datenmenge. Somit ist festzuhalten, dass die Speicherung der Logfiles ganz bewusst eingerichtet wird. Denn http ist an sich ein zustandsloses Protokoll. Sobald der Webserver die Frage des Browsers beantwortet hat, löscht er den Vorgang. Mittels des Einsatzes von Cookies bzw. Session-IDs kann dennoch eine Identifikation des Benutzers erfolgen.

Personenbezogene Daten eines Nutzers dürfen gemäß § 15 Telemediengesetz nur erhoben und verwendet werden, soweit es für die Inanspruchnahme von Telemedien erforderlich ist, um den Dienst als solchen und die Abrechnung zu ermöglichen. Ist der Nutzungsvorgang beendet, dürfen Nutzungsdaten nur zu Abrechnungszwecken gespeichert werden. Eine weitergehende Protokollierung ist grundsätzliche unzulässig. Die IP-Adresse ist vielmehr zu löschen. Eine Ausnahme gilt für den Fall, dass der Nutzer vorher, freiwillig einer Speicherung zugestimmt hat.

Testarchive

Zu Beweiszwecken und um aufwendige Neuerhebungen zu sparen, ist die dauerhafte Nutzung von Testarchiven für viele Wissenschaftler ein wichtiges Werkzeug. Gerade in den Bereichen Medizin, Psychologie und Soziologie enthalten die Rohdaten sehr persönliche Informationen über die Probanden. Werden diese Testarchive Bibliotheken angeboten, stellt sich die Frage, ob die Datenbestände übernommen werden können und sollen. Die Übernahme von Testarchiven in den Bestand einer Bibliothek bedeutet eine Neubewertung der Datensicherheit innerhalb der Bibliothek. Davon umfasst ist sowohl die eigentliche Nutzung des Archivs als auch die Anbindung des Archivs an eine zentrale Serviceeinheit. Keiner aktuellen Neubewertung bedürfen hingegen Vorgänge, die mit der Nutzung des neuen Archivs in keiner Verbindung stehen. Vor der Übernahme des Archivs ist sicherzustellen, dass der Archivbestand den datenschutzrechtlichen Bestimmungen entspricht. So müssen notwendige Anonymisierungen bereits vorgenommen worden sein. Der Inhalt der Einwilligungserklärung ist auch für die Bibliothek bindend. Die Öffnung eines solchen Archivs für weitere Interessierte oder die Entwicklung neuer Serviceleistungen auf Grund dieser Datenbestände ist nur in engen Grenzen möglich. Sind Fehler bereits beim Aufbau des Archivs erfolgt, so können sich die bisherigen Betreiber sofort um eine Genehmigung durch die Be-

troffenen bemühen. Erfolgt diese nicht, so ist das Archiv zu vernichten und keinesfalls in den Bestand der Bibliothek zu überführen. Datenschutzrechtliche Fehler besitzen eine Fernwirkung. Eine Nichtbeachtung dieser Fernwirkung ist ein organisatorischer Fehler, der neue Ansprüche wegen der Verletzung datenschutzrechtlicher Bestimmungen begründet.

Folgen von IT-Dienstleistungen

Die Fernwartung von Software ist in vielen Bundesländern ausdrücklich in den Landesdatenschutzgesetzen geregelt[27]. In diesen Fällen kommt es auf den Streit um die rechtliche Qualifikation, ob es sich um eine Datenübermittlung oder um eine Datenverarbeitung im Auftrag handelt nicht an.

Werden alte Rechner entsorgt, so sind die auf den Festplatten enthaltenen Daten so zu vernichten, dass sie definitiv nicht mehr auffindbar sind. Dabei ist eine einfache logische Löschung nicht ausreichend. Je nach Brisanz der Daten können unterschiedliche gründliche Vernichtungsverfahren erforderlich sein.[28]

Konfliktmanagement

Der hier vorliegende Beitrag geht davon aus, dass es trotz allem Bemühen keinen technisch und organisatorisch perfekten Datenschutz gibt. Und auch der Idealfall garantiert nicht, dass ein Benutzer der Bibliothek nicht anderer Meinung sein kann. Daher gehört ein entsprechendes Konfliktmanagementkonzept als organisatorische Maßnahme dazu.

Maßnahmen zur Konfliktvermeidung

Wie aber gerade betont, kann durch eine konsequente Umsetzung technischer Maßnahmen für die Einhaltung des Datenschutzes eine Vielzahl von Konflikten verhindert werden. Daher werden hier ausdrücklich die BSI-Standards 100-1 bis 100-4 empfohlen. Die Anwendung kann wie in den Beispielen gezeigt erfolgen:

Zu den organisatorischen Maßnahmen zählt die Belehrungen der Kunden und der Verantwortlichen in der Bibliothek. Einen besonderen und erwähnenswerten Stellenwert hat die Organisation der Zugriffsvergabe. So ist festzulegen, wer in welchem Fall Zugriff auf die persönlichen Daten haben soll. Der Intention des Datenschutzes nach soll es sich dabei um möglichst wenige Personen handeln.

27 Z.B. § 11a Brandenburgisches Datenschutzgesetz

28 Die Einhaltung der gebotenen Sorgfalt ist essentiell. Übertreibungen werden aber damit nicht gerechtfertigt und wirken als Belustigung eher kontraproduktiv. Vgl. Computer Zeitung Nr. 3 vom 15. Januar 1998, S. 1

Hier gibt es aber eine gewisse Flexibilität, die sich an den Anforderungen vor Ort orientiert. So ist eine wirksame Vertretung sicherzustellen. Ebenso sollen arbeitsplatzorganisatorische Fragen wie Job-Rotation nicht mit Datenschutzargumenten blockiert werden. Beispielsweise ist es nicht erforderlich, dass Mitarbeiter aus der Abteilung Medienbearbeitung in der gleichen Art und Weise auf die Datensätze der Bibliothekskunden zugreifen können, wie dies in der Benutzungsabteilung erforderlich ist. Hier ist eine differenzierte Zugriffsrechtevergabe notwendig.

Bedrohung	Sicherheitsmaßnahme
Falsches Personalisieren	Authentifikation von Personen
Beobachten	Anonymitätsverfahren
Verfälschen von Nachrichten	Authentifikation der Nachrichten (digitale Signatur)
Abhören	Verschlüsseln von Nachrichten

Wenn es doch zum Streit kommt…

Ziel der Bibliothek in einem Konfliktfall ist:

- Herstellung des rechtmäßigen Zustands
- Schadensregulierung
- Imagepflege

Mittel für die Zielerreichung ist zunächst die genaue Feststellung der Rechts- und Beweislage. Im Falle eines Schadenseintritts erfolgt in einem weiteren Schritt die Feststellung des Schadensumfangs. Der Schadensumfang betrifft zum einen den Schaden, den das Sicherheitsleck verursacht hat. Für das künftige Auftreten in der Öffentlichkeit ist ferner eine Dokumentation und Abschätzung des Imageschadens erforderlich.

Das Datenschutzrecht kennt eine Fülle von Möglichkeiten, wie Verletzungen des Datenschutzes behandelt werden können. Weitere als die aufgezählten Ansprüche kommen nach den Landesdatenschutzgesetzen sowie nach Sondergesetzen in Betracht:

Zivilrechtliche Schadensersatzansprüche können auf § 7 BDSG und § 280 BGB und §§ 823 ff. BGB gestützt werden.

Für den öffentlichen Bereich hat sich der Gesetzgeber mit § 7 BDSG für eine Gefährdungshaftung entschieden. D.h. es kommt nicht darauf an, ob die öffentliche Stelle schuldhaft (vorsätzlich oder fahrlässig) i.S.v. § 276 BGB gehandelt hat. Für nicht-öffentliche Stellen hat sich der Gesetzgeber auf eine Beweislastregelung in § 8 BDSG beschränkt.

Als sonstige Ansprüche kommen in Betracht:

- Auskunftsanspruch z.B. gem. §§ 19, 34 BDSG
- Berichtigungsanspruch z.B. gem. §§ 20 Abs. 1 35 Abs. 1 BDSG
- Löschungsanspruch z.B. gem. §§ 20 Abs. 2, 35 Abs. 2 BDSG
- Sperrungsanspruch z.B. gem. §§ 20, 35 BDSG

In besonders schweren Fällen kommen ferner ein Ordnungswidrigkeitenverfahren (§ 44 BDSG) oder ein Strafverfahren (§ 43 BDSG) in Betracht.

Ziel der Öffentlichkeitsarbeit in Krisenfällen ist die Glaubhaftmachung, dass spätestens ab sofort alle technischen und organisatorischen Maßnahmen, die erwartet werde konnten, auch getroffen wurden. Eine solche Reaktion kann allerdings erst dann erfolgen, wenn entsprechende Punkte auch tatsächlich umgesetzt wurden. Vor inhaltsleeren Erklärungen mit Vertuschungseffekt wird ausdrücklich gewarnt. Diese schaden dem eigenen Haus. Ferner ist bei Aufklärung und Öffentlichkeitsarbeit darauf zu achten, dass keine neuen Sicherheitslecks erzeugt werden. Ausdrücklich empfohlen wird in Schadensfällen eine enge Zusammenarbeit mit den jeweiligen Datenschutzbeauftragten.

Datenschutz als Serviceleistung der Bibliothek 2.0

Vertrauen in den richtigen Umgang mit Informationen

In welchem Ausmaß eine Serviceleistung angenommen wird, hängt vom Inhalt des Angebots und deren Usabiblity ab. Die Usabiblity ist ein wichtiges praktisches, aber kein rechtliches Argument. Sie kann daher den Weisungen des Datenschutzes nicht entgegengehalten werden. Die Aufgabe für die Serviceleistungen und deren Präsentation lautet daher, dem Datenschutz zu entsprechen und gleichzeitig ein Höchstmaß an Usabiblity zu gewährleisten. Datenschutz und Usability können, müssen aber nicht gegenläufige Interessen haben.

Bildungseinrichtungen genießen tendenziell ein höheres Vertrauen in ihre Glaubwürdigkeit als beispielsweise Wirtschaftsunternehmen.[29] Der Grund für den Vertrauensvorschuss begründet sich in der Unabhängigkeit von Werbe- und Verkaufseinnahmen und der damit verbundenen finanziellen Unabhängigkeit. Dieser Vertrauensvorschuss ist durch entsprechende Maßnahmen zu rechtfertigen und damit auszubauen. Ein sensibles Aktionsfeld ist der Datenschutz. Die allgemeine Erwartung einer besseren Einhaltung des Datenschutzes kann durch positive Maßnahmen gesteigert werden.

29 Die Tendenz in verschiedenen Meinungsumfragen ist eindeutig. Vgl. z.B. Schupp, Jürgen; Wagner, Gert G. Wagner: Wochenbericht des DIW Berlin 21/04: Vertrauen in Deutschland: Großes Misstrauen gegenüber Institutionen http://www.diw.de/sixcms/detail.php/284240#HDR0. Zuletzt besucht am: 10.05.2010; Allensbacher Berichte 2009 Nr. 6: Zu wenig Datenschutz? http://www.ifd-allensbach.de/pdf/prd_0906.pdf. Zuletzt besucht am: 10.05.2010

Hierzu kommen folgende Möglichkeiten in Betracht:

1. konsequenter Verzicht auf jede entbehrliche Datenhaltung
2. Transparenz

Ein hohes Maß an Transparenz wird durch eine konsequente Aufklärung über die jeweiligen Datenerfassungs- und Verarbeitungsschritte erzielt (Transparenz durch Aufklärung). Häufig gehen in der Praxis die Erklärungen in den Erläuterungen zum Datenschutz nicht über den notwendigen Mindeststandard hinaus. Begründet wird dies mit dem Wunsch, sich Probleme und Diskussionen vom Hals zu halten. Durch das Aussparen von weiterreichenden Informationen wird aber auch nicht in diesem Bereich nachhaltig investiert und damit Standards geschaffen. Für eine öffentliche Einrichtung bedeutet eine strikte Beachtung und Forcierung des Datenschutzes eine Ausspielung ihrer Stärken. Marketingmaßnahmen alleine, wie die reine Behauptung, den Datenschutz einzuhalten, genügen jedoch nicht.

Eine inhaltlich fundierte und ausführliche Erläuterung ist treffend formuliert, nicht notwendigerweise aber umfangreich im Wortgebrauch. Denn die Qualität einer Datenschutzerklärung steigt nicht mit zunehmender Länge.[30] Die Transparenz wird dadurch hergestellt, dass die verwendeten Formulierungen der Zielgruppe entsprechen. So werden beispielsweise Fachbegriffe entweder aufgelöst oder erläutert. Vorgänge können durch Grafiken veranschaulicht werden. An den erforderlichen Stellen sind die in der Datenschutzerklärung getroffenen Aussagen zu belegen – beispielsweise durch Normenzitate. Werden unterschiedliche Zielgruppen mit verschieden umfangreichen Datenverarbeitungskenntnissen angesprochen, so sind die Erläuterungen an der Gruppe mit den geringsten DV-Kenntnissen auszurichten. Ebenso ist eine Teilung der Erläuterungen in einen kurzen und in zusätzliche Ausführungen denkbar.

Ein nützliches und verwertbares Informationsmanagement - was die Kernaufgabe von Bibliotheken ist - und ein effektiver Datenschutz haben beide das Vertrauen in den richtigen Umgang mit Informationen als Wurzel. Daher ist der Datenschutz in Informationseinrichtung nicht als ein vorgeschriebenes „Etwas“ zu verstehen, sondern auf Grund des eigenen Selbstverständnisses in die alltäglichen Dienstleistungen zu integrieren. Ziel ist die Rechtfertigung und Steigerung des Vertrauens der Kundinnen und Kunden in den gewährleisteten Datenschutz. Durch das erhöhte Sicherheitsgefühl lassen sich Anteile am Informationsmarkt halten und gewinnen. Auf der Grundlage eines eingestellten hohen Vertrauens in die Sicherheit und Transparenz der Verarbeitung personenbezogener Daten lassen sich weitergehende Projekte erfolgreich(er) durchführen. Aus der zwar freiwilligen, zunächst aber doch als notwendiges Übel angesehenen Datenüberlassung, kann eine bewusste und freiwillige Datenspende zur Unterstützung der Effizienzsteigerung eines Kulturbetriebes werden. Auf dieser Basis steigt auch die Akzeptanz von neuen und weiteren Angeboten der Bibliothek. Das Schaffen von Standards beim Datenschutz sichert zudem einen partiellen Wettbewerbsvorsprung auf

30 Schuler in Gehrke, 2005, S. 45, S. 50

dem Informationsmarkt. In der Wirtschaft hat man den Datenschutz als Mittel der Festigung der Marktmacht und Kundenbindung durch Vertrauen erkannt.[31]

Datenschutz als Thema in der Informationskompetenz

Eine weitere Möglichkeit, ein hohes Maß an Transparenz zu erreichen, ist das Anheben des Kenntnisstandes der Bibliotheksbenutzer (Transparenz durch Schulung). Informationskompetenz umfasst den verantwortungsbewussten Umgang mit Informationen. Dies gilt bei der Informationsbeschaffung, der Informationsverarbeitung als auch beim Hinterlassen eigener Informationen. Ein Datenschutz als Serviceleistung respektiert nicht nur die persönliche Informationshoheit des Einzelnen und weist ihn auf seine Rechte hin, sondern klärt über mögliche Schwachstellen auf und gibt Hinweise zu deren Vermeidung. Das klassische Beispiel hierfür sind Fotos von ausgelassenen Feiern, die im Internet auch für künftige Arbeitgeber abrufbar sind. Die Hinweise können umfangreich sein, finden aber ihre Grenze in der individuellen Rechtsberatung. Letzteres ist nicht Aufgabe der Bibliothek. Die Integration von absichernden Maßnahmen schafft Vertrauen und erhöht damit den Wert des Serviceangebots der Informationskompetenz und damit der dahinterstehenden Einrichtung Bibliothek. Ziel ist es, dass der Kunde qualifiziert entscheiden kann, welches Risiko er für eine Serviceleistung bereit ist einzugehen.

Zusammenfassung und Ausblick

Ein effektiver Datenschutz ist ein Kernbestandteil von fortschrittlichen Informationseinrichtungen. Die Bibliothek 2.0 nimmt das ihr entgegengebrachte Vertrauen an, rechtfertigt es und führt es zu neuen Serviceleistungen. Zentrum der innovativen Dienste ist der in seiner Autonomie respektierte Kunde.

Literaturverzeichnis

(Gehrke, 2005) Gehrke, Gernot (Hrsg.): Datenschutz- und Sicherheit im Internet – Handlungsvorschläge und Gestaltungsmöglichkeiten, Schriftenreihe Medienkompetenz des Landes Nordrhein-Westphalen, Düsseldorf, München, kopaed Verlag, 2005

(Flisek, 2004) Flisek, Christian: Datenschutzrechtliche Fragen des E-Learning an Hochschulen – Lernplattformen im Spannungsfeld zwischen didaktischem Nutzen und datenschutzrechlichen Risiken, CR 2004, 62-69

31 Ulmer in Gehrke, 2005, S. 58, S. 78

(Tinnefeld et. al., 2005) Tinnefeld, Marie-Theres; Ehmann, Eugen; Gerling, Rainer, W.; Einführung in das Datenschutzrecht – Datenschutz und Informationsfreiheit in europäischer Sicht, 4. völlig neubearb und erw. Aufl., München, Oldenbourg Verlag, 2005