e-beratungsjournal.net

2. Jahrgang, Heft 1, Artikel 4 – März 2006

Qualitätsmanagement mit integriertem Datenschutzmanagement bei Online-Beratung

Joachim Wenzel

Zusammenfassung

Qualitätsmanagementkonzepte sind im Bereich wirtschaftlicher Warenproduktion entstanden, wurden später auch auf Dienstleistungen übertragen und finden mehr und mehr Eingang in die Arbeitsabläufe und Prozesse psychosozialer Einrichtungen. Diese Konzepte bedürfen dabei jedoch einer Weiterentwicklung und Spezifizierung auf das jeweilige Arbeitsfeld, wie etwa das der psychosozialen Beratung, wenn sie den vielschichtigen Qualitätsdimensionen dieses komplexen Feldes gerecht werden sollen. Hinsichtlich Online-Beratung kommt die Internettechnik – zusätzlich zum ohnehin bereits komplexen Beratungsprozess – noch als weiterer Bereich hinzu, den es differenziert zu beachten gilt. Die Integration des Datenschutzmanagements in das Qualitätsmanagement von Online-Beratung bietet sich dabei geradezu an, weil so die entsprechenden Prozesse aufeinander abgestimmt werden können. Für angemessenen Datenschutz und Datensicherheit im Internet gilt es dabei zunächst die jeweils für eine Organisation geltenden Normen in den Blick zu nehmen und die gesamte technische Infrastruktur einschließlich Datentransfer durch das ungesicherte Internet konzeptionell einzubeziehen. In der Praxis der Online-Beratung werden manche relevanten Punkte bislang noch nicht angemessen berücksichtigt. Im vorliegenden Artikel sollen deshalb die zentralen Eckpunkte bezüglich Qualität, Datenschutz und Datensicherheit übersichtsartig vorgestellt und in einem Schichtenmodell für Online-Beratung zusammengefasst werden. Dies kann zu einer ersten Orientierung für Verantwortliche in Organisationen dienen, die Qualität, Datensicherheit und Datenschutz von Online-Beratung auf angemessenem Niveau realisieren und sichern wollen.

Keywords

Online-Beratung, Qualität, Datenschutz, Qualitätsmanagement, Datenschutzmanagement, Datensicherheit, Internettechnik, Schichtenmodell

Autor

- Diplom-Pädagoge **Joachim Wenzel**
- Studium der Erziehungswissenschaft an der Universität Mainz mit den Fächern Psychologie, Soziologie und Theologie, Schwerpunkt Erwachsenenbildung
- Systemischer Berater / Therapeut (DGSF), Systemischer Organisationsentwickler / Supervisor (DGSF)
- Seit 1997 Mitglied im hauptamtlichen Leitungsteam der Telefonseelsorge Mainz-Wiesbaden: Aus- und Weiterbildung der Ehrenamtlichen, Beratungsformen: Telefonberatung, face-to-face-Beratung und Mailberatung (http://www.telefonseelsorge.de/)
- 1997 bis 1999 Gesellschaftergeschäftsführer einer Unternehmensberatung, bis 2004 Gesellschafter
- Seit 1997 freiberuflich tätig als Coach, Trainer, Supervisor und Organisationsberater
- 2000: Entwicklung des Konzepts der webbasierten Online-Beratung (Sewecom)
- Seit Ende 2004 Forschungsprojekt zum Themenfeld Online-Beratung an der Universität Mainz
- **Kontakt**: Alexander-Fleming-Str. 29a,
  D-55130 Mainz
  Tel: +49 (0)6131/ 881086
  http://www.systemische-beratung.de/wenzel
  eMail: wenzel@systemische-beratung.de

-

0. Einleitung

Online-Beratung vollzieht sich in einem komplexen Kontext. Die medial vermittelte Kommunikation funktioniert schließlich nur mit Hilfe der Internettechnik. Die Realisierung dieser Form der Beratung benötigt dabei eine Vielzahl technischer Komponenten auf unterschiedlichen Ebenen wie Hardware, Software und Netze. Die Informations- und Kommunikationstechnik hat dabei direkte Auswirkung auf die Qualität der Beratung selbst, da die Ausformung des Beratungsprozesses von der verwendeten Technik mitbestimmt wird. Beim Qualitätsmanagement (QM) der Online-Beratung muss neben den Anforderungen durch die Kunden, Fragen von Ethik und Menschenbild in der Beratung und den fachlichen Fragen die benutzte Technologie im Blick sein, will man die Qualität der Beratung gewährleisten. Dabei gibt es Übereinstimmungen zwischen QM und Datenschutzmanagement (DSM). In beiden Bereichen geht es um die zielgerichtete Steuerung und Verbesserung von Prozessen, die alle beteiligten Personen und technischen Komponenten einbeziehen müssen, um wirksam zu sein. Es bietet sich somit an, das DSM einer Organisation in das QM zu integrieren. Dabei sind allerdings Besonderheiten aufgrund gesetzlicher Vorgaben zu beachten, die das DSM über ein QM hinausgehen lassen.

1. Qualitätsmanagement

Die Einführung von QM-Systemen etwa nach DIN EN ISO 9000ff nimmt auch im Non-Profit-Bereich zu. Dies ist nicht verwunderlich, da die Angebote an Waren und Dienstleistungen immer unüberschaubarer werden und in ihrer konkreten Ausgestaltung einem permanenten Wandel unterworfen sind. Angebot und Nachfrage verändern sich in zuvor nicht gekanntem Ausmaß. Daraus erwächst selbst in einzelnen Marktsegmenten eine Unübersichtlichkeit, die für die Handhabbarkeit des Angebots nach neuen Orientierungsmöglichkeiten sucht, um verlässliche Entscheidungskriterien für die Auswahl unterschiedlicher Angebote zu entwickeln. Auch der Boom von Zertifikaten und Gütesiegeln, die zusätzlich zu einem internen QM eine externe Referenz liefern entspricht der Logik der sich ausdifferenzierenden Märkte. Es genügt nicht mehr, in Form von Werbung die Qualität eines Produktes oder einer Dienstleistung zu postulieren. Vielmehr muss für die Glaubwürdigkeit der Aussage auch eine rationale Begründung geliefert werden. Dies kann beispielsweise durch ein Qualitätsmanagement geleistet werden.

Die acht Grundsätze des Qualitätsmanagements nach DIN EN ISO 9000ff:

1. **Kundenorientierung**
2. **Führung**
3. **Einbeziehung der Personen**
4. **Prozessorientierter Ansatz**
5. **Systemorientierter Managementansatz**
6. **Ständige Verbesserung**
7. **Sachbezogener Ansatz zur Entscheidungsfindung**
8. **Lieferantenbeziehungen zum gegenseitigen Nutzen**

Im Kern geht es beim QM um das Verhältnis zwischen Anbieter und Kunden (was in großen Organisationen auch interne Beziehungen umfassen kann). Die Prozessorientierung ist im QM zentral angelegt. Gerade in einer dynamischen Nachfragelage und ständigen Veränderung der Umwelt (Wandel der Märkte, Veränderung der Technologien und des Rechtssystem) bedarf es einer abstrakten Fassung der Abläufe, die flexibel auf neue Anforderungen reagieren las-

sen. Aber auch der Qualitätsbegriff selbst darf nicht statisch begriffen werden. Die Benutzung des Begriffs Qualität (lat.: „qualitas“: Beschaffenheit, Eigenschaft) suggeriert im Alltag häufig, die beteiligten wüssten klar, was er bedeutet. Letztlich bedarf er jedoch immer der näheren Vereinbarung und Spezifizierung. Was als Qualität verstanden wird ist zwischen Anbieter und Kunde auszuhandeln. Gerade im Non-Profit-Bereich ist jedoch die Frage zu erörtern, wer denn als Kunde verstanden wird. Im sozialen Bereich ist nämlich der (Dienst-) Leistungsempfänger häufig nicht identisch mit dem Geldgeber für eine Leistung. Der Kundenbegriff muss letztlich differenziert werden – etwa in „Klientel“ und „(Leitungs-)Träger“. Das macht die Sache natürlich nicht einfacher: Was letztlich als Qualität zu verstehen ist, muss mit unterschiedlichen Personen und Organisationen ausgehandelt werden, wobei es dabei mit hoher Wahrscheinlichkeit zu unterschiedlichen Einschätzungen – auch auf Grund von Interessenskonflikten – kommen wird. Ein QM im sozialen Bereich muss dabei Instrumente in Form von Prozessen zur Verfügung stellen, die eine Vermittlung zwischen den unterschiedlichen Qualitätsvorstellungen von Kostenträgern, Dienstleistungsanbietern und Klienten ermöglichen kann.

Für die Online-Beratung kommen durch die besonderen medialen Gegebenheiten noch weitere Fragestellungen hinzu. So wird ein Online-Beratungsangebot nur dann wahrgenommen, wenn es entsprechend der Beratungsinhalte auch als vertrauenswürdig eingestuft wird. Diese Merkmale der potentiellen Klientel sind jedoch sehr schwer zu erfassen, da diejenigen, die ein Angebot nach dem Besuch einer Webseite nicht nutzen, auch nicht erfasst werden können. So hat Dzeyk (2005) experimentell nachgewiesen, dass entsprechend der vorher gefassten Hypothese eine Beratungsseite signifikant als vertrauenswürdiger eingestuft wird, wenn sie auf der „Datenschutz- und Sicherheitsseite“ detailliertere Informationen zur Verfügung stellt und nicht nur pauschale. Demgegenüber konnte kein signifikanter Effekt nachgewiesen werden, indem ein Foto auf der Startseite des Beraters angeboten wurde, obwohl in Fachkreisen häufig vermutet wird, dass ein Foto die Vertrauenswürdigkeit eines Online-Beratungsangebots deutlich erhöhen würde. Dabei wird deutlich, dass die mangelnde Kenntnis potentieller Nutzer durch gezielte Forschung wie im genannten Experiment überbrückt werden kann und muss. Eine weitere Begründung für ein QM liegt auch in der Rationalisierungsnotwendigkeit durch zunehmenden Kostendruck. Die Prozesse zur Leistungserbringung müssen effizient gestaltet werden. Reibungsverluste durch mangelhafte Organisation sind nicht mehr finanzierbar. Die Kosten der sozialen Dienstleistungen sollen dabei zu möglichst großen Teilen in die (wie auch immer definierte) Qualität der Leistung einfließen. Das, was als zu erbringende „Qualitas“ z.B. von Leistungsträgern oder durch gesetzliche Vorgaben definiert wird, muss dabei allerdings fachlich und ethisch nicht unbedingt wünschenswert sein, was sich derzeit beispielsweise im Bereich der Pflege zeigt. Hier bedarf es beständig eines kritischen Diskurses.

Die Motivationen zu einem QM sind somit also vielfältig. Gerade für den Bereich Online-Beratung ist auf Grund der Komplexität der Technik und der relativen Neuheit des Gegenstandsfeldes ein QM sinnvoll. Ohne eine gezielte Steuerung der Prozesse ist sonst davon auszugehen, dass wichtige Qualitätsaspekte nicht im Blick sind oder zumindest mit der Zeit aus dem Blick geraten.

2. Datenschutzmanagement

Zunächst sollte auf Grund der missverständlichen Begrifflichkeit geklärt werden was Datenschutz nicht ist, um danach positiv zu bestimmen, welche Begründung er hat. Beim Datenschutz geht es nicht primär um die Daten, wie der Begriff zunächst nahe legen mag. Diese im Deutschen eingebürgerte Bezeichnung ist leicht irreführend, da sie mit „Datensicherheit“ zu

verwechseln ist. Im Englischen gibt es den treffenderen Begriff „privacy“, der auf den Punkt bringt, dass es um den Schutz der Privatheit von Menschen geht. Rechtlich gesehen handelt es sich bei Datenschutz um das grundgesetzlich verbürgte „Recht auf informationelle Selbstbestimmung“ der Individuen. Das gesamte Datenschutzrecht zielt dabei also darauf, dass der Einzelne nicht einfach zum Objekt von Informationen über ihn selbst gemacht werden darf. Das bekannteste Schreckensszenario diesbezüglich stellt der bekannte Roman „1984“ von George Orwell dar. Einer unkontrollierten Überwachung von Menschen – sei es durch Privatpersonen oder Organisationen, sei es durch den Staat – soll Datenschutz von Anfang an entgegenwirken. Im so genannten „Volkszählungsurteil“ des Bundesverfassungsgerichts wurde dabei konkretisiert, dass alle personenbezogenen Daten ausnahmslos unter den grundgesetzlichen Schutz fallen. Durch die Leistungsfähigkeit moderner Computertechnologie mit ihren Datenbanksystemen kann danach kein noch so unscheinbar wirkendes einzelnes Personendatum ungefährlich sein. Es ist im voraus nämlich nicht absehbar, was mit personenbezogenen Daten – möglicherweise zum Schaden der betreffenden Person – gemacht wird, wenn sie unkontrollierbar erhoben, verarbeitet und genutzt werden. Die Redensart „Wissen ist macht“ kann hier versinnbildlichen, dass Wissen über eine Person auch Macht über diese Person bedeuten kann.

Datenschutz ist dabei ausschließlich ethisch begründbar. Datensicherheit (entsprechend: IT-Sicherheit, EDV-Sicherheit) kann demgegenüber auch andere Interessen bedienen und ggf. sogar dem Datenschutz widersprechen. Werden Datenbestände mit personenbezogenen Daten gut nach außen abgeschottet kann das ganz im Sinne des Datenschutzes sein, muss es aber nicht. Die Frage ist dabei, ob z.B. auch die Verarbeitung dieser Daten innerhalb der Organisation den geltenden Datenschutzbestimmungen entspricht oder nicht. So wird der Unterschied zwischen Datenschutz und Datensicherheit deutlich: Datenschutz benötigt Datensicherheit in dienender Funktion, um die Daten von Personen vor unberechtigtem Zugriff zu schützen. Datensicherheit ist demgegenüber wertneutral, wobei sich nur in der konkreten Umsetzung zeigen kann, ob die Sicherheit im Dienste bzw. konform mit diesem und anderen Grundrechten ist oder ob Datensicherheit sogar dazu missbraucht wird, ungesetzliche Datenbestände zu schützen.

Geschichtlich zeigt sich, dass sich Datenschutzregelungen bei solchen Berufen als erstes entwickelt haben, die ein hohes Maß Vertrauen voraussetzen. So können die ärztliche Schweigepflicht und das Beichtgeheimnis von Priestern als älteste bekannte Datenschutznormen belegt werden. Der Eid des Hippokrates, aus dem die ärztliche Schweigepflicht hervorgeht, stammt aus dem Jahre 400 vor Chr. Seit 1215 n. Chr. sind Beichtgeheimnis und Seelsorgegeheimnis im Kirchenrecht verbürgt.

Dass auch in der Beratung im Zusammenhang mit vertraulichen, persönlichen und intimen Inhalten ein hohes Maß an Vertrauen nötig ist, steht außer Frage. Diese Voraussetzung von Beratung und dieser Anspruch an Beratung spiegelt sich sowohl in berufsrechtlichen als auch in gesetzlichen Regelungen wie beispielsweise im Strafrecht wider.

Die konkrete Praxis im Umgang mit sensiblen Daten einschließlich Privatgeheimnissen und die daraus resultierende Gefahr, vertrauliche Inhalte vielleicht sogar unbeabsichtigt weiter zu geben, hat sich durch die Entwicklung der Technik dramatisch verändert. Geheimnisse im Kopf eines Geheimnisträgers sind in der Regel relativ gut „gesichert“. Es bedarf zumindest einer Äußerung des Geheimnisträgers, um die gedanklich gespeicherten Inhalte weiterzugeben. Erst die Verschriftlichung vertraulicher Inhalte begründet die Notwendigkeit eines Schutzkonzepts der Inhalte, da die Daten nun getrennt vom Geheimnisträger sind. In Papier-

form ist es möglich, die Daten zu entwenden oder vielleicht sogar unbemerkt zu kopieren. Dies muss effektiv, z.B. durch gesicherte Aktenschränke verhindert werden. Die Möglichkeit zur unbefugten Weitergabe erhöht sich, sobald sie in elektronischer Form vorliegen. Der Kopiervorgang selbst großer Datenbestände ist durch diese Technik weit leichter und bei fehlendem Schutzkonzept sogar eher unbemerkt möglich als dies bei einem Kopiervorgang von Papier am Kopierer der Fall wäre. Aus diesem Grund unterliegen elektronische personenbezogene Daten einem weit höheren Anspruch an die Realisierung des entsprechenden Sicherheitskonzepts als die gleichen Daten auf Papier.

Die größte Bedrohung für vertrauliche Daten hat sich aber erst durch die weltweite Vernetzung von Computern durch das Internet ergeben. Wie die Metapher des Netzes anschaulich zeigt, sind alle Teile eines solchen Netzes direkt oder indirekt miteinander verbunden. Anders als von Internetnutzern oft gedacht, ist die Nutzung der beteiligten Leitungen prinzipiell in beide Richtungen machbar: Nicht nur der Internetnutzer kann von seinem PC auf andere Computer zugreifen, vielmehr ist das grundsätzlich auch umgekehrt möglich. Hier gibt es ohne ein effektives Schutzkonzept kein Außen oder Innen. Das heißt wer sich im Internet bewegt muss damit rechnen, dass auch auf seinen Computer zugegriffen werden kann, wenn dies nicht aktiv verhindert wird.

Spätestens an diesem Punkt wird deutlich, dass Personen und Organisationen, die vertrauliche Daten per Computer verarbeiten ein Konzept haben müssen wie sie die Daten konkret vor unbefugtem Zugriff sichern, wenn sie nicht zumindest fahrlässig riskieren wollen, dass vielleicht sogar Privatgeheimnisse in falsche Hände geraten.

Bei Online-Beratung kann das hohe Risikopotential durch einen Internetanschluss im Gegensatz zur face-to-face-Beratung überhaupt nicht vermieden werden. Online-Beratung ohne Internetanschluss ist schließlich nicht möglich. Somit gilt bei der Beratung mit sensiblen Inhalten im Internet ein erhöhter Schutzbedarf, wenn die Vertraulichkeit auch in der Beratungspraxis realisiert werden soll. In den ersten Jahren der Pionierphase der Online-Beratung (1995-2000) in Deutschland hat diese Fragestellung kaum eine Rolle gespielt. Dennoch haben einige Einrichtungen schon in dieser Zeit eine Verschlüsselung (PGP oder GnuPG) zur Verfügung gestellt. Diese Maßnahmen haben sich jedoch nicht durchgesetzt. Haben in den ersten Jahren beispielsweise bei der Telefonseelsorge Deutschland noch ca. 2 % der Ratsuchenden ihre Mails verschlüsselt waren es im Jahr 2001 nur noch weniger als 1 %. Nicht zuletzt durch die Realisierung der webbasierten und SSL-verschlüsselten Online-Beratung ab 2002 hat sich bei vielen namhaften Anbietern die Überzeugung durchgesetzt, dass die Verantwortung für einen sicheren und vertraulichen „virtuellen Beratungsraum“ nicht auf den Nutzer verschoben werden darf. Die durchschnittlichen Internetnutzer kennen sich schließlich immer weniger mit der dahinterliegenden Technologie aus. Außerdem ist es Menschen in Krisen- und Problemsituationen nicht zumutbar, vor Beginn der Beratung erst Verschlüsselungsmechanismen auf dem eigenen Computer zu installieren. Dies wird auch von unabhängigen Datenschützern so eingeschätzt: Der Anbieter ist auf Grund unterschiedlicher rechtlicher Anforderungen verantwortlich eine datenschutzverträgliche Beratungsplattform für sensitive Beratung im Internet anzubieten.

Dies zeigt, dass die Realisierung der Datenschutzanforderungen bei einer derart komplexen und dazu noch dynamischen Technologie keine triviale Anforderung darstellt. Gerade in mittleren und größeren Organisationen und Verbänden ist ein Datenschutzmanagement notwendig, das alle beteiligten Personen und Prozesse auf den unterschiedlichen Ebenen einbezieht *(siehe Abbildungen auf nachfolgenden Seiten)*. Hier kann es effektiv und kostensparend sein,

das Datenschutzmanagement in Zusammenhang mit dem Qualitätsmanagement zu realisieren. Dabei ist jedoch zu beachten, dass es beim Datenschutz auch um unveräußerbare Rechte geht, die nicht im Rahmen einer Anbieter-Kunden-Vereinbarung verhandelbar und nur begrenzt vertraglich regelbar sind. Rechtliche Vorgaben und technische Problemstellungen sind somit in das Qualitätsmanagement zu integrieren.

3. Qualitäts- und Datenschutzdimensionen von Online-Beratung

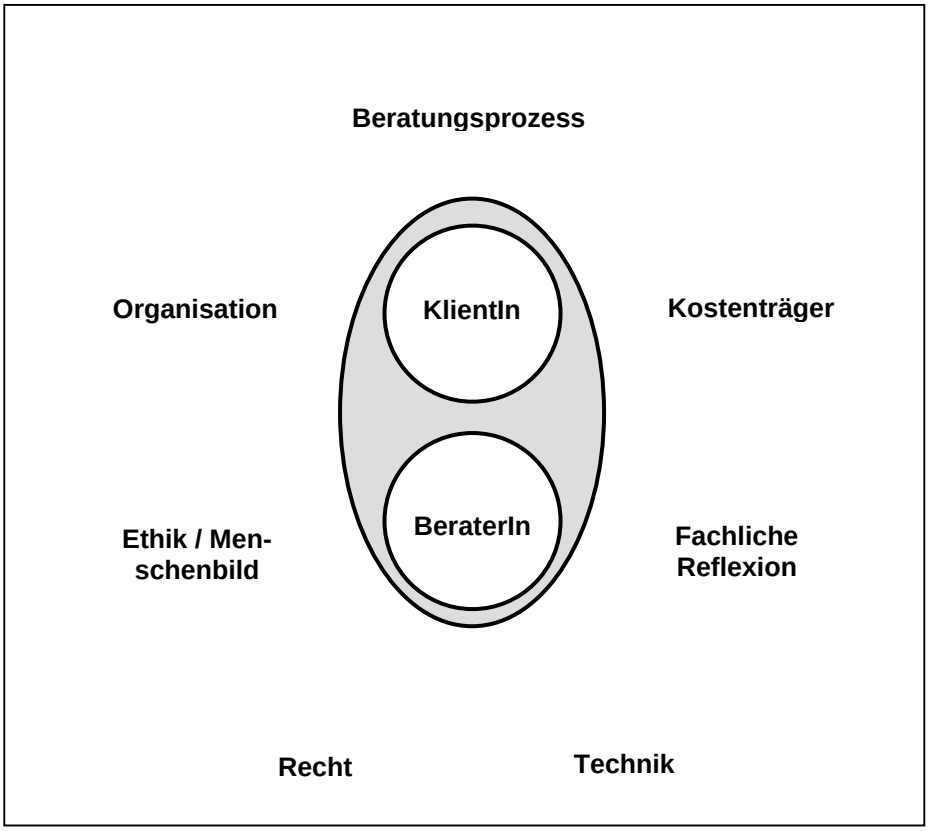
Qualitätsmanagement-Systeme entstammen geschichtlich dem Bereich der industriellen Produktion und wurden später auf Dienstleistungsangebote übertragen. Die Frage der Anwendbarkeit auf Bereiche verschiedener Professionen wird kontrovers diskutiert. Auf die Fragestellung der Professionalität sei beispielsweise auf Combe/Helsper (1997) verwiesen. Die Diskussion des Spannungsfelds Qualitätsmanagement und Profession kann hier nicht näherer erörtert werden. Hierzu sei auf die Dissertation von Gerull (2005,S. 15) verwiesen, der ausführt:

> *“Von der Qualitätsdiskussion werden mehrheitlich Impulse erhofft, die Professionalisierung der Hilfesysteme zum Nutzen der "VerbraucherInnen" voranzubringen (z. B. Späth, 1999; Merchel, 2001). Allerdings dürften die Erwartungen der verschiedenen Interessengruppen nicht alle miteinander zu vereinbaren sein (Gerull, 2000, S. 6f), was den diskursiven Charakter des Qualitätskonstrukts im Sozialbereich unterstreicht“.*

Bei aller notwendiger Formalisierung im Qualitätsmanagement scheint die Diskursivität zur Bestimmung der Qualität gerade im Bereich psychosozialer Beratung notwendig. Es ist in diesem Zusammenhang wichtig darauf hinzuweisen, dass es im Gegensatz zur Produktion von Waren im Blick auf professionelles Handeln in der Gestalt von Beratung von Menschen unbedingt auch das Menschenbild reflektiert und beschrieben werden muss, vor dessen Hintergrund sich die Beratung vollzieht. Ethische Fragestellungen zur Begründung des professionellen Handelns gehören ebenfalls grundlegend dazu. Als Kunden können sowohl die KlientInnen als auch etwaige Kostenträger verstanden werden. Des weiteren sind die fachliche Reflexion der Handlungskompetenz vor dem Hintergrund wissenschaftlicher Forschung der BeraterInnen sowie die rechtlichen, technischen und organisatorischen Rahmenbedingungen zu berücksichtigen. Der zentrale Qualitätsfokus sollte dabei auf dem Beratungsprozess selbst liegen.

Somit ergibt sich für das Qualitäts- und Datenschutzmanagement von Online-Beratung ein Komplexitätsgrad, den es zu operationalisieren gilt. Nachfolgende Abbildung zeigt entsprechend den genannten Fokus und die zentralen Rahmenbedingen.

Qualitätsfokus mit Rahmenbedingungen von Online-Beratung



Qualitätsmanagement von Online-Beratung muss also sehr unterschiedliche Ebenen und Bereiche berücksichtigen, will sie der Komplexität des Gegenstandsfeldes gerecht werden. Bei einer materiellen Ware sind die Qualitätsmerkmale noch relativ einfach beschreibbar, wenn sich auch in diesem Feld der Qualitätsbegriff gewandelt hat und auch beim QM der Produktion von Waren eine Prozessorientierung heute grundlegend ist. Beratung hinsichtlich der Qualität zu erfassen ist weitaus schwieriger, da Kommunikationsprozesse in ihrer Vielschichtigkeit schwer zu beschreiben sind. Darüber hinaus vollzieht sich Beratung immer in einem konkreten gesellschaftlichen Kontext, den es zu berücksichtigen gilt. Was schließlich in fachlicher Hinsicht als Qualität verstanden wird, ist das Ergebnis von Kommunikationsprozessen auf unterschiedlichen Ebenen. Um zu klären, auf welcher Ebene und hinsichtlich welcher Prozesse man sich beim Qualitätsmanagement (bzw. beim Datenschutzmanagement) gerade bewegt, bedarf es einer zielgerichteten und nachvollziehbaren Reduktion der Komplexität. Dies kann in Anlehnung an technische Schichtenmodelle geschehen, wie etwa an das OSI-Modell der Netzwerktechnik.

Das nachfolgend aufgezeigte Modell „Schichtenmodell mediale Kommunikation und Beratung“ erhebt keinen Anspruch auf Vollständigkeit und bedarf voraussichtlich der Ergänzung bzw. Spezifikation. Es muss ggf. an die konkreten Praxisbedingungen von Online-Beratung angepasst werden, kann in dieser allgemeinen Form aber bereits dazu dienen, sich darüber zu verständigen, über welche Qualitätsdimension von Online-Beratung jeweils die Rede ist, und einen Beitrag dazu leisten, wichtige und dabei sehr unterschiedliche Dimensionen in einem Diskurs zur Qualität im Blick zu behalten.

Das hier vorgeschlagene Schichtenmodell für Online-Beratung kann hier nicht in seiner Gesamtheit vorgestellt werden. Vielmehr soll im Überblick gezeigt werden, wie QM und DSM zusammenwirken können und wie Datenschutz in ein Gesamtmanagement (zusammen mit anderen Managementsystemen) integriert werden kann. Die makrosoziale Ebene betrifft die gesellschaftlichen Rahmenbedingungen, die Einfluss auf das konkrete mediale Beratungssetting haben; rechtliche Rahmenbedingungen und wirtschaftliche Einflussfaktoren inkl. der technischen Entwicklungen, aber auch das Wissenschaftssystem, das fachliche Begründungen für Qualitätsmerkmale der Online-Beratung z.B. durch Wirkungsforschung liefert. Die weiteren Konkretisierungen auf den Ebenen Mikrosozial bis Technik sollen die relevanten „Schichten“ als Arrangement heterogener Einheiten erfassen und ins Bewusstsein rufen.

Schichtenmodell mediale Kommunikation und Beratung (Online-Beratungsmodell)

Ebenen	**Schicht**	**Relevante Bereiche (Systeme)**	***Ausformung / Beispiele***
Makrosozial	Ma1	Gesellschaft	*Sprache, Institutionen, Kultur*
	Ma2	Recht	*Online-Recht, Datenschutzrecht, Strafrecht, Privatrecht, SGB*
	Ma3	Wirtschaft	*Softwarelizenzen, Monopole, Märkte, Entwicklungstrends der Technik*
	Ma4	Wissenschaft	*(Interdisziplinäre) Forschung und Lehre zu Beratung / Online-Beratung*
Mikrosozial	Mi1	Kostenträger	*Finanzierung und Verträge (z.B. nach SGB)*
	Mi2	Verbände	*(Fach-, Berufs-)Verband, Rechts-träger, Kammern, Berufsrecht, Qualitätsstandards*
	Mi3	Organisation - Führung - Qualitätsbeauftragte/r - Datenschutzbeauftragte/r - Sicherheitsbeauftragte/r	*Beratungsstelle, Menschenbild mit Ethik-Richtlinien, Ausbildungskonzept, Beratungskonzept, Datenschutz- und Sicherheitskonzept, Regeln, Zuständigkeiten, Supervision, Evaluation*
	Mi4	Subkultur	*Netzwerk, Kommunikationsplattform, Netiquette, Soziales Milieu*
	Mi5	Beratungskontext	*Konkretes Beratungsangebot: Chat, Mail, Foren, Präsentation, Selbstbeschreibung, Abrechnungsmodus*
Kommunikation	K	Beratung als Kommunikation	*Interaktionsebene: Konkrete Situation, Kommunikationssequenzen*
Subjekt	S1	Ratsuchende	*Anforderungen an Beratungsangebot, Auswahlkriterien bei Beratungsangeboten (bewusst oder unbewusst), medialkommunikative Kompetenz*
	S2	BeraterInnen	*Medialkommunikative Kompetenz, Online-Beratungskompetenz*
Inhalt	I1	Beratungsinhalt	*Texte, speicherbare Inhalte (bei Video entsprechend auch Bilder)*
	I2	Sonstiger Inhalt	*Verträge zwischen Anbieter und Nutzer, Allgemeine Geschäfts-bedingungen*
Lieferanten	L	Leistungserbringer	*EDV-Abteilung, Softwarefirma, Provider, Externe Sicherheitsberater, Beratungsplattform*
Technik	T1	Anwendungsprogramme / Dateien	*Internetseiten, Beratungssoftware, Statistikmodule, Anpassungsmöglichkeiten durch BeraterInnen und/oder Ratsuchende, Anwendungs-programme, Betriebssysteme*
	T2	Sicherheitsinfrastruktur	*Sicherheitsgateway, Firewall, Virenwall, VPN*
	T3	Anwendung: Protokolle	*HTTP, HTTPS, FTP, SMTP, POP3, Telnet, SSH*
	T4	Transport	*TCP, UDP*
	T5	Internet	*IP*
	T6	Netz	*Ethernet, Token Ring, WLAN*

4. Datenschutzmanagement von Online-Beratung konkret

Datenschutzmanagement vollzieht sich in den Bereichen Recht, Technik und Organisation. Um dem Recht der Menschen auf informationelle Selbstbestimmung gerecht zu werden, müssen die bei der konkreten Online-Beratung geltenden gesetzlichen und sonstigen rechtlichen Regelungen berücksichtigt werden. Die Technik muss - soweit möglich - an die Anforderung der Beratungseinrichtung und die notwendigen Datenschutzaspekte unter Beachtung der Rechtslage angepasst werden. Ein effektives Management der EDV (Datensicherheits-Management / IT-Sicherheitsmanagement) ist dabei grundlegend, weil nur so der Schutz der personenbezogenen Daten vor unerlaubten Eingriffen gewährleistet werden kann. Organisatorisch bedarf es eines umfassenden Datenschutz- und Sicherheitskonzepts inklusive Aus- und Weiterbildungskonzept, Notfallplan, Prozessplanung, klarer Zuständigkeiten und Realisierungsstrategie unter Berücksichtigung der psychologischen und pädagogischen Grundfragen.

4.1 Datenschutzrecht in Deutschland

Die rechtliche Systematik macht es notwendig vom Rechtssystem eines Staates auszugehen. Beispielhaft wird nachfolgend die deutsche Rechtssituation in vereinfachter Weise schematisch dargestellt. Für eine differenzierte Konkretisierung des Internetrechts sei verwiesen auf Schaar 2002 und Hoeren/Sieber 1998.

4.1.1 Grundprinzipien des Datenschutzrechts

Das Datenschutzrecht wird in Deutschland durch ein höchstrichterliches Urteil des Bundesverfassungsgerichts von 1983 („Volkszählungsurteil“) unmittelbar von den Grundrechten abgeleitet: Art. 2 Abs. 1 GG „Recht auf freie Entfaltung der Persönlichkeit“ in Verbindung mit Art. 1 Abs. 1 GG „Menschenwürde“. Namentlich als das **Recht auf informationelle Selbstbestimmung** bezeichnet. Hier geht es im Kern um das Freiheitsrecht einer Person: dass sie grundsätzlich darüber wissen soll, welche Daten über sie vorliegen und wie und zu welchen Zwecken diese verarbeitet und genutzt werden. Hier hat die einzelne Person umfassende Rechte z.B. auf umfassende Information über die sie selbst betreffenden personenbezogenen Daten.

Begriffsbestimmung: „Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).“ (§ 3 Abs. 1 Bundesdatenschutzgesetz (BDSG))

In dieser Definition wird deutlich, dass es sich nicht erst dann um personenbezogene Daten handelt, wenn beispielsweise der Name einer betroffenen Person dabei steht, sondern allein schon dann, wenn die Daten auf eine bestimmte Person schließen lassen.

Im Gegensatz zur später dargelegten und für juristische und technische Laien schwer durchschaubaren konkreten Rechtslage, sind die Grundprinzipien des Datenschutzes einheitlich und für die Praxis in der Beratung nachvollziehbar. Sie sind für das gesamte Datenschutzmanagement grundlegend:

Grundsätzlich gilt für die
Erhebung,
Verarbeitung (Speicherung, Veränderung, Sperrung, Löschung, Übermittlung) und
Nutzung
von **personenbezogenen Daten** ein **Verbot mit Erlaubnisvorbehalt** (vgl. § 4: BDSG).

Das heißt, Erhebung, Verarbeitung und Nutzung sind grundsätzlich verboten, es sei denn, es gibt dafür entweder eine Rechtsgrundlage oder eine bewusste Zustimmung des jeweils Betroffenen.

Weitere Grundsätze des Datenschutzrechts:

- **Erforderlichkeit**
- **Strenge Zweckbindung**
- **Datenvermeidung und Datensparsamkeit**
- **Gewährleistung von Integrität, Vertraulichkeit und Verfügbarkeit der Daten**
- **Es gibt unabdingbare Rechte der Betroffenen**

Die Erhebung, Verarbeitung und Nutzung muss also erforderlich (d.h. begründbar) sein. Für einen bestimmten Zweck erhobene Daten dürfen beispielsweise nicht für einen anderen Zweck verwendet werden. Personenbezogene Daten sollen möglichst vermieden werden. Sind sie begründet nicht zu vermeiden, sind die Daten nach Möglichkeit zu anonymisieren bzw. zu pseudonymisieren.

Anders als im Qualitätsmanagement sind beim Datenschutzmanagement auch rechtliche Vorgaben zu beachten, die zwischen Kunden und Dienstleistern nicht verhandelbar sind :

BDSG: *"§ 6 Unabdingbare Rechte des Betroffenen*
(1) Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden."

Rechte der Betroffenen im Überblick:

- **Recht auf Grundinformation über gespeicherte Daten**
- **Auskunftsrecht**
- **Recht auf Berichtigung der Daten**
- **Recht auf Sperrung, d.h. Einschränkung der Nutzungsmöglichkeit**
- **Recht auf Löschung von Daten**
- **Recht auf Anrufung des Datenschutzbeauftragten**
- **Recht auf Schadensersatz**

Für das Datenschutzmanagement ist zunächst die Klärung der je konkreten rechtlichen Situation grundlegend. Dabei zeigt sich, dass es kein einheitliches Datenschutzkonzept für alle Organisationen geben kann, selbst wenn sie vergleichbare Dienste erbringen, da jeweils unterschiedliche rechtliche Normen gelten. Auf gesetzlicher Ebene macht es Sinn, zunächst das Europarecht in den Blick zu nehmen. In der Europäischen Datenschutzrichtlinie werden die Datenschutzgrundsätze geregelt, die von den Mitgliedsstaaten in nationales Recht umzusetzen sind. Bundesweit gilt das Bundesdatenschutzgesetz (BDSG) im öffentlichen Bereich für

Bundesbehörden und Körperschaften des öffentlichen Rechts, darüber hinaus aber auch für privatrechtliche Vereine und Wirtschaftsunternehmen. Das BDSG gilt grundsätzlich in den Bereichen, die nicht speziell geregelt sind. Wo es eigene Regelungen gibt, gilt das jeweilige spezielle Datenschutzrecht. Auf Länderebene sind die Datenschutzgesetze der Bundesländer (LDSG) für die Behörden und Einrichtungen des öffentlichen Bereichs (Landesbehörden und Gebietskörperschaften) zuständig. In Deutschland regeln die öffentlich-rechtlich verfassten Kirchen ihre Datenschutzfragen durch eigene Gesetze bzw. durch Verordnungen in je eigener Verantwortung. In der römisch-katholischen Kirche gilt die Anordnung über den kirchlichen Datenschutz (KDO). In der evangelischen Kirche gilt das Datenschutzgesetz der EKD (DSG-EKD). Das Berufsrecht wird durch öffentlich-rechtliche Kammern konkretisiert. Dabei gibt es unterschiedliche Rechtsgrundlagen (z.B. das Heilberufegesetz) das für die jeweiligen Kammern als Vorgabe verbindlich ist. Im Bereich der sozialen Leistungen (Rente, Gesundheit, Jugendhilfe,...) ist das Sozialgesetzbuch (SGB) maßgeblich, das spezielle Datenschutzregelungen und den speziellen Begriff „Sozialgeheimnis“ (§ 35) enthält. Für die Telekommunikation ist das Telekommunikationsgesetz (TKG) maßgebliche Rechtsgrundlage. Desweiteren gelten hinsichtlich Telediensten und Mediendiensten zwei Gesetze. Zum einen das Informations- und Kommunikationsdienstegesetz (IuKDG) des Bundes und der zwischen den Ländern vereinbarte Mediendienstestaatsvertrag (MDStV). Das IuKDG enthält dabei u.a. das Teledienstegesetz (TDG) sowie das Teledienstedatenschutzgesetz (TDDSG) und das Signaturgesetz (SigG). Was die mögliche Verletzung von Privatgeheimnissen durch bestimmte Berufsgruppen und Amtsträger angeht ist in § 203 StGB geregelt. Privatrechtliche Regelungen sind im Bürgerlichen Gesetzbuch (BGB) zu finden. Dort wird beispielsweise die Schadensersatzpflicht geregelt, die z.B. einen Diensteanbieter im Internet betreffen kann, selbst dann wenn er nicht vorsätzlich sondern lediglich fahrlässig zuwider gehandelt hat.

Die Zuordnung welches Gesetz in welchem Bereich hinsichtlich technischer Fragen Geltung hat ist nicht auf den ersten Blick zu erkennen. Rost (2005) beschreibt die Systematik, mit der Juristen die moderne Kommunikationstechnik einordnen, in der Beantwortung der Frage „Welches Gesetz gilt eigentlich?“. Dabei lehnen sich die Juristen - wie oben bereits für die Online-Beratung (OB) vorgeschlagen - an das technische Schichtenmodell an. Schleipfer (2004) hat das Modell des Multimediadatenschutzrechts näher ausgeführt. Nachfolgend hierzu eine schematische Übersicht:

Synopse: 3-Schichten-Modell des Multimediadatenschutzrechts / Online-Beratungsmodell

Schicht	Beschreibung	Protokolle	Recht	OB-Schicht
Schicht 3	Bedeutungs- und Inhaltsebene	Inhalte	BDSG, LDSG, Verträge, AGB, BGB, SGB, StGB	I1-I2
Schicht 2	Interaktionsebene des Nutzers mit der Technik	HTTP, HTTPS FTP, SMTP, POP3, Telnet, SSH	TDG, TDDSG, MDStV	T1 / T3
Schicht 1	Telekommunikationsebene	TCP, IP, UDP	TKG	T4-T6

Hierbei ist allerdings zu beachten, dass sich Daten auf den unterschiedlichen Schichten bewegen. So sind auch bei Online-Beratung – je nachdem an welchem Punkt sich die Daten im Prozess befinden – rechtlich jeweils andere Gesetze zu beachten.

4.1.2 Strafbarkeit, Ordnungswidrigkeit und Schadensersatzpflicht

Hinsichtlich der Fragestellung Qualität kann es im Wettbewerb von Dienstleistungen negative Auswirkungen auf einen Anbieter geben. So ist es möglich, dass ein fragwürdiges Angebot zum schlechten Ruf eines konkreten Angebots oder sogar des Anbieters führt. Unter bestimmten Voraussetzungen kann sich der Kunde weigern für die vereinbarte Dienstleistung auf Grund von Mängeln den vereinbarten Preis zu bezahlen.

Bei Verstößen gegen Datenschutzregelungen einschließlich der Schweigepflicht und technikrechtlichen Regelungen kann es darüber hinaus aber auch zu strafrechtlichen Folgen, Ordnungsgeldern und nicht zu letzt sogar zu Schadensersatzverpflichtungen kommen. Berufsrechtlich sind unter Umständen auch Berufsverbote mögliche. Um als Freiberufler oder Beratungseinrichtung nicht in unkalkulierbare Konsequenzen zu geraten, ist es sinnvoll die geltende Rechtgrundlage auch auf solche möglichen Folgen (Freiheitsstrafe / z.T. empfindliche Ordnungsgelder und Schadensersatzpflicht) zu untersuchen. Dabei kann es leicht passieren, dass die Geltung mancher Gesetze nicht bekannt ist.

So kann unter Umständen ein Anbieter von Online-Beratung nach § 12 TDG mit einem Ordnungsgeld von bis zu 50.000,- Euro belangt werden. Dafür bedarf es nicht einmal eines Vorsatzes durch den Anbieter. Es genügt bereits die fahrlässige Weglassung geforderter Angaben bei der Anbieterkennzeichnung des Internetangebots (Impressumsseite). Der Gesetzestext im Wortlaut:

„(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 6 Satz 1 eine Information nicht, nicht richtig oder nicht vollständig verfügbar hält.
(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.“

Der Verstoß gegen unterschiedliche Datenschutznormen wird ebenfalls durch Ordnungsgeld oder sogar durch Haftandrohung bewehrt.

Insbesondere § 203 StGB erfährt durch das Internet besondere Brisanz: Die Offenbarung eines Privatgeheimnisses ist durch die Gefahren des Internets leichter möglich als das vor dem Aufkommen dieser Vernetzungstechnologie wahrscheinlich war. § 203 ist für viele Online-BeraterInnen maßgeblich, da sie zu den genannten Berufsgruppen oder Amtsträgern gehören. Um dem hohen Anspruch an vertrauliche Beratung gerecht zu werden, bedarf es bei der Internetnutzung durch Beratungseinrichtungen und erst Recht bei der Beratung im Internet einem besonderen Maß an Sorgfalt. Wie das im Rahmen des Datenschutzmanagements für Online-Beratung umsetzbar ist, werden die nachfolgenden Bereiche „Technik“ und „Organisation“ konkretisieren.

4.2 Datenschutz-Technik

Die geltenden Datenschutzbestimmungen können nur erfüllt werden, wenn die beteiligten Computer inklusive Infrastruktur sicher sind. Beim Anschluss an das Internet und erst recht bei Online-Beratung, die sich im Netz vollzieht, sind besondere Maßnahmen notwendig, um den Prozess vertraulicher Beratung und die anfallenden personenbezogenen Daten zu schützen. Um die Komplexität der Technologie zu reduzieren haben EDV-Fachleute die bereits genannten Schichtenmodelle entwickelt. Auf der Technikebene sind diese unterschiedlich

komplex wie die nachfolgende Synopse zeigt. Für das Qualitäts- und Datenschutzmanagement von Online-Beratung scheinen die 4 Schichten des TCP/IP-Modells ausreichend zu sein. (Die Anwendungsschicht wurde für Onlieneberatung aus pragmatischen Gründen noch einmal differenziert, unabhängig von der Protokollebene.)

Synopse: OSI-Modell / TCP/IP-Referenzmodell / Online-Beratungsmodell

OSI-Schicht	**Nr.**	**Englisch**	**TCP/IP-Schicht**	**Protokolle**	**OB-Schicht**
Anwendung	7	Application	Anwendung	HTTP, HTTPS FTP, SMTP, POP3, Telnet, SSH	T1, T3
Präsentation	6	Presentation			
Sitzung	5	Session			
Transport	4	Transport	Transport	TCP, UDP	T4
Vermittlung	3	Network	Internet	IP	T5
Sicherung	2	Data Link	Netz	Ethernet, Token Ring, WLAN	T6
Physikalisch	1	Physical			

Das Internet besteht aus unterschiedlichsten Netzwerken und Diensten. Die technischen Standards des Internets - u. a. die so genannten Protokolle - wurden ursprünglich nicht nach Kriterien der Sicherheit entwickelt, da es sich bei der Entwicklung damals um ein Netzwerk mit geschlossenem Benutzerkreis handelte und die Erfordernisse heutiger Anwendungsmöglichkeiten nicht vorhergesehen wurden. Fragen nach Sicherheitsstandards wurden erst später aktuell, als das Internet öffentlich zugänglich wurde und trotzdem sensible Daten transferiert werden sollten.

Datenpakete, die zwischen zwei Rechnern im Internet ausgetauscht werden, können prinzipiell jederzeit "abgehört" werden, da die Übertragung der Daten über unzählige Computer erfolgt, an denen Zugriffsmöglichkeiten für Dritte bestehen. Die zum Mitlesen nötigen Programme lassen sich z. T. aus dem Internet beziehen und ohne größere Sachkenntnis einsetzen. Die Sicherheitsvorkehrungen vieler Organisationen stehen allerdings in keinem Verhältnis zu diesen offensichtlichen Sicherheitsbedrohungen.

Zu den unsicheren Übertragungsarten gehören neben dem Versand von E-Mails auch der Transfer von Dateien und das Abrufen von Seiten aus dem World Wide Web (WWW). Dabei lassen sich diese Übertragungen durchaus sicher gestalten.

Will man einen hohen Sicherheitsstandard in der Internetkommunikation gewährleisten, so sind unbedingt die verschiedenen Dimensionen von Sicherheit zu beachten:

Unter **Verbindlichkeit** versteht man die Nachvollziehbarkeit darüber, dass die Datenübertragung auch tatsächlich stattgefunden hat. Dies ist beispielsweise grundlegend für den elektronischen Handel zur Erteilung verbindlicher Aufträge oder Zusagen. Aber auch in anderen Bereichen der Kommunikation über das Internet schützt dieser Nachweis vor Missverständnissen. Möglichkeiten einer Bestätigung sind etwa ein beigefügter elektronischer Zeitstempel, eine Eingangsbestätigung oder die Beglaubigung durch eine dritte, vertrauenswürdige

Autorität. Beim Versand von E-Mails ist i.d.R. nicht gesichert, dass die Nachricht auch wirklich angekommen ist. Hier kann es im Beratungsprozess zu Störungen kommen, wenn ein/e Online-BeraterIn eine Antwort wegschickt, die nicht beim Ratsuchenden ankommt und dieser Verlust im weiteren Beratungsverlauf nicht bemerkt wird.

Vertraulichkeit bei Daten heißt, dass diese nur von einem zugelassenen Nutzerkreis eingesehen werden können. Im Internet als öffentlichem Netz bedeutet dies, dass der Inhalt einer Datenübermittlung nur Absender und Adressat bekannt sind. Ein solcher Transfer von Kommunikationsinhalten ist durch eine entsprechend sichere Verschlüsselung der Daten zu gewährleisten.

Die **Authentizität** der kommunizierenden Parteien muss in sensiblen Bereichen gewährleistet sein. Sowohl der Empfänger muss den Absender eindeutig identifizieren können als auch umgekehrt. Auf technischer Ebene kann dies durch eindeutige Merkmale, z.B. beigefügte digitale Signaturen oder Zertifikate einer Website (Server-Pass), realisiert werden.

Auf der anderen Seite muss, falls dies gewünscht ist, durch das Entfernen solcher eindeutigen Merkmale **Anonymität** hergestellt werden können, d.h. eine oder beide Parteien dürfen anhand von Übertragungsparametern u.ä. nicht feststellen können, wer der Kommunikationspartner ist. Manche Beratungsdienste im Internet benötigen dabei eine asymmetrische Lösung: Sie selbst sollen als eine bestimmte Einrichtung eindeutig und sicher identifizierbar sein. Der Ratsuchende soll anonym bleiben können.

Integrität meint, dass eine Mitteilung auf dem Übertragungsweg nicht verändert wurde. Eine Manipulation der übertragenen Daten muss verhindert werden. Gerade in einem Beratungsprozess muss gewährleistet sein, dass es nicht zu inhaltlichen Manipulationen durch Dritte kommen kann.

Datensicherung geschieht durch das geregelte Kopieren des Datenbestands (Back-Up) und die Aufbewahrung dieser Daten in einem geschützten Bereich.

Sicherstellung der **Verfügbarkeit** meint das Sichern der Daten innerhalb eine EDV-Infrastruktur durch gezielte Abwehrmaßnahmen von äußeren Bedrohungen. Geeignete Maßnahmen beziehen sich auf Brandgefahr, Hochwasser, Stromausfall und Spannungsschwankungen und (physischen) Diebstahl.

Das Gewährleisten dieser Sicherheitsdimensionen geschieht im IT-Sicherheitsmanagement das aus der Perspektive des Datenschutzes ein Teilbereich des Datenschutzmanagements darstellt. In Sachen IT-Sicherheit haben sich auch nationale und internationale Standards entwickelt. Für die grundlegenden Anforderungen an Datensicherheit hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) Sicherheitsstandards entwickelt. Diese beziehen sowohl technische Sicherheitsstandards ein als auch organisatorische Maßnahmen und Prozesse. Unter dem Begriff „BSI-Grundschutz“ sind diese Standards im online verfügbaren Grundschutzhandbuch veröffentlicht. Bei IT-Sicherheit gilt es in besonderer Weise auf dem Laufenden zu bleiben, wenn die Sicherheitsmaßnahmen wirksam sein sollen. Die Sicherheitsstandards müssen also regelmäßig angepasst werden. Beim BSI zeigt sich dabei in jüngster Zeit eine grundlegende Weiterentwicklung der Standards des BSI: „Neue Grundschutzgeneration. Vom IT-Grundschutzhandbuch zu den BSI-Standards für das IT-Sicherheitsmanagement“ (Münch 2005).

4.2.1 Technikgestaltung in Richtung Datenschutzverträglichkeit

Die rasante technische Entwicklung zwingt auch den Datenschutz zu beständiger technischer Weiterentwicklung. Das Recht kommt bei diesen Geschwindigkeiten nicht nach. Kaum ist ein Bereich rechtlich geregelt, hat sich die konkrete Technik bereits weiterentwickelt und dabei neue Fakten geschaffen, die von den Regelungen nicht mehr oder nur unzulänglich erfasst werden. In diesem Sinne ist auch die Rede von „lex informatica“. Das „Gesetz der Informatik“ schafft neue Rechtssituationen und Gegebenheiten. Eine Strategie von Datenschützern ist es, sich dieser Gestaltungsmöglichkeit anzuschließen und zum einen bereits in der Entwicklung neuer Technologien mitzuwirken und zum andern auch eigene Datenschutztechnik zu entwickeln, die den Menschen in der Praxis hilft, ihr Recht auf informationelle Selbstbestimmung auch wahrnehmen zu können (Schaar 2002). Drei Beispiele seien hier genannt, die auch für Einrichtungen der Online-Beratung praxisrelevant sind:

P3P ist ein Softwaretool, das standardisiert Datenschutzinformationen erfasst. Es kann in einem Browser installiert werden. Der Nutzer kann so bestimmte Datenschutzwünsche für das Internetsurfen voreinstellen. Geht dieser Nutzer auf eine Webseite, deren Anbieter serverseitig Datenschutzinformationen im P3P-Format zur Verfügung stellt, kann der Nutzer sehr schnell Informationen über die Datenschutzbestimmungen des Anbieters erfahren und ggf. bestimmte Interaktionen auf Internetseiten vermeiden, die keine verlässlichen Datenschutzinformationen bereitstellen.

Das Projekt **ANON/JAP** ermöglicht Surfen ohne dabei beobachtet zu werden. Durch den Anonymisierungsdienst JAP benutzt man beim Internet-Surfen eine feste IP-Adresse, die sich die Nutzer mit den anderen JAP Nutzern teilen. Dadurch erfährt weder der angefragte Server noch ein Lauscher auf den Verbindungen, welcher Nutzer welche Webseite aufgerufen hat.

Sewecom-Verfahren für sichere Kommunikation im Internet: Beim Sewecom-Verfahren handelt es sich um ein Verfahren, das technische Standards und organisatorische Rahmenbedingungen zusammenfasst, um obligatorisch verschlüsselte Kommunikation zum Beispiel mit Einrichtungen der Online-Beratung zu ermöglichen. Dieses Verfahren wird seit 2002 von der TelefonSeelsorge Deutschland eingesetzt. Die gesamte Beratung wird per SSL-Verschlüsselung gesichert.

4.3 Datenschutz-Organisation

Die Datenverarbeitung muss in der Praxis so gestaltet werden, dass sie den Anforderungen des Datenschutzes entspricht. Konkrete Kontrollmaßnahmen im Datenschutzmanagement sind gesetzlich vorgegeben. Was diese organisatorischen Anforderungen an den Datenschutz angeht, wird die Anlage zu § 9 des BDSG sehr konkret. Der Wortlaut dieser Anlage nachfolgend *(Hervorhebung „fett“ durch Autor):*

„Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

*1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),*
*2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),*
*3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),*
*4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtung zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),*
*5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),*
*6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),*
*7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),*
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.“ **(Trennung der Daten nach Zwecken)**

5. Psychologische und pädagogische Herausforderungen

Datensicherheit ist insgesamt also nur zum Teil ein technisches Problem. Zwar ist die Technik bezüglich Hard- und Software-Sicherheit noch lange nicht ausgereift und wird es sicherlich niemals ganz und gar sein. Die meisten bestehenden technischen Sicherheitsmöglichkeiten werden jedoch nicht ausgeschöpft, weil die Computer-Anwender/innen sich der Problematik nicht bewusst sind und nicht zielgerichtet Abhilfe schaffen.

Das Ausmaß der Sicherheitsproblematik wird gemeinhin unterschätzt. Gründe dafür liegen am mangelnden Risikobewusstsein. Erst durch die weltweite Vernetzung im Internet kam es zu einer neuen Bedrohung, die es bei den früher relativ abgeschotteten einzelnen Netzwerken so nicht gab. Außerdem handelt es sich um ein relativ neues Erfahrungsfeld. Aufgrund weniger eigener negativer Erfahrungen, ist die mögliche Gefahr nicht im Bewusstsein. Bedrohungen werden in anderen (nicht medialen) Zusammenhängen selbst erlebt, und sei es nur durch die Wahrnehmung anderer, die affektiv auf Gefahrensituationen reagieren. Die noch vorherrschenden durchschnittlich geringen Computerkenntnisse tragen ebenfalls dazu bei, die Risiken zu unterschätzen.

Das teilweise irrationale Vertrauen ausschließlich in technische Lösungen ist ein weiterer Punkt, der für sichere Prozesse nicht angemessen ist. Selbst in technologienahen Unternehmen kommt es vor, dass der Begriff „Firewall“ wie ein Zauberwort verwendet wird: "Wir haben eine Firewall - uns kann nichts passieren".

Eine Firewall (bzw. Sicherheitsgateway) ist in der Realität jedoch nur ein (wenn auch zentraler) Teil eines Gesamtkonzepts, das nicht wirksamer sein kann als der Kenntnisstand der Beteiligten. Selbst eine Firewall macht dabei nur Sinn, wenn sie von Menschen angemessen kon-

figuriert und gewartet wird und in ein Gesamtkonzept eingebunden ist. Zentrale Sicherheitsfaktoren sind also die Sicherheitskompetenzen der Mitarbeitenden: Grundkenntnisse der Sicherheitsfragen müssen vorhanden sowie Mindeststandards verbindlich sein. Diese umfassen die Bereiche der sicheren Datenübermittlung ebenso wie Aspekte der Sicherheit der Daten auf den lokalen PCs und dem Rechner der Beratungseinrichtung. Die Erfahrung in Unternehmen mit sensiblen Daten zeigt, dass die Schulung der Sicherheitskompetenzen der Mitarbeitenden die wichtigste Herausforderung darstellt, da das Sicherheitsbewusstsein die kritische Variable im gesamten Sicherheitskonzept darstellt. Die gezielte Weiterbildung der Mitarbeitenden ist deshalb ein zentraler Punkt eines Sicherheitskonzeptes. Ein hohes Maß an Sicherheit ist nur zu gewährleisten, wenn den Mitarbeitenden die verschiedenen Sicherheitsaspekte bekannt sind und die aktuellen Sicherheitsstandards eingehalten werden.

Dabei gilt es vor allem die Beteiligten in diesem Prozess „mitzunehmen“. Nachhaltig sind Datenschutz und Datensicherheit in einer Organisation nur voranzutreiben, indem den Verantwortlichen und Mitarbeitenden die entsprechenden Regelungen plausibel sind. Dann sind Menschen auch bereit, mitzuwirken, um Sicherheit und Datenschutz als Recht der beteiligten Personen weiterzuentwickeln.

6. Gesamtkonzept notwendig

Für die wirksame Implementierung eines Datenschutzmanagements bedarf es eines Gesamtkonzepts, das auf die jeweilige Situation angepasst wird und Datenschutz und Datensicherheit prozesshaft begreift. Im Sewecom-Verfahren (secure web communication) habe ich die wichtigsten Eckpunkte für ein Gesamtkonzept sicherer und datenschutzverträglicher Online-Beratung allgemein beschrieben und veröffentlicht (Wenzel 2003b). Die nachfolgenden Punkte sollten dabei jedoch nicht unkritisch von Organisationen übernommen werden. Sie können vielmehr als erste Anhaltspunkte dienen, wobei vor allem der jeweiligen Situation (rechtlich, technisch und organisatorisch) entsprochen werden muss.

A) Organisation
A1) Gesamtkonzept erforderlich
A2) Leitungsebene der Organisation ist eingebunden
A3) Konkretes Datenschutz- und Sicherheitskonzept: Prozesse definieren
A4) Datenschutz- und Sicherheitsbeauftragte
A5) Interne Datenschutz- und Sicherheitsrichtlinien definieren
A6) Schulung der Mitarbeiter/innen
A7) Mehrstufige Sicherheitsebenen
A8) Beteiligte PCs, Software und Netzwerke
A9) Strategisches Informations- und Kommunikationskonzept

B) Internet-Technik
B1) Mögliches Problem: Outsourcing
B2) Technische Sicherheits-Infrastruktur
B3) Sichere Server-Infrastruktur
B4) VPN - virtual private network
B5) Administrative Zugänge zu Servern besonders gesichert
B6) Kommunikationslösung geschieht webbasiert
B7) SSL-Server-Zertifizierung nach Signaturgesetz
B8) Intranet besonders gesichert
B9) Systemüberwachung

C) Darstellung nach Außen
C1) Aufklärung der Nutzer über Risiken durch ihren eigenen PC
C2) Erklärung zu Datenschutz und Datensicherheit / Privacypolicy

D) Varianten: Anonymität / Authentizität
D1) Organisation authentifiziert / Nutzer anonym
D2) Organisation authentifiziert / Nutzer authentifiziert

7. Entwicklungstendenzen von Online-Beratung und Ausblick

Die gezeigte Vielschichtigkeit von Datenschutz- und Qualitätsmanagement macht deutlich, dass es für einzelne Online-BeraterInnen, aber auch für kleinere Beratungsstellen kaum möglich sein dürfte, den komplexen Anforderungen mangels zeitlicher und finanzieller Ressourcen alleine gerecht zu werden. Es bedarf bei diesen Anforderungen einer infrastrukturellen Unterstützung, die etwa von Kammern und Verbänden geleistet werden kann. Insbesondere der Bedarf an multiprofessioneller Kompetenz macht es notwendig, Unterstützungssysteme zur Weiterentwicklung der Qualität und des Datenschutzes von Online-Beratung zu nutzen. Größere Verbände und Beratungsanbieter haben für den eigenen Bereich bereits Qualiltätsstandards entwickelt. Diese beziehen sich u.a. auf Rahmenbedingungen, Sicherheits- und Datenschutzaspekte, Aus- und Weiterbildung etc. Darüber hinaus zeichnet sich aber auch bereits eine übergreifende Verständigung über konkrete Standards ab. Dies wird beispielsweise in der Gründung der Deutschen Gesellschaft für Online-Beratung (DGOB) und der Österreichischen Gesellschaft für Online-Beratung (ÖGOB) deutlich. Die DGOB hat beispielsweise verbindliche Zertifizierungsrichtlinien für die Weiterbildung in Online-Beratung verabschiedet. Reiners (2005) benennt eine Rahmenempfehlung „Qualitätsmerkmale der Internet-Beratung für Eltern, Kinder, Jugendliche, und für Mitarbeiter in sozialen und pädagogischen Berufsfeldern“. Bei dieser Rahmenempfehlung aus dem Jahre 2003 haben Vertreter unterschiedlicher Verbände und Einrichtungen mitgewirkt. Bezogen auf Datenschutz und Datensicherheit kristallisiert sich bei den unterschiedlichen Standards und Empfehlungen bezüglich Online-Beratung heraus, dass von Anbieterseite aus für einen sicheren „virtuellen Beratungsraum“ etwa durch obligatorische SSL-Verschlüsselung zu sorgen ist. Dies deckt sich auch mit den Einschätzungen und Forderungen namhafter unabhängiger Datenschützer und Sicherheitsexperten (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein 2005 / Bundesamt für Sicherheit in der Informationstechnik 2004).

7.1 Globalisierung von Qualitäts- und Sicherheitsstandards

Entsprechend der Globalisierung der Technik und des Rechts (Lutterbeck 2000 / Rieß 2002) haben auch Qualitäts-, Sicherheits- (A Campo 2005) und Datenschutzstandards eine Tendenz zur Globalisierung. Rechtsnormen aber auch Regulierungen jenseits des Rechts wie transnationale Standards bewirken, dass in vielen Bereichen eine Angleichung geschieht. So wurden die ISO-Normen in unzählige nationale Normen übernommen. Auch in Europa geschieht eine fortschreitende Harmonisierung hinsichtlich Normierung (z.B.: EN ISO 9000ff), aber auch bezüglich gesetzlicher Regelungen.

Die Beauftragten für Datenschutz und den Schutz der Privatsphäre sind auf ihrer 27. Internationalen Konferenz 2005 in Montreux (14. bis 16. September 2005) übereingekommen, die Anerkennung des universellen Charakters der Datenschutzgrundsätze zu fördern, und haben eine Schlusserklärung „Ein universelles Recht auf den Schutz personenbezogener Daten und

der Privatsphäre unter Beachtung der Vielfalt in einer globalisierten Welt“ verabschiedet (Erklärung von Montreux).

Diese Form der Globalisierung zeigt, dass Normen vor Ort tendenziell an Bedeutung verlieren gegenüber übergreifenden Regelungen. Dieser Trend bedeutet in der Konsequenz, dass es beim Qualitäts- und Datenschutzmanagement immer wichtiger wird, größere Entwicklungstendenzen zu verfolgen, will man nicht permanent von den technischen Entwicklungen überholt werden.

7.2 Ausblick: Mitgestaltung und Humanisierung der Technik

Thiery (2005) beschreibt die Entwicklung der medialen Beratung „Von der Telefonseelsorge zur Beratung im Netz“. In dieser Betrachtung wird sehr anschaulich, dass die Entwicklung medialer Beratung sehr stark abhängig von der Entwicklung der Technik ist. Dieser Zusammenhang gilt natürlich nicht nur für Beratung, sondern für Kommunikationsverhalten generell und für Entwicklungen in den unterschiedlichsten Bereichen menschlichen Lebens. Manuel Castells hat diese ineinander verwobenen Zusammenhänge in seinem Werk „Das Informationszeitalter“ detailliert dargestellt. Am Ende dieser Trilogie schreibt er: *„Die Rekonstruktion der Institutionen der Gesellschaft durch kulturelle soziale Bewegungen, die die Technologie unter die Kontrolle der Bedürfnisse und Wünsche der Menschen bringt, scheint einen langen Marsch zu erfordern“*. (2003, S. 404)

Qualifizierte Online-Beratung muss sich also bewusst den Herausforderungen der Technik stellen. Dies dürfte allerdings für die psychosoziale Beratung insgesamt gelten, da Tendenzen zu entdecken sind, dass die face-to-face-Beratung immer häufiger medial eingeleitet oder in Form von Nachbetreuung ausgedehnt wird. Dabei gilt es insgesamt die beraterische Kommunikation per Telefon und/oder Internet in die Beratungskonzepte zu integrieren. Häufig werden jedoch beraterische Interventionen noch gar nicht als mediale Beratung begriffen und reflektiert (z.B. Terminvereinbarung zur ersten Beratungssitzung). Aktuelle kommunikationstechnische Entwicklungen scheinen diese Notwendigkeiten noch zu beschleunigen. So etwa durch die Entwicklung so genannter Konvergenz von Informationstechnologie. Das bedeutet, dass alle möglichen Formen medialer Kommunikation immer stärker in ein Gerät integriert werden. Dadurch entsteht eine Vereinheitlichung der Kommunikationsstandards (zumindest auf Anwenderebene). Die unterschiedlichsten medialen Kommunikationsformen (Mail, Chat, Foren, Videokonferenz) können beispielsweise in einem Browser geführt werden. Hinzu kommt die voranschreitende Miniaturisierung der Kommunikationstechnologie. Dies führt in den nächsten Jahren dazu, dass sich neue Kommunikationsgeräte etablieren, die bisher getrennte Medien mobil zusammenführen (Handy, PC, TV). Eine Folge davon ist beispielsweise, dass die Unterscheidung E-Mail vs. SMS in absehbarer Zeit keinen Sinn mehr machen wird, wenn die Mobiltelefone weitgehend die Computerfunktionalität übernommen haben. Die Verknüpfung verschiedener medialer Kommunikationskanäle wird dann immer einfacher möglich sein, so dass auch während einer bestimmten Kommunikation ein unmittelbarer Medienwechsel sehr leicht machbar sein wird.

Will man der Technik nicht ausgeliefert sein, ist beim Qualitäts- und Datenschutzmanagement proaktives Handeln notwendig, um den Herausforderungen gerecht zu werden, die durch eine immer schnellere Technikentwicklung entstehen. Proaktivität bedeutet dabei ein *„frühzeitiges und differenziertes Vorbereiten auf mindestens zwei unterschiedliche Umweltkonstellationen oder bewusstes Gestalten ausgewählter strategischer Tatbestände in eine Richtung“* (Scholz 2000).

Beispiele für proaktive Gestaltung hinsichtlich technischem Datenschutz wurden bereits aufgezeigt (P3P, JAP/ANON, Seweocm-Verfahren).

Die komplexen Anforderungen an ein wirkungsvolles und somit vorausschauendes Datenschutz- und Qualitätsmanagement sind hoch und bedürfen nicht unerheblicher zeitlicher und materieller Ressourcen, die einzelne Beratungseinrichtungen und erst recht Freiberufler nicht einbringen können. Im Sinne von Castells wird es schließlich einen langen Marsch bedeuten, bis die Kommunikationstechnologie unter die Kontrolle der Bedürfnisse und Wünsche der Menschen gebracht ist. Kräfte in diese Richtung durch Kooperation und synergetische Konzepte zu mobilisieren wird die Herausforderung der nahen Zukunft sein.

Dies ist für den Bereich psychosozialer Beratung und für Freiberufler voraussichtlich nur zu bewerkstelligen durch ein konstruktives Zusammenwirken gestaltender Kräfte aus der Online-Beratungspraxis, aus den verschiedenen beteiligten Verbänden, aus dem Bereich Datenschutz aber auch aus Wissenschaft, Politik und Wirtschaft.

Viele Wirtschaftsunternehmen haben frühzeitig in ein wirksames Sicherheitsmanagement investiert. Der Staat holt auf beim Sicherheitslevel der Behörden im Zuge der Entwicklung des E-Governments. Durch Investitionen im mehrstelligen Millionenbereich und behördenübergreifende Projekte wie BundOnline wird die staatliche Infrastruktur an das Informationszeitalter angepasst. Dies ist im sozialen Bereich entsprechend noch nicht abzusehen und es bleibt abzuwarten, wie sich dies beispielsweise auf die Wettbewerbsfähigkeit sozialer Organisationen im sich öffnenden sozialen Markt auswirken wird.

Ressourcen zu mobilisieren und Synergie-Effekte zu konstellieren, um auch die Kommunikationstechnik auf unterschiedlichen Ebenen – im Dienste der Beratungsqualität und Sicherheit – mitgestalten zu können, scheint zur Zeit die vordringliche Aufgabe von Datenschutzmanagement und Qualitätsmanagement bei Online-Beratung zu sein, zum Wohle der zu beratenden Menschen.

Literatur

A Campo, M. (2005): Kombinierte Sicherheit. ISO17799 und BSI-Grundschutzhandbuch im Duett. In: <kes>. Die Zeitschrift für Informationssicherheit. 21. Jahrgang. Nr. S. 13-15. Ingelheim.

Bundesamt für Sicherheit in der Informationstechnik [BSI] (Hrsg.) (2004): IT-Grundschutzhandbuch. Bonn.
Elektronische Ressource: http://www.bsi.bund.de/gshb/deutsch/index.htm

Bundesamt für Sicherheit in der Informationstechnik [BSI] (Hrsg.) (2004): Sichere Kommunikation imE-Government. Modul aus dem E-Government-Handbuch. Bonn.
Elektronische Ressource:
http://www.bsi.de/fachthem/egov/download/4_SiKomm.pdf

Castells, M. (2003): Jahrtausendwende. Teil 3 der Trilogie. Das Informationszeitalter. Opladen .

Combe, A. / Helsper, W. (Hrsg.) (1997): Pädagogische Professionalität. Untersuchungen zum Typus pädagogischen Handelns. Frankfurt a.M.

Dzeyk, W. (2005): Vertrauen in Internetangebote: eine empirische Untersuchung zum Einfluss von Glaubwürdigkeitsindikatoren bei der Nutzung von Online-Therapie- und Online-Beratungsangeboten. Köln
Elektronische Ressource: http://deposit.ddb.de/cgi-bin/dokserv?idn=130817554

Die Beauftragten für Datenschutz und den Schutz der Privatsphäre (2005): Erklärung von Montreux: „Ein universelles Recht auf den Schutz personenbezogener Daten und der Privatsphäre unter Beachtung der Vielfalt in einer globalisierten Welt“. Montreux
Elektronische Ressource:
http://www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_d.pdf

Gerull, P. (2000): Hand- und Werkbuch Soziales Qualitätsmanagement. Hannover.

Gerull, P. (2005): Qualitätsmanagement in der Jugend- und Sozialhilfe. Literaturanalytische und empirische Studien. Göttingen.
Elektronische Ressource: http://webdoc.sub.gwdg.de/diss/2005/gerull/gerull.pdf

Heyder, J.-U. / Atts, M. (2005): Aktive Inhalte. Sichere Nutzung – Überblick und Empfehlungen. In: BSI Forum. Organ des Bundesamtes für Sicherheit in der Informationstechnik. 13. Jahrgang. S. 54-58. Bonn . Bestandteil von: <kes>. Die Zeitschrift für Informationssicherheit. 21. Jahrgang. Nr. 6. S. 13-15. Ingelheim 2005.

Koch, F.A.: Internet-Recht (2005): Praxishandbuch zu Dienstenutzung, Verträgen, Rechtsschutz und Wettbewerb, Haftung, Arbeitsrecht und Datenschutz im Internet, zu Links, Peer-to-Peer-Netzen und Domain-Recht, mit Musterverträgen. Oldenbourg.

Lutterbeck, B. (2000): Globalisierung des Rechts - am Beginn einer neuen Rechtskultur? In: Computer & Recht. Seite 52-60. Köln

Merchel, J. (2001): Qualitätsmanagement in der Sozialen Arbeit. Ein Lehr- und Arbeitsbuch. Münster

Münch, I. (2005): Neue Grundschutzgeneration. Vom IT-Grundschutzhandbuch zu den BSI-Standards für das IT-Sicherheitsmanagement. In: <kes>. Die Zeitschrift für Informationssicherheit. 21. Jahrgang. Nr. 6. S. 6-12. Ingelheim.

Reiners, B. (2005): E-Mail-Beratung in der Jugendhilfe. Ein Handbuch für die Fortbildung. Nach dem Modell der Kinderschutz-Zentren. Eigenverlag der Bundesarbeitsgemeinschaft der Kinderschutz-Zentren [Hrsg.]. Köln

Rieß, J. (2002): Globalisierung und Entgrenzung des Rechts. Baustellen globaler Architekturen des Rechts. In: Bizer, J. / Lutterbeck, B. / Rieß, J. (Hrsg.) (2002): Umbruch von Regelungssystemen in der Informationsgesellschaft. Freundesgabe für Alfred Büllesbach. Stuttgart
Elektronische Ressource: http://www.alfred-buellesbach.de

Rost, M. (2005): Welches Gesetz gilt eigentlich? Kiel
Elektronische Ressource:
http://www.datenschutzzentrum.de/systemdatenschutz/meldung/sm91.htm

Schaar, P. (2002): Datenschutz im Internet. Die Grundlagen. München

Schleipfer, St. (2004): Das 3-Schichten-Modell des Multimediadatenschutzrechts. In: DuD - Datenschutz und Datensicherheit. Jahrgang 28. Nr. 12. S. 727-733. Wiesbaden

Scholz, Ch. (2000): Personalmanagement. Informationsorientierte und verhaltenstheoretische Grundlagen. München

Hoeren, T. /Sieber, U. (Hrsg.) (1998): Handbuch Multimedia-Recht. Rechtsfragen des elektronischen Geschäftsverkehrs. Loseblattsammlung. München

Späth, K. (1999): Erwartungen an die neuen Regelungen der §§ 78 a-g KJHG. In: Jugendwohl 2, S. 59-69. Freiburg i. Br.

Thiery, H (2005): Von der Telefonseelsorge zur Beratung im Netz. München 2005.
Elektronische Ressource:
http://www.jff.de/dateien/Telefonseelsorge_bis_Onlineberatung.pdf

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Hrsg.): 27. Tätigkeitsbericht des Landesbeauftragten für Datenschutz und Informationsfreiheit. Kapitel 7.5. Sensitive Internetberatung. Kiel
Elektronische Ressource: http://www.datenschutzzentrum.de/download/tb27.pdf

Wenzel, J. (2003): Telefonseelsorge. In: Helmut Bäumler, Astrid Breinlinger, Hans-Hermann Schrader (Hrsg.) (1999): Datenschutz von A - Z. (7. Lfg.). Gruppe T 350. S. 1-4. Neuwied / Kriftel (Loseblattsammlung, Grundwerk).

Wenzel, J. (2003): Vertraulichkeit und Anonymität im Internet. Problematik von Datensicherheit und Datenschutz mit Lösungsansätzen. In: Elmar Etzersdorfer, Georg Fiedler, Michael Witte (Hg.): Neue Medien und Suizidalität - Gefahren und Interventionsmöglichkeiten. S. 56-70. Göttingen.

Links

Genannte Einrichtungen, Projekte, Portale:

ANON/JAP
http://anon.inf.tu-dresden.de
www.datenschutzzentrum.de/projekte/anon

Bundesamt für Sicherheit in der Informationstechnik
www.bsi-fuer-buerger.de
www.bsi.bund.de

BundOnline - Wissensmanagement
www.wmsbundonline.de

Deutsche Gesellschaft für Online-Beratung
www.dg-online-beratung.de

P3P
www.datenschutzzentrum.de/p3p

Sewecom-Verfahren
www.sewecom.de/sewecom-verfahren
www.sewecom.de/pc (Sicherheits-Tipps für Nutzer)

TelefonSeelsorge
www.telefonseelsorge.de

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
www.datenschutzzentrum.de

Virtuelles Datenschutzbüro
www.datenschutz.de

Weitere Ressourcen:

Datenschutz in der Europäischen Union
http://europa.eu.int/comm/justice_home/fsj/privacy/index_de.htm

Der Datenschutzbeauftragte des Kantons Zürich:
www.datenschutz.ch

Der Eidgenössische Datenschutzbeauftragte (EDSB):
www.edsb.ch/d/gesetz/schweiz

Datenschutz in der katholischen Kirche
www.datenschutz-kirche.de

Österreichische Datenschutzkommission:
www.dsk.gv.at

Rechtsinformationssystems (RIS) der Republik Österreich:
www.ris.bka.gv.at

”