

# Datenschutz durch Selbstregulierung und Qualitätskontrolle

Vortrag von Rechtsanwalt Lukas Fässler, Zug  
anlässlich des Anwaltskongress 2001  
des Schweizerischen Anwaltsverbandes SAV in Luzern am 23. Juni 2001.

---

1. **Einleitung und Themenabgrenzung**
2. **Selbstregulierung im Internet**
3. **Selbstregulierung im Datenschutz**
4. **Standardisierung über CEN / ISO**
5. **Internationale Vertrauensinitiative e-comtrust**

|                       |   |
|-----------------------|---|
| Dokument              | C:\Eigene Dateien\Anwaltstag2001\Vortrag.doc                        |
| Version:              | 2.0   |
| Datum:                | 17.2.2002   |
| Ersetzt Dokument vom: | Version 1.0 vom 22.6.2001   |
| Autor:                | © lic.iur. Lukas Fässler, Rechtsanwalt, Artherstrasse 23a, 6300 Zug |
| Letzte Änderung von:  | 17.2.2002   |
| Autorisiert:          | Lukas Fässler   |
| Freigabe am:          | 17.2.2002   |

# 1. Einleitung

Solange das Internet noch die Spielwiese der Universitäten war - lange bevor Vizepräsident Al Gore den „Information Superhighway“ als Ziel der amerikanischen Regierung ausgerufen hatte -, war es der „Ort“, an dem alles möglich war. Von staatlichen Stellen unbehelligt und auch unbemerkt entwickelte sich das „Netz der Netze“ zum Kommunikationsmedium - nicht nur für Computerfreaks, sondern auch für Gesellschaftskreise, die ansonsten von Massenkommunikationsmitteln eher ausgeschlossen waren. Schon in dieser Zeit entwickelten sich auf der Basis freiwilliger Selbstbeschränkung und gegenseitig kommunizierter Abmachungen gewisse Grundverhaltensweisen, welche von allen Teilnehmern als Mindestvoraussetzungen für einen geordneten Ablauf und einigermaßen standardisierte Verhaltensweisen anerkannt und eingehalten wurden.

Doch inzwischen ist das Internet den Universitäten entwachsen, hat seine militärischen Wurzeln abgelegt und hat sich zu einem weltumspannenden Massenkommunikationsmittel entwickelt.

Kein Wunder also, wenn das Internet weiterhin exponentiell wächst. Damit hat das Netz aber auch gesellschaftliche und politische Bedeutung erhalten. Politische Bedeutung meint in diesem Sinne vor allem auch Bedeutung für die Politik. Die beginnende Berichterstattung beschränkte sich mangels tieferen Verständnisses des Internet auf Sensationelles, wie Pläne zum Bombenbauen oder pornographische Inhalte. Nicht zuletzt durch solche Berichte wachgerüttelt, wurde weltweit begonnen, an **Regulierungen** für dieses unkontrollierte, dynamisch wachsende Phänomen „Internet“ zu arbeiten. Und so war die Internetberichterstattung erstmals ab dem Jahre 1996 weltweit geprägt von den ersten Zensur- und Regulierungsversuchen, die auch im *Netz* selbst sehr eifrig diskutiert wurden<sup>1</sup>.

Das Internet gehört neben dem Telefonnetz zu den komplexesten technischen Artefakten, die je von Menschen ersonnen und verwirklicht worden sind. Es mangelt jedoch an passenden Modellen, um Organisations- und Funktionsweise dieses Netzes in seiner gesamten Vielfalt darstellen zu können. Nicht zuletzt aus diesem Grund wird das Internet von vielen Personen als 'ziemlich anarchistisch' angesehen.

Eine gewisse Plausibilität gewinnt diese Einschätzung bereits bei der Betrachtung grundlegender *technischer Aspekte* des Netzes. Sieht man nämlich von der Vergabe der Domain- und Hostadressen einmal ab, so unterliegt das **Gesamtsystem keiner zentralen Administration und Kontrolle**. Welche Services auf einem Host zur Verfügung stehen und in welchem Umfang sie genutzt werden können, liegt allein im Ermessen der Hostbetreiber und Systemadministratoren. **Weitestgehende Dezentralisierung** ist eine der fundamentalen strukturellen Eigenschaften des Internet und wird von einigen seiner Protagonisten als richtungsweisend für zukünftige Formen von Telekommunikation angesehen:

Anarchistisch anmutende Zustände lassen sich auch in der *Struktur der Informations- und Kommunikationsbeziehungen* im Internet nachweisen. Das Internet ist das erste Medium, das gleichzeitig Individual- und Massen-, synchrone und asynchrone, angebots- und nachfrageorientierte, moderierte und unmoderierte, personalisierte und anonyme, offene und verschlüsselte Kommunikation unterstützt. Jeder Informationskonsument ist potentieller Informationsproduzent. Nicht Macht- und Verwertungsinteressen, sondern persönliche Vorlieben und freier Zusammenschluß mit Gleichgesinnten, argumentative und inhaltliche Kompetenz der Beteiligten und ausgeprägter Gemeinssinn sind bis heute bestimmend für die Informationskultur im Internet<sup>2</sup>.

Anarchistischer Wildwuchs ist besonders bei den über Internet verfügbaren *Informationsinhalten* zu beobachten. Ein Kunterbunt von News-Gruppen und Datenarchiven deckt heute jedes nur vorstellbare Thema ab. Die über Internet verfügbaren Daten bilden -- zusammen mit den im Netz agierenden Menschen und deren spezifischen Fähigkeiten -- einen Korpus, auf den jede angeschlossene Person Zugriff besitzt und zu dem sie beitragen kann. Die Frage nach den Besitzverhältnissen an diesem Korpus verfehlt offensichtlich dessen Wesen<sup>3</sup>.

---

<sup>1</sup> Christian Obad, Meinungsfreiheit und Zensur im Internet; Hausarbeit im Proseminar 28 730; Sommersemester 1996 (<http://paedpsych.jk.uni-linz.ac.at/PAEDPSYCH/NETLEHRE/NETLEHREL.../Obad96.htm>)

<sup>2</sup> Steve Stecklow, Computer Users Battle High Tech Marketers Over Soul of Internet.. Wall Street Journal, 16.9.94 Zitiert nach: Michael Hauben, The Netizens And The Wonderful World Of The Net. Literary Freeware, 1994

<sup>3</sup> Gero Hoffmann, Dirk Kuhlmann: Das Projekt Internet / Regulierung und Selbstregulierung im Internet; Netiquette, Nutzungsregeln, Rechtsvorschriften, Verträge; Technische Universität Berlin, Forschungszentrum für Netzwerktechnologie und Multimedia-Anwendungen; German Version July 1994.

Standen zu Beginn der gelebten Existenz des Internet vor allem die Mindestverhaltensabmachungen unter Gleichgesinnten im Vordergrund, hat sich das Prinzip der Selbstregulierung im Internet jedoch bis heute nicht nur gehalten, sondern ganz stark als ein quasi internet-eigenes Prinzip verwirklicht. Das beigetragen hat in den Anfängen des Internet die Internetgemeinde selber, die jede staatliche oder regulatorische Einmischung als Angriff auf die Autonomie des Internets als freien Kommunikationsraum vehement zurückgewiesen hat. Diese starke Verteidigungshaltung hat in der Folge dazu geführt, dass sich zunehmend auch der Gesetzgeber mit diesem Prinzip auseinandergesetzt hat und sich dessen Existenz im Internetumfeld selber zu nutze gemacht hat. Heute verweist selbst der Gesetzgeber z.B. in der europäischen Union (EU) oder auch in der Schweiz explizit darauf, dass in gewissen zugewiesenen Regelungsräumen anstelle der hoheitlichen Reglementierung die Selbstregulierung durch die Online-Anbieter und Konsumenten, insbesondere durch deren Verbände, Organisationen und Interessensgemeinschaften wahrzunehmen ist.

In der Folge soll gezeigt werden, wie sich dieses Prinzip der Selbstregulierung auch im Bereich des Datenschutzes zunehmend durchzusetzen beginnt und mit welcher Konsequenz solche Selbstregulierung behaftet ist.

## 2. Selbstregulierung im Internet

### 2.1. Ein Modell

Das Fehlen eines *master plan*, eines übergeordneten Entwurfs, ist es, was die Beschreibung der im Internet wirksamen Regulationsmechanismen schwierig macht. Dies führt leicht zu ad hoc Etikettierung wie "anarchistisch". Solange jedoch unklar ist, worin die funktionalen und strukturellen Grundlagen des Netzes bestehen, kann die Rolle von Gesetzen, Verordnungen, Verträgen und Netiquette für das Internet nur schwer eingeschätzt werden<sup>4</sup>.

Ich versuche trotzdem, ein Erklärungsmodell als Arbeitshypothese darzustellen. In dem von Gero Hoffmann und Dirk Kuhlmann<sup>5</sup> bereits im Juli 1994 vorgeschlagenen Modell werden drei Ebenen des Internet unterschieden. Dieses Erklärungsmodell basiert auf der Hypothese, die besagt, daß die **Nutzungskultur (Informationsinhalte)** des Internet neben der **technischen Infrastruktur** eine eminent wichtige Rolle für die Regulierungs- und Selbstregulierungsprozesse spielt.

Dabei liegt es nahe, die Betrachtung der **technischen Infrastruktur** von derjenigen der **Informationsinhalte** zu trennen, die über diese Infrastruktur zur Verfügung gestellt werden. Diese Trennung hat sich - zumindest in den USA - als *common carrier* Prinzip bis in die Gesetzgebung hinein durchgesetzt. Zwischen diesen beiden Ebenen ist eine weitere angesiedelt, die Aspekte der **Strukturierung von Information und Konventionen der Nutzung** des Netzes umfaßt. Eine eindeutige Zuordnung einzelner Regulierungsgegenstände und -instrumentarien zu einer dieser Ebenen kann nicht immer getroffen werden.

Auf den drei verschiedenen Ebenen werden die behandelten Regulationsinstrumente (Gesetze, Verträge, Nutzungsordnungen, Netiquette) in unterschiedlichem Umfang wirksam. Der Zusammenhang zwischen Regulierungsebenen und -instrumenten wird durch Abb. 1 (im Anhang) graphisch veranschaulicht.

Aus diesem Modell ist bisher noch nicht ersichtlich, welche Handlungsträger von Regulierungsmaßnahmen betroffen sind und welche Reichweite für Regulierungen gilt. Es muß daher um ein Modell ergänzt werden, das die verschiedenartigen Beziehungen im Internet und die verschiedenen Regulierungsdomänen sichtbar macht. Dies soll durch Abb.2 (im Anhang) verdeutlicht werden.

Customer-Provider Beziehungen sind in aller Regel innerhalb eines gemeinsamen Rechtsraumes angesiedelt und werden im Einzelnen durch Verträge und Nutzungsbestimmungen geregelt. Dies ist bei Customer-Customer Beziehungen oft nicht gegeben. Diese sind in der Regel weder an gemeinsame Verträge und Bestimmungen gebunden noch den gleichen rechtlichen Rahmenbedingungen unterworfen.

---

<sup>4</sup> Gero Hoffmann, Dirk Kuhlmann; a.a.O.; Kapitel 1

<sup>5</sup> Gero Hoffmann, Dirk Kuhlmann: Regulierung im Internet: Ein Modell; Technische Universität Berlin, Forschungszentrum für Netzwerktechnologie und Multimedia-Anwendungen; German Version July 1994

Ihre Beziehungen sind informationeller Natur und werden weniger durch juristische Rahmenbedingungen als durch Fragen des Umgangs, des Stils und der ausgetauschten Inhalte geprägt.

Die Einteilung *Provider* und *Customer (User)* ist allerdings nicht unproblematisch, da Personen und Personengruppen in elektronischen Netzen oft beide Funktionen gleichzeitig wahrnehmen. Provider nehmen in der Regel Dienste anderer Anbieter in Anspruch. Nutzer von Internet-Diensten können ihrerseits als Informationsanbieter fungieren. Wenn wir die Einteilung in Provider und User trotzdem für nützlich halten, dann deswegen, weil zwischen zwei Providern bzw. zwischen Providern und Usern in der Regel andere Regulierungsmechanismen eine Rolle spielen als zwischen Usern.

## 2.2. Evolution der Nutzungskultur im Usenet

Erste Schritte in Richtung einer geordneten und geregelten Selbstregulierung konnten im Internet-Dienst des **Usenet** beobachtet werden. Bei Usenet handelt es sich also um eine Anzahl von mehreren tausend Interessengruppen, deren Mitglieder auf elektronischem Wege Nachrichten miteinander austauschen. Jede Person, die Zugang zu Usenet hat, kann sämtliche Nachrichten jener News-Foren lesen, die auf dem Rechner seines Providers zur Verfügung gestellt werden. Abgesehen von ihren thematischen Schwerpunkten werden moderierte und unmoderierte Gruppen unterschieden. Bei ersteren werden Beiträge, die innerhalb des elektronischen Forums veröffentlicht werden sollen, zuerst an den Moderator des Forums gesandt. Diese(r) entscheidet darüber, ob der Artikel öffentlich gemacht wird. In unmoderierten Gruppen erscheint ein Beitrag ohne vorherige Kontrolle.

In diesem Umfeld entstanden die ersten Formen der Selbstregulierung durch das Aufstellen von sogenannten **Netiquetten**, **Posting-Guides** oder die Bereitstellung von **FAQ's** (Frequently asked Questions). Sie sind nicht als Usenet-Gesetze, sondern als Hilfsmittel zur Tradierung einer Kultur der Techniknutzung und zur Einübung bestimmter sozialer Fähigkeiten zu verstehen. Im von Ron Dippold im Mai 1994 verfassten „*Usenet Newsgroup Creation Companion*“<sup>6</sup> wurde denn auch schon auf diesen Wertcharakter hingewiesen:

*„This is not in any way an official document, it has no force of law – rather it helps you with the informal conventions which have evolved over the years...“*

### 2.2.1. Netiquette

Am stärksten ausgebildet wird der Selbstregulierungscharakter in den sogenannten „Netiquette“. Netiquette und verwandte Dokumente können als Versuch angesehen werden, das in den Köpfen der treibenden Internet-Kräfte vorhandene traditionelle Wissen der gesamten „Netzgemeinde“ zugänglich zu machen. Neben die Erfahrung einer gemeinsamen Praxis der Techniknutzung tritt das Wissen um eine gemeinsame kulturelle Geschichte und bestimmte Werte, die sich in ihrem Verlauf herausgebildet haben und die an alle Teilnehmer zur Einhaltung und Befolgung weitergegeben werden sollen. Netiquette ist damit der Ausdruck einer Kultur der Techniknutzung. Sie macht Handlungskonventionen explizit, die älter sind als ihre schriftliche Abfassung. Und sie tradiert die Geschichte der technischen Entwicklung, der Strukturierung von Kommunikation und der verhandelten Inhalte<sup>7</sup>.

Aus der Umgebung des Usenet heraus haben Netiquette den Weg auch in andere Dienstbereiche des Internet gefunden. So insbesondere in den [www.Dienst](#) oder den eMail-Dienst. Als Beispiel dafür kann die Netiquette des damaligen Wirtschaftsinformatik-Fachverbandes WIF angeführt werden, welche zu Beginn der Internet-Euphorie in der Schweiz zusammen mit SWITCH, der Domain-Name Registrierungsorganisation in der Schweiz herausgegeben wurde. In der Einleitung dieses Dokumentes wird ausdrücklich darauf hingewiesen, dass es

*„entgegen einer weit verbreiteten Meinung durchaus so ist, dass auch im virtuellen Raum die Gesetze der realen Welt volle Geltung haben. Der Schutz der Persönlichkeit oder der Urheberrechte zum Beispiel, gilt auch hier ohne Einschränkung. Die Netiquette, wie das ungeschriebene Gesetz des Cyberspace oft auch bezeichnet wird, ist als Ergänzung zu diesen Gesetzen zu verstehen. Ähnlich wie in jeder Kultur neben den geschriebenen Gesetzen auch die ungeschriebenen Verhaltensregeln und der gesunde Menschenverstand*

<sup>6</sup> Ron Dippold, *The Usenet Newsgroup Creation Companion*, Version 1.07; news.answers, 18 May 1994

<sup>7</sup> Gero Hoffmann, Dirk Kuhlmann; a.a.O.; Kapitel 3, Seite 5

den täglichen Umgang mit anderen einfach und angenehm machen, soll die Netiquette Reibungsflächen vermindern und das Leben aller Beteiligten vereinfachen. Man bezeichnet diese letztlich nicht eindeutig definierten Regeln daher oft auch als „Knigge des Internet“<sup>8</sup>

### 2.2.1.1. Regulierungsgegenstände

Daraus können folgende formalen Eigenschaften von Netiquette abgeleitet werden:

1. Netiquette besitzt primär Apell- und Informationscharakter. Sie setzt auf freiwillige Selbstkontrolle der Netzbenutzer, die aus Einsicht in technische und organisatorische Zusammenhänge erwächst,
2. Netiquette wird als Regulierungsinstrument in erster Linie dort eingesetzt, wo administrative Kontrolle und Sanktionen nicht praktikabel sind,
3. Netiquette stellt – im Gegensatz zu Gesetzen, Verordnungen und Verträgen – ein Instrument *indirekter Verhaltenssteuerung* dar<sup>9</sup>.

In materieller Hinsicht beschäftigen sich Netiquetten mit unterschiedlichen Regelungsgegenständen. Im Vordergrund stehen technische, organisatorische und persönliche Voraussetzungen bei der Nutzung von Internet-Diensten.

#### 2.2.1.1.1. Regulierungsgegenstand: Inanspruchnahme technischer Ressourcen

Der Regulierungsgegenstand „Inanspruchnahme technischer Ressourcen“ befasst sich insbesondere damit, das Bewusstsein der Benutzer für den Umfang der von ihnen in Anspruch genommenen Ressourcen zu schärfen. In diesem Bereich geben Netiquetten Verhaltensanweisungen für einen möglichst sparsamen Umgang mit technischen Ressourcen. Hierzu gehören in erster Linie Hinweise zur Benutzung der richtigen Werkzeuge für den jeweiligen Zweck. Doch auch stilistische Faktoren wie exzessives Zitieren oder Verwendung von überlangen Unterschriften werden abgemahnt, weil solche Verhaltensweisen direkte Auswirkungen auf die Belastungen des Netzes haben können.

#### 2.2.1.1.2. Regulierungsgegenstand: Kommunikationsstrukturen und Kommunikationskonventionen

Gerade im Bereich des Usenet sind grosse Teile der Netiquette dem Ziel gewidmet, Benutzern den angemessenen Gebrauch des News-Systems zu verdeutlichen. So werden Hinweise zu den unverzichtbaren Ordnungselementen wie die Namensgebung der Newsgruppen abgegeben, um einen möglichst präzisen Aufschluss über den thematischen Schwerpunkt und den Inhalt einer Newsgruppe sicherzustellen. Ebenso gehört dazu die Anleitung zum Verfahren über die Einrichtung neuer News-Gruppen innerhalb bestehender Hierarchien und das Verfahren zur Meinungsbildung und zur Entscheidungsfindung innerhalb eines Diskussionsforums oder für die Ausarbeitung neuer Strukturen oder Konventionen.

Zu erwähnen ist in diesem Zusammenhang auch, dass hier erstmals auch Sanktionsandrohungen für die Nichtbeachtung der ausgearbeiteten Grundregeln entwickelt wurden. Vorsätzliche Missachtung der strukturierenden Form wird – im Gegensatz zu kontroversen Inhalten – als Attacke auf konstitutive Elemente des Netzes angesehen. Solche Verstösse wurden bereits in den Anfängen des Internet mit massiven Gegenreaktionen durch die betroffenen Teilnehmer selber bekämpft. Zu erwähnen seien hier zwei exemplarische Fälle aus den Jahren 1993 und 1994. Es sind dies einerseits

#### **Der Fall Corsar Argic**

In diesem Falle wurde das Fehlverhalten eines Netzteilnehmers mit Namen Corsar Argic durch eine virtuelle Petition von über 600 Internetteilnehmer bekämpft. Der Besagte resp. sein Hostbetreiber wurden aufgefordert, den Missbrauch durch

- mailbombing,
- das Löschen oder Fälschen von Informationen,
- das robo-posting (regelmässiges automatisiertes Versenden umfangreicher Nachrichten identischen Inhalts),

---

<sup>8</sup> Netiquette für das Internet, herausgegeben durch den Wirtschaftsinformatik-Fachverband, Zürich (WIF), Ausgabe 1996, Titeltext Seite 1.

<sup>9</sup> Vgl. Fachgebiet „Informatik und Gesellschaft“ am FB Informatik der TU Berlin: Skript zur Veranstaltung „Informationssicherheit und Recht II“, Berlin, 1994, S. 6

- Versenden von Nachrichten in Newsgruppen, die keinerlei Verbindung zum Inhalt der Nachricht aufwiesen,
- die Bedrohung und Beschimpfung von Netzteilnehmern etc.

sofort einzustellen, was dieser, angesichts der Tatsache seiner Identifikation, sofort nach Publikation dieser öffentlichen Publikation vornahm.

und

### ***Der Fall Canter&Siegel***

Die Rechtsanwälte Canter & Siegel boten im Frühjahr 1994 im Zusammenhang mit „Green Card Lottery“ (Verlosung von mehreren zehntausend Aufenthaltsgenehmigungen) Benutzern des Internet ihre Unterstützung bei der Teilnahme an der Verlosung an. Dass es sich hierbei um ein kommerzielles Angebot handelte, ging aus der Nachricht nicht unmittelbar hervor. Die Rechtsanwälte versandten ihre Nachrichten in jede der über 6000 Gruppen einzeln. Sie hatten dazu extra einen Unix-Spezialisten beauftragt, ein entsprechendes Shell Script zu schreiben, welches das automatisierte Versenden dieser Anzeige vornahm. Auf Proteste hin liessen die Anwälte verlauten, dass sie keinen Anlass sähen, ihre Aktion zu beenden, da sie weder gegen ein Gesetz noch gegen den Vertrag mit dem Provider verstossen würden. Das aus allen Teilen der Welt einsetzende mailbombing führte innerhalb einer Woche zu mehrfachen Abstürzen des Providerhosts. Dieser sperrte schliesslich den account der Anwälte, welche in der Folge viermal den Provider wechseln mussten, da sie ihr Verhalten nicht beendeten und die Internet-Gemeinde jeden neuen Provider wieder mit mailbombing lahmlegte.

#### **2.2.1.1.3. Regulierungsgegenstand: Inhalt**

Die Durchsetzung inhaltlicher Freiheit war ein wichtiger Meilenstein in der Geschichte des Internet. Konsequenterweise beschränken sich Versuche zur Regelung von Inhalten über Netiquette auf ein absolutes Minimum.

Die Netiquette machen klar, daß insbesondere Verstösse gegen das Persönlichkeitsrecht nicht als Kavaliersdelikt angesehen werden. Als Tabu gilt z.B. das öffentliche Zitieren privater email in den Usenet-News ohne die vorherige Einwilligung der Verfasser. Gewarnt wird ebenfalls vor persönlichen Angriffen (Beschimpfungen und Beleidigungen). Als verpönt gelten auch Kettenbriefe wie auch unaufgeforderte Werbung nach dem Giesskannenprinzip (heute als Spamming bezeichnet) und Werbung nach dem Zielgruppenprinzip (in Newsgruppen mit bestimmten thematischen Schwerpunkten) oder unaufgeforderte emails.

In jüngster Zeit erhält jedoch auch wieder die Inhaltskontrolle gewissen Aufwind. Ein von der Bertelsmann-Stiftung unterstütztes wissenschaftliches Projekt befasst sich mit Fragen der Inhaltsregulierung im Internet. Seit Anfang 1999 hat sich ein internationales Netzwerk aus Vertretern von Regierungen, Industrie, Strafverfolgungsbehörden, Nichtregierungsorganisationen, Stiftungen und renommierten Wissenschaftlern gebildet. Aufgabe des Netzwerkes war die Entwicklung eines internationalen Lösungsansatzes zum Umgang mit problematischen Inhalten im Internet und die Ausarbeitung von Empfehlungen an Politik, Industrie und Nutzer. In einem entsprechenden Memorandum werden die Ergebnisse der gemeinsamen Untersuchungen dargestellt und als Empfehlungen an Regierungen, Internetindustrie, Regulierungs- und Strafverfolgungsbehörden, an Selbstregulierungsinitiativen, Jugendschützer und die Internet-Nutzer formuliert<sup>10</sup>.

<sup>10</sup> <http://www.stiftung.bertelsmann.de/internetcontent/deutsch/frameset.htm?content/c2310.htm>

### 2.2.2. Request for Comments

Neben der Usenet-Netiquette existierten bereits in den Anfängen der verschiedenen Internet-Dienste eine Reihe weiterer Ansätze, die Arbeit mit verteilten Ressourcen zu regulieren und die Funktionsfähigkeit des Internet sicherzustellen.

Die sogenannten *Request for Comments* sind Dokumente, die im Rahmen eines Internet-internen Normierungsprozesses diskutiert und verabschiedet werden. Obwohl diese Dokumente – etwa im Gegensatz zu Normen des CCITT<sup>11</sup> oder IEEE<sup>12</sup> – keinerlei rechtlichen Status besitzen, kommt ihnen wichtige praktische Bedeutung zu.

Relevant für den Bereich der Verhaltenssteuerung ist zum einen das von Internet Activities Board verfasste Memo *Ethics and the Internet*<sup>13</sup>. In diesem Dokument wurden beispielhaft fünf Arten unakzeptabler Nutzung explizit definiert, nämlich:

- Versuche, sich unautorisiert Zugang zu Internet-Ressourcen zu verschaffen,
- Die vorgesehene Betriebsweise des Internet zu stören,
- Ressourcen (Mannstunden, Kapazität oder Computer) durch derartige Aktionen zu verschwenden,
- Die Integrität von Daten zu zerstören und
- Die Privatsphäre von Benutzern zu verletzen.

Dieses Dokument wurde im Januar 1989 unter der Nummer 1087 in die Sammlung der RFC's aufgenommen.

### 2.2.3. Acceptable Use Policy

In neuerer Zeit finden Aspekte von Netiquette und verantwortungsvoller Nutzung des Internet Eingang in Leitfäden und Bestimmungen, die durch Betreiber von Hosts oder Subnetzen erstellt werden. Dies ist als Versuch einer mehr formalen Regulierung zu werten, da Leitfäden und Benutzerbestimmungen eine Erweiterung von Nutzungsverträgen darstellen. Sie können damit insbesondere auch in der Form von allgemeinen Geschäftsbedingungen direkt zum Vertragsbestandteil erklärt werden. Die Aufnahme von Aspekten, die sich auf die Nutzung von Ressourcen ausserhalb der eigenen Domäne beziehen, hält dem *provider* die Möglichkeit offen, ein Vertragsverhältnis bei mißbräuchlicher Nutzung des Netzes aufzulösen.

### 2.2.4. Mindeststandards von Verbänden und Organisationen

Diese Nutzungsbestimmungen (AUC Acceptable Use Policies) werden zunehmend nun auch von Interessenverbänden oder Organisationen erarbeitet und publiziert, womit sie einen zusätzlichen Verbindlichkeitscharakter erhalten. Sie werden damit einerseits zum Ausdruck von verbands- oder organisationsübergreifenden Standards, welche für eine Branche spezifische Verhaltensregeln und damit anerkannte Mindeststandards umschreiben. Andererseits erhalten sie durch die Publikation den Status der „Öffentlichkeit“, d.h. für alle interessierten Dritten sind sie zugänglich. Die Mitglieder der betreffenden Branche tun deshalb gut daran, sowohl bei der Erarbeitung solcher Standards mitzuwirken und beeinflussend auf den Inhalt einzuwirken, als auch sich an die einmal erarbeiteten und publizierten Branchenstandards zu halten resp. alles daran zu setzen, den dort publizierten Mindeststandard auch tatsächlich einzuhalten.

Solchen branchenspezifischen Mindeststandards kommt nämlich immer dann besondere Bedeutung zu, wenn sich die Sorgfaltspflichtenfrage stellt. In diesen Fällen greifen dann Lehre und insbesondere Rechtsprechung auf jene normativen Charakter enthaltenden Selbstregulierungsstandards der Branche zurück und erklären diese resp. die darin niedergelegten Prinzipien als „Stand der anerkannten Verhaltensweise“ oder als „aktuellen Stand der Technik“.

---

<sup>11</sup> International Telegraph and Telephone Consultative Committee

<sup>12</sup> The Institute of Electrical and Electronics Engineers, Inc. / [www.ieee.org](http://www.ieee.org)

<sup>13</sup> Internet Activities Board: RFC 1087 Ethics and the Internet 1989;  
<ftp://ftp.fu-berlin.de/pub/doc/rfc/rfc1087.gz>

## 2.3. Zwischenbilanz

Die Selbstregulierung ist seit den Anfängen des Internets und der breiten Nutzung der verschiedenen Internetdienste (Usenet, www, e-mail, ftp etc.) eine bekannte und bereits erprobte Tatsache. Sukzessive wurden verschiedene Formen der Selbstregulierung entwickelt und weiterentwickelt. Anfänglich standen

- **Netiquette**
- **Computer Ethics**
- **User Guides**
- **Acceptable Use Policies**
- **Penalties of Misuse of Computing Resources**

im Vordergrund.

Heute werden diese Vorarbeiten der Selbstregulierung als Ausgangsbasis für verbands- oder organisationsweite Branchen-Mindeststandards genutzt, womit den darin enthaltenen Aussagen bei entsprechender Publikation und Bekanntmachung ein zusätzlicher Grad an Verbindlichkeit zuerkannt werden muss. Insbesondere bei vertraglicher Einbindung über allgemeine Geschäftsbedingungen seitens der Provider oder Internet-Diensteanbieter kommt selbstregulierenden Bestimmungen vertragliche Verbindlichkeit zu.

Verbands- oder Branchenregulierungen werden zu Messgrößen für die Entscheidung über verschuldetes oder unverschuldetes Verhalten im Rahmen der anzuwendenden Sorgfalt bei einer Leistungserbringung. Der „anerkannte Stand der Technik“ oder die Leistungserbringung nach „bestem Wissen und Gewissen“ werden durch solche Selbstregulierungen mit qualitativem Inhalt gefüllt.

## 3. Selbstregulierung im Datenschutz

Aus diesen im Internet seit jeher bekannten Formen der Selbstregulierung bilden sich in jüngster Zeit neue und weitergehende Formen der Selbstregulierung heraus, welche neben der Eigenverantwortung auch die Qualität und die Vertrauensbildung in den Vordergrund rücken. So zeichnet sich derzeit im Bereich des Datenschutzes neben der **freiwilligen Datenbearbeitungs- oder Datenschutzerklärung** des Online-Anbieters eine alternative Form der Selbstregulierung im sogenannten **Datenschutzaudit** ab.

### 3.1. Freiwillige Datenbearbeitungserklärungen

Der globale Charakter des elektronischen Geschäftsverkehrs (e-commerce) bringt einen intensiven Austausch von Personendaten mit sich, der unter Umständen die Privatsphäre der betroffenen Personen verletzen kann. Deshalb ist es von grösster Bedeutung, dass aus der Sicht des Datenschutzes dessen Grundprinzipien auch im Umfeld des e-commerce Anwendung finden. Durch einen effektiven Schutz der Privatsphäre wird das Vertrauen der Benutzer in den e-commerce gestärkt. Ein potentieller Kunde, ob Unternehmen oder Konsument, wird Angebote des e-commerce eher nutzen, wenn Aussenstehenden der Zugriff auf vertrauliche Informationen vollkommen unmöglich ist und die eigenen Daten nicht gegen seinen Willen für andere Zwecke bearbeitet und gespeichert werden. Der konsequente Schutz der Privatsphäre im e-commerce kann bewusst als Wettbewerbsvorteil marketingmässig genutzt werden. Um das Vertrauen der Benutzer in den e-commerce zu stärken, sollen – wie dies auch vom Datenschutzgesetz vorausgesetzt wird – die Anbieter die Kundendaten transparent bearbeiten. Sie müssen die Benutzer informieren, welche Personendaten sie für welchen Zweck bearbeiten möchten.

Verhaltensregeln, niedergelegt in freiwilligen Datenschutzerklärungen des jeweiligen Online-Anbieters, können für die Vertrauensbildung durchaus nützlich sein. Aber trotzdem bilden Verhaltensregeln keine Alternative zu Gesetzen; immerhin aber sind sie eine gute und wirksame Ergänzung dazu. Es muss darauf hingearbeitet werden, dass solche Verhaltensregeln mindestens folgende Elemente enthalten:

- **Klare und verständliche Information, v.a. hinsichtlich der Art und Weise, wie Personendaten bearbeitet werden.**

- **Grundsätzliches Wahlrecht des Benutzers für die Verwendung seiner Daten.**
- **Effektive Rechtsdurchsetzungsmechanismen**
- **Schaffung einheitlicher Kriterien für die Anerkennung von Verhaltensregeln (Internationale Kriterien)**
- **Im Anerkennungsprozess von Verhaltensregeln sind sowohl Behörden als auch Wirtschaft zwingend einzubeziehen.**
- **Der Inhalt muss Informationen zur Datenbearbeitung, Lieferung, Entschädigung sowie zur Gerichtsbarkeit in Streitfällen geben.**

Datenbearbeitungserklärungen sollen die Benutzer einer Website über die vom Dienstleistungsanbieter praktizierten Verfahren zum Schutz der Privatsphäre informieren. Voraussetzung dazu ist, dass die Erklärung die erforderliche Genauigkeit aufweist. Nur so wird der Benutzer in die Lage versetzt, frei zu entscheiden, ob und wie er seine persönlichen Daten bearbeiten lassen möchte.

Der Online-Anbieter hat darauf zu achten, dass er eine transparente Datenbearbeitungspolitik betreibt, indem er solche freiwilligen Datenbearbeitungserklärungen entwickelt und diese auf seiner Website einblendet. Bevor mit der Ausarbeitung einer Datenbearbeitungserklärung begonnen wird, sind der Datenbedarf des Unternehmens zu untersuchen, die gegenwärtigen Datenschutzpraktiken zu analysieren und klare Richtlinien im Umgang mit Personendaten zu erstellen. Die Datenbearbeitungserklärung muss mit dem Datenschutzgesetz und den tatsächlich vorgenommenen Datenbearbeitungen übereinstimmen. Folgende Vorfragen sollten geklärt sein:

- Wie und woher (interne und externe Quellen) werden Personendaten beschafft ?
- Zu welchen Zwecken werden Personendaten gesammelt ?
- Zu welchen Zwecken werden Personendaten verwendet ?
- Wer ist für die Kontrolle der gesammelten Personendaten verantwortlich ?
- Wie und wo werden Personendaten gespeichert ?
- Zu welchem Zweck werden Personendaten mit Dritten ausgetauscht ?
- Existieren bereits Richtlinien oder Vorschriften für das Sammeln, das Bearbeiten und die Weitergabe dieser Daten ?
- Besteht bereits die Möglichkeit der Einsicht und der Berichtigung der Daten ?

Die Datenschutzerklärung muss den Benutzer mindestens über folgende Punkte informieren:

- **Welchen Rechtsbestimmungen untersteht die Datenbearbeitungspraxis des Online-Anbieters ?**
- **Welche Personendaten werden gesammelt und zu welchen Zwecken ?**
- **Welche Daten werden an Dritte weitergegeben und für welche Zwecke ?**
- **Welche Wahlmöglichkeiten zur Bearbeitung seiner Daten stehen dem Benutzer zu?**
- **Welche Rechte (insbesondere Auskunfts- und Berichtigungsrecht) hat der Benutzer ?**
- **Welche Stelle beantwortet Fragen über die Bearbeitung von Personendaten ?**
- **Welche Sicherheitsmassnahmen werden zum Schutz von Personendaten angewendet ?**
- **Die Datenschutzerklärung ist auf der Website so zu plazieren, dass sie für den Benutzer leicht zugänglich ist<sup>14</sup>.**

Es gibt heute bereits verschiedene Möglichkeiten, die den Online-Anbieter bei der Analyse und Erstellung von Datenschutzerklärungen unterstützen. Erwähnt sei an dieser Stelle der Generator für Datenschutzerklärungen der OECD ([www.oecd.org/scripts/PW/Pwhome.asp](http://www.oecd.org/scripts/PW/Pwhome.asp)) und die Richtlinien des Europarates über den Schutz der Privatsphäre im Internet ([www.coe.fr/dataprotection](http://www.coe.fr/dataprotection)).

## **3.2. Datenschutzaudit**

### **3.2.1. Allgemeines**

Mit dem Datenschutzaudit wird eine Objektivierung und Aussenkontrolle der vom Online-Anbieter vorgenommenen Selbstregulierungsmassnahmen und der eigenen Datenschutzerklärungen (Data Protection Policy) angestrebt. Das Prinzip der Auditierung, welches insbesondere im Rahmen der unternehmensweiten Qualitätskontrolle als Elemente des Risk-Managments bekannt ist, wird in den Bereich

<sup>14</sup> Schreiben des Eidg. Datenschutzbeauftragten an Verein e-comtrust Schweiz vom 5.12.2000

des Datenschutzes hinübergenommen. Das Prinzip beruht darauf, dass unabhängige, aussenstehende Datenschutz- und IT-Security Spezialisten das zu auditierende Online-Unternehmen von aussen unter die Lupe nehmen und die Einhaltung der Branchenstandards, Selbstregulierungsmassnahmen und der publizierten Erklärungen bezüglich Datenschutz und Datensicherheit begutachten. Das Datenschutzaudit wird damit zu einer Mischung zwischen technischer Begutachtung und inhaltlicher Ueberprüfung des Online-Unternehmens. Das Datenschutzaudit ist eine Antwort auf das gestiegene Datenschutzbewußtsein bei der Verarbeitung personenbezogener Daten bei Anwendern und Nutzern. Datenschutz ist ein entscheidender Akzeptanzfaktor für alle Formen des elektronischen Handels und der elektronischen Verwaltung.

Entsprechend seinem Vorbild, dem Umweltschutz-Audit, sollte das Datenschutzaudit vier zentrale Ziele verfolgen.

- **Stärkung der Selbstverantwortung und Stimulierung von Wettbewerb**  
Das Datenschutzaudit sollte in erster Linie ein geeignetes Instrument sein, die Selbstverantwortung des Datenverarbeiters für den Datenschutz zu fordern und zu fördern
- **Verringerung des Vollzugsdefizits**  
Nicht nur im Umweltschutzrecht, auch im Datenschutzrecht besteht ein erhebliches Vollzugsdefizit. Die öffentlichen Datenschutzbeauftragten und die Aufsichtsbehörden sind durch die weltweite Vernetzung und die ubiquitäre Verwendung von Informations- und Kommunikationstechniken überfordert. Hier könnte das Datenschutzaudit zu einer Entlastung beitragen. Mit dem von ihm geschaffenen Anreiz zur Selbstkontrolle verringert das Datenschutzaudit Defizite in der Einhaltung des geltenden Datenschutzrechts.
- **Kontinuierliche Verbesserung des Datenschutzes und der Datensicherung**  
Beim Umweltschutz-Audit haben die teilnehmenden Unternehmen nicht nur die einschlägigen Vorschriften einzuhalten, sondern auch auf eine angemessene kontinuierliche Verbesserung des betrieblichen Umweltschutzes hinzuwirken, wie sie sich mit der wirtschaftlich vertretbaren Anwendung der besten verfügbaren Technik erreichen läßt. Ebenso sollte das materielle Hauptziel des Datenschutzaudits die kontinuierliche Verbesserung des Datenschutzes und der Datensicherung sein.
- **Datenschutzaudit als Lernsystem**  
Das Ziel einer kontinuierlichen Verbesserung kann das Datenschutzaudit nur erreichen, wenn es als ein Lernsystem verstanden wird. Wie beim Umweltschutz-Audit sollte auch im Datenschutz der Regelungsschwerpunkt auf der Normierung des "Lernprozesses" des Datenschutzmanagementsystems liegen. Dieser Lernprozeß wird dadurch strukturiert, daß der Datenverarbeiter in einer umfassenden Betriebsprüfung eine Bestandsaufnahme der Verarbeitung personenbezogener Daten erstellt und die hierfür relevanten Anforderungen des Datenschutzrechts zusammenträgt.

### 3.2.2. Gegenstand des Datenschutzaudits

Gegenstand eines Datenschutzaudits können sein:

1. einzelne automatisierte oder nicht automatisierte Verfahren, in denen personenbezogene Daten verarbeitet werden,
2. ein abgrenzbarer Teilbereich der datenverarbeitenden Stelle, innerhalb dessen mehrere Verfahren nach Nr. 1 eingesetzt werden,
3. die gesamte Verarbeitung personenbezogener Daten einer datenverarbeitenden Stelle. Soweit sich die nachfolgenden Ausführungen auf einzelne Verfahren beziehen, gelten sie in diesem Fall sinngemäß für die gesamte Stelle oder abgrenzbare Teilbereiche derselben.
4. Gegenstand des Datenschutzaudits können auch Verfahren sein, die sich erst in der Planung oder Entwicklung befinden.

Insbesondere die rechtlichen Auditaspekte betreffen in einer ersten Stufe die einzuhaltenden gesetzlichen Grundlagen (nationales Datenschutzgesetz; internationale Vorgaben wie EU-Richtlinien) und in einer zweiten Stufe die Prüfung der Prozessbeherrschung im Datenschutz- und Datensicherheitsbereich sowie die Ueberprüfung des Online-Unternehmens bezüglich Umsetzung und Einhaltung seiner eigenen Datenschutzerklärungen (Policies) und bezüglich der in der Branche entwickelten Grundsätze (Guidelines) und Mindeststandards von internationalen Verbänden wie OECD, Vereinigung der Datenschutzbeauftragten Europas; Konsumentenorganisationen, europäische oder weltweite Standardisierungs- und

Normierungsgremien wie CEN oder ISO). Zu diesen Grundlagen werden im Kapitel 4 noch weitere Details angeführt.

Ziel des Datenschutzaudits ist somit eine externe Bescheinigung über die Datenschutzkonformität des geprüften Online-Anbieters. Damit wird das Datenschutzaudit sowohl zu einem unterstützenden strategischen Element im Rahmen der Erfüllung von prozessorientierten Management-Systemen, welche u.a. auch die Einhaltung aller gesetzlichen Normen (so auch bezüglich Datenschutz) verlangen (z.B. ISO 9001:2000). Die Geschäftsleitung erhält dadurch Gewissheit, dass sie resp. ihr Unternehmen die Prozesse im kritischen Bereich der Datenhaltung und Datenbe- und Datenverarbeitung beherrscht. Auf der anderen Seite kann das Datenschutzaudit auch als Marketingmassnahme angesehen werden, welche insbesondere in den Beziehungen zum Kunden das Vertrauensniveau erheblich verbessern resp. auf hohem Niveau aufrecht erhalten kann.

Die Einsicht in die Notwendigkeit der Selbstregulierung im Datenschutz durch Bekanntgabe der eigenen Verhaltensgrundsätze, die Überprüfung der Einhaltung der selbsterklärten Grundsätze durch externe Auditoren und die Erhöhung des Vertrauens in das datenschutzrelevante Handeln des Online-Anbieters ist bereits soweit gediehen, dass man weltweit seit einiger Zeit intensiv über Datenschutzaudit und Gütesiegel für IT-Produkte diskutiert.

### **3.2.3. Datenschutz Audit-Modell Schleswig-Holstein**

Das Bundesland Schleswig-Holstein hat hier für die Datenschutzauditierung im öffentlichen Bereich Pionierarbeit geleistet und im Frühjahr 2001 sowohl auf Gesetzes- wie auf Verordnungsstufe die notwendigen Voraussetzungen geschaffen. Dahinter steckt die Idee, Datenschutz und Datensicherheit von vornherein in IT-Produkten und bei öffentlichen Stellen zu implementieren. Audit und Gütesiegel sollen den Verbrauchern, Nutzern und Kunden signalisieren, dass das Produkt, die Dienstleistung oder die Behörde vorab in einem geregelten Verfahren geprüft worden sind. Es wird erwartet, dass die Kunden im Zweifel solche Produkte bevorzugen, die mit einem Datenschutz-Gütesiegel ausgezeichnet sind.

Mit dem Datenschutzaudit können Behörden den Bürgerinnen und Bürgern demonstrieren, dass sie das Thema Datenschutz gut "im Griff" haben. Das schleswig-holsteinische [Landesdatenschutzgesetz 2000](#) enthält zu Audit und Gütesiegel bereits die notwendigen gesetzlichen Regelungen. Basis dazu bildet § 4 des neuen Datenschutzgesetzes, welcher unten wiedergegeben ist.

Die Landesregierung von Schleswig-Holstein hat auch bereits die ergänzende Rechtsverordnung zum Gütesiegel verabschiedet. Der Text, die Verordnung und weitere Informationen zum Gütesiegel können abgerufen werden unter <http://www.datenschutzzentrum.de/guetesiegel/>.

In der entsprechenden Verordnung der Landesregierung ist vorgesehen, dass die Zertifizierung von Gutachtern erbracht wird, die beim Unabhängige Landeszentrum für Datenschutz akkreditiert sind. Das eigentliche Gütesiegel verleiht das Unabhängige Landeszentrum für Datenschutz. Es bescheinigt damit dem jeweiligen Produkt die Vereinbarkeit mit dem Landesdatenschutzgesetz und empfiehlt seinen Einsatz bei den öffentlichen Stellen des Landes.

Gleichzeitig hat das Unabhängige Landeszentrum für Datenschutz die Ausführungsbestimmungen zum Datenschutzaudit erlassen. Sie regeln die Einzelheiten des Auditverfahrens, insbesondere die Antragsvoraussetzungen, die notwendige Bestandsaufnahme, die Festlegung der Datenschutzziele, die Einrichtung eines Datenschutzmanagementsystems sowie die Begutachtung durch das Unabhängige Landeszentrum für Datenschutz. Informationen zum Datenschutzaudit und den Text der Ausführungsbestimmungen finden Sie unter <http://www.datenschutzzentrum.de/audit/>.

Mit dem Datenschutzaudit können Behörden oder Behördenteile ihr Datenschutzkonzept vom Unabhängigen Landeszentrum für Datenschutz überprüfen und sich anschließend dessen Ordnungsmäßigkeit förmlich bescheinigen lassen. Beide Regelungen traten mit der Verkündung im Gesetzesblatt bzw. im Amtsblatt des Landes Schleswig-Holstein in der Woche vom 26.-30.03.2001 in Kraft.

Diese Datenschutz-Auditregelungen sind erste konkrete Umsetzungen einer vom Bundesministerium für Wirtschaft und Technologie eingeleitete Phase der standardisierten und gesetzgeberisch abgestützten Durchsetzung von datenschutz- und datensicherheitsrelevanten Regulierungsmassnahmen. Prof. Dr.

Alexander Roßnagel von der Universität Kassel hatte in Mai 1999 ein entsprechendes Rechtsgutachten über ein **Konzept und Entwurf eines Gesetzes für ein Datenschutzaudit**<sup>15</sup> abgeliefert.

## 4. Standardisierung über CEN und ISO

Die Selbstregulierung im Internet ist in den vergangenen Monaten eine Dimension höher gerückt, indem sich die europäische und die internationale Standardisierungs- und Normierungsorganisationen dem Thema der Co-Regulation im Internet-Bereich angenommen haben.

### 4.1. CEN / ISSS

CEN, das europäische Komitee für Normung<sup>16</sup> hat für den Bereich Internet-Standardisierung ein spezielles Arbeitssystem bereitgestellt, die CEN/ISSS (CEN / i-triple S) das **Information Society Standardization System**<sup>17</sup>. Aufgabe von CEN/ISSS ist die Bereitstellung von Standards, Richtlinien und allgemein anerkannten Grundsätzen im Bereich der Informationstechnologie, insbesondere natürlich mit Blick auf das Internet. Neben den Hauptaktivitäten wie die Erarbeitung von Grundlagen, Standards und Normen im Bereich e-Business sind auch noch spezielle Projekte lanciert, so unter anderem Technische Komitee (sogenannte TC) oder Workshop Agreements (CWA). Während in den TC Grundlagen für die Verabschiedung von europäischen Normen (EN-Norm) in einem standardisierten, länderübergreifenden Vernehmlassungsverfahren erarbeitet werden, schaffen CWA's Diskussionspapiere und Guidelines von unverbindlichem Charakter. Sie gelten aber trotz Nichterreichung eines EN-Normenstatus noch immer als Ausdruck von „best practice“ oder europäisch anerkannter Co-Regulation, da auch CWA-Statements in internationalen Gremien ausgearbeitet werden.

Die Schweiz ist in CEN ebenfalls eingebunden, indem die **Schweizerische Normenvereinigung SNV** in Winterthur Mitglied von CEN ist und an deren gesamtem Programm teilnimmt. Die SNV fördert ebenfalls die Erarbeitung und die Harmonisierung von Normen und Standards. Die SNV kann ihrerseits selber entsprechende Initiativen für die Erarbeitung von EN-Normen oder CWA's starten. Dies hat sie im Bereich e-Business denn auch konkret gemacht, indem sie am 29.3.2001 die Gründung eines INB/TK 191 „Online-Dienstleistungen“ bekanntgegeben hat<sup>18</sup>. Die Initianten des Normungsprojektes des INB/TK 191 (interdisziplinärer Normenbereich / Technisches Komitee) „Online-Dienstleistungen“ sind überzeugt, dass Normen den Internethandel sicher und zuverlässig machen. Diese Normen werden durch die Schweizerische Normen-Vereinigung SNV in der Expertengruppe INB/TK191 erarbeitet. Dieses Technische Komitee hat am 29.3.2001 am Sitz der SNV in Winterthur mit über 20 Gründungsmitgliedern die Arbeit aufgenommen. Weitere Interessenten sind jederzeit zur Mitarbeit und Mitgliedschaft eingeladen.

Die Gründungsversammlung wählte zum Vorsitzenden des INB/TK191 Robert P. Hilty, b.a.s. AG, Digitalmarketing Service, 5001 Aarau.

#### **Absicht und Aufgaben des INB/TK191**

In einer ersten Phase soll ein Satz von „CH-Standards“ erstellt werden. Diese sollen beim Europäischen Komitee für Normung, CEN, als Basis für die Erstellung von Europäischen Standards eingebracht werden und durch die Mitarbeit von europäischen Experten – voraussichtlich in Form von CEN/Workshop Agreements CWA – im Rahmen von CEN/ISSS weiterentwickelt werden. Ein erster Antrag an CEN ist gestellt. Zudem sind auch die Arbeiten der ISO im Rahmen des „Committee on Consumer Policy (COPOLCO)“ zu berücksichtigen<sup>19</sup>.

#### **Prüffelder und Qualitätsmerkmale für Online-Anbieter**

Anlässlich der Gründungsversammlung am 29.3.2001 wurden zwei Arbeitsgruppen bestimmt. Die

<sup>15</sup> <http://www.iid.de/iukdg/gus/DASA.html>

<sup>16</sup> <http://www.cenorm.be/>

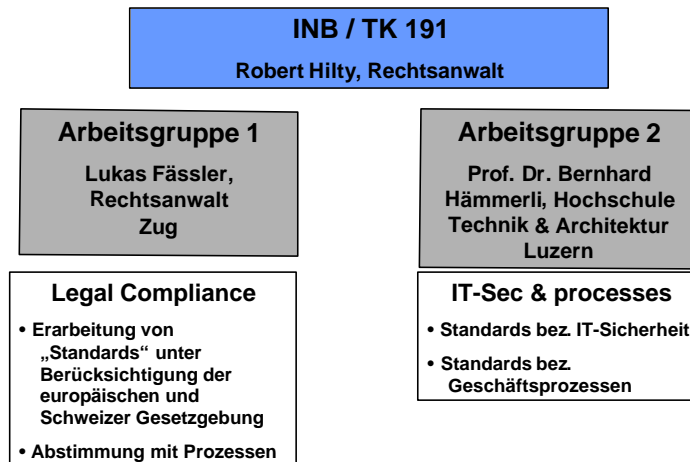
<sup>17</sup> <http://www.cenorm.be/iss/>

<sup>18</sup> SNV-Bulletin 2001/05, Seite 45

<sup>19</sup> <http://www.iso.ch/infoe/comm/COPOLCO.html>

## SNV - INB/TK 191

### Standardisierung von Online-Dienstleistungen



Die **Arbeitsgruppe 1** unter der Leitung von Rechtsanwalt Lukas Fässler, Zug, hat folgende Aufgaben:

- Erarbeitung von „Standards“ unter Berücksichtigung der europäischen und Schweizer Gesetzgebung,
- Die Anforderungen sollen höher als die gesetzlichen Mindestanforderungen sein.
- Es wird kein abschliessendes Normenwerk erwartet.

Der Arbeitsgruppe 1 vorgelagert arbeitet ein Expertenteam von bekannten und erfahrenen Internet-Anwälten der Schweiz an den ersten, von der AG1 zu detaillierenden Grundlagen. Dieser Expertengruppe (legal expert group) gehören an:

- Rechtsanwalt Dr. Rolf Auf der Maur, Zürich
- Rechtsanwalt Dr. Oliver Sidler, Zug
- Rechtsanwalt Dr. Ralph Wyss, Zürich – St. Gallen
- Rechtsanwalt Patrick Dehmer, Zürich
- Rechtsanwalt Dirk Trüten, Europainstitut Universität Zürich
- Jurist und Publizist David Rosenthal, Zürich – Basel

Prof. Rolf H. Weber von der Universität Zürich hat sich bereit erklärt, die Arbeiten der legal expert group zu begleiten und Feedback zu den Arbeitsergebnissen abzugeben.

Die **Arbeitsgruppe 2** hat folgende Aufgaben:

- Zielsetzungen bezüglich IT-Sicherheit definieren.
- Zielsetzungen bezüglich Geschäftsprozesse definieren.
- Nach der ersten Sitzung soll entschieden werden, ob eine separate Arbeitsgruppe „Geschäftsprozesse“ gebildet werden soll.

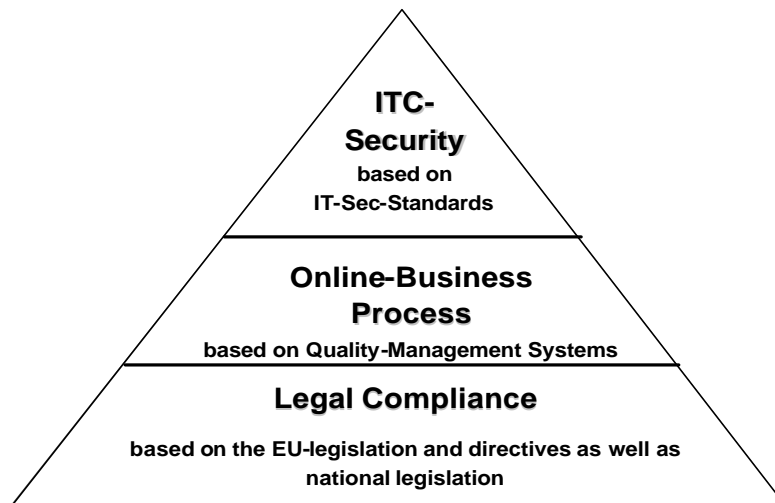


Abbildung 3.1: 3-Ebenen Modell der Standardisierungsarbeiten von SNV

Die ersten Ergebnisse eines Entwurfs mit Qualitätsmerkmalen ist am 29.6.2001 in der 2. Plenarsitzung präsentiert worden. Bis Ende August 2001 sind die Zwischenergebnisse konsolidiert und gegenüber international anerkannten Grundlagenarbeiten (wie OECD Guidelines; ICC-Grundlagen; Ergebnisse von nationalen Standardisierungsorganisationen wie Kanada, Australien, Japan etc.) qualitätsgeprüft worden. Am 31.12.2001 hat die Schweizerische Normenvereinigung SNV eine SN-Regel 1:2002 mit dem Titel „Elektronischer Handel – Mindestanforderungen an Marktauftritt und Markttransaktionen“, publiziert. Die Standards können bei der SNV ([www.snv.ch](http://www.snv.ch)) bestellt werden. Bereits ist beantragt, diese Standards zu einer Schweizerischen Norm zu erklären und unter der Bezeichnung SN 191001 zu publizieren, was noch im ersten Halbjahr 2002 Wirklichkeit werden dürfte.



Abbildung 3.2: SN-Regel 1:2002 – Elektronischer Handel: Mindestanforderungen für Marktauftritt und Markttransaktionen

## **CEN Workshop Agreement (CWA)**

Das Verfahren<sup>20</sup> für die Erarbeitung von CEN Workshop Agreements ist von CEN festgelegt:

1. Eine interessierte Partei hat zu Beginn der Arbeiten einen Antrag an das CEN Management Centre (CMC) einzureichen.
2. Das CMC evaluiert zusammen mit dem Antragsteller, ob der Antrag die Anforderungen für ein CEN Workshop Agreement überhaupt erfüllt.
3. Der Antragsteller erarbeitet im Bejahungsfalle unter Mithilfe des CMC einen Entwurf zu einem Businessplan (basierend auf einem vorgegebenen Workshop Businessplan Formular) sowie notwendige Begleitdokumentationen für den CEN Workshop.
4. Das CMC informiert unverzüglich die nationalen CEN-Mitglieder über den Antrag für einen CEN Workshop. Der Antrag wird auf der Website von CEN als neuer Workshop publiziert und enthält:
  - a) den Businessplan
  - b) ein Anmeldeformular, welches den potentiellen Interessenten eine Anmeldung zur Mitwirkung erlaubtSollte ein nationales CEN-Mitglied in diesem Verfahrensstadium einen Einwand gegen den Antrag erheben, wird das CMC die Situation durch „Management by Exception“ klären.
5. Mitwirkungswillige Parteien reichen ihren Registerierungsantrag an CMC ein. Die nationalen Mitglieder können sich für die Position des CEN Workshop Sekretariates bewerben.
6. Das CMC organisiert das erste „Kick-Off Meeting“ und sendet den mitwirkungswilligen Parteien mit der Einladung eine Traktandenliste sowie den vorgeschlagenen Businessplan zu.
7. Das CMC und die Antragssteller identifizieren allfällige offene Fragen und Problemfelder und versucht diese vor dem Kick-Off Meeting zu lösen.
8. Das Kick-Off Meeting entscheidet gemeinsam und übereinstimmend über den Businessplan und bezeichnet den CWA-Vorsitzenden sowie das Sekretariat.
9. Wenn das Kick-Off Meeting Einigkeit unter den Mitwirkenden bezüglich Businessplan erzielt, ist das CEN Workshop Agreement offiziell gegründet. Wenn keine Einigkeit erzielt werden kann, geht es zurück zu Ziffer 7 oben.
10. Die CEN WS-Teilnehmer erarbeiten einen Erstentwurf bezüglich der im Businessplan genannten Zielsetzungen und Anforderungen. Anschliessend wird der Entwurf den nationalen CEN-Mitgliedern und allen CEN WS-Teilnehmern zur Stellungnahme unterbreitet. Ebenso wird der Erstentwurf auf der Website von CEN allgemein zugänglich gemacht.
11. Alle eingehenden Stellungnahmen zum Entwurf werden vom WS Sekretariat in einem Bericht zusammengefasst.
12. Der WS-Vorsitzende entscheidet auf der Grundlage der eingegangenen Stellungnahmen und allfälligen weiteren Konsultationen unter den registrierten WS-Teilnehmern, ob unter den offiziell registrierten WS-Teilnehmern ein Konsens zum definitiven Text erreicht werden konnte.
13. Das CWA wird offiziell beendet. Das Sekretariat des CWA übersendet den angenommenen CWA-Text an CMC, welches das CEN-Vorwort zum Agreement-Text verfasst und eine entsprechende Kennzeichnungsnummer (CWA xxxxx) vergibt, bevor der CWA-Text an alle nationalen CEN-Mitglieder zur Publikation zugestellt wird. Die nationalen CEN-Mitglieder zeigen daraufhin dem CMC an, wann und wie sie das CEN Workshop Agreement in ihrem Land verbindlich erklären werden.

---

<sup>20</sup> vgl. Abbildung 3 hinten

Die oben abgebildete SN-Regel als Arbeitsergebnis der Standardisierungstätigkeiten in der Schweiz ist am 27. und 28.11.2001 in Brüssel bei CEN präsentiert worden. Gleichentags ist auf Antrag der Schweizerischen Normenvereinigung der Projektplan (Business-Plan) für die Initialisierung eines CEN Workshop Agreements unter dem Namen „e-Trust“ (Workshop on Regulatory and Self-Regulatory Compliance and Trust for e-business) eröffnet worden. Es wurden 3 Arbeitsgruppen gebildet, welche nun die schweizerischen Vorarbeiten überprüfen, ergänzen und anschliessend entsprechend dem obgenannten Verfahren validieren und europaweit für die CEN-Mitglieder bereitstellen werden. Der Businessplan des CWA „e-Trust“, die Protokoll der Sitzungen vom 27./28.11.2001 sowie die Ziele der einzelnen Arbeitsgruppen sind auf dem Internet publiziert<sup>21</sup>.

## 4.2. ISO COPOLCO

ISO ist die Internationale Organisation für Standardisierung. Die Organisation setzt sich zusammen aus den nationalen Standardisierungsorganisationen von grossen und kleinen, industrialisierten und in Entwicklung begriffenen Staaten. ISO entwickelt freiwillige technische Standards, welche in allen Bereiche des Geschäftslebens einen beachtlichen Mehrwert schaffen. ISO entwickelt nur jene Standards, welche vom Markt explizit verlangt werden. Die Standards werden von Experten aus allen Ländern und den fraglichen Bereichen erarbeitet, indem sie ihre Gesichtspunkte zu einzelnen Regelungsbereichen einbringen und gemeinsam mit allen Teilnehmern, welche an der Entwicklung solcher Standards mitwirken wollen, einen Konsens bezüglich Mindestanforderungen aushandeln. Unter der Bezeichnung ISO veröffentlicht beinhalten die erarbeiteten Standards das aktuelle Wissen und die notwendigen Anforderungen in einem speziellen technischen Bereich. Sie geben damit den „Stand der Technik“ wieder und werden durch periodische Überprüfung an allenfalls veränderte Rahmenbedingungen angepasst.

COPOLCO ist das ISO-Komitee für Konsumenten Aspekte und rapportiert direkt an den ISO-Rat. Das Komitee wurde 1978 eingerichtet und steht allen ISO-Mitgliedern als entweder direkt Mitwirkende oder nur Beobachtende offen. COPOLCO hat derzeit rund 75 Mitglieder. Zwei bekannte internationale Organisationen haben direkte Verbindungen mit dem Komitee, einerseits die Consumer International (CI), andererseits die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD). COPOLCO setzt sich insbesondere in verschiedenen Arbeitsgruppen für die internationale Standardisierung der Konsumentenschutzaspekte in einer globalisierten Welt ein<sup>22</sup>.

Auf Antrag des ISO-Mitgliedes Kanada wurde im vergangenen Jahr eine Arbeitsgruppe für die Standardisierung von Konsumentenschutzaspekten im E-Commerce lanciert. Kanada ist in diesem Fragenkomplex schon sehr weit und hat selber in verschiedenen gemischten **Arbeitsgruppen Standards und Richtlinien u.a. auch für Datenschutzaspekte** entwickelt. Die Arbeiten laufen zur Zeit auf Hochtouren und werden durch direkte persönliche Kontaktnahmen zwischen SNV (für das CWA „Online-Dienstleistungen INB / TK 191) und COPOLCO abgestimmt.

## 4.3. DIN Certco

Dasselbe findet auch zwischen SNV und DIN (Deutsches Institut für Normung)<sup>23</sup> statt. Im Bereich der Zertifizierung ist DIN CERTCO die Zertifizierungsorganisation des DIN und genießt aufgrund ihrer Unabhängigkeit, Neutralität, Kompetenz und langjährigen Erfahrung im In- und Ausland hohes Ansehen.

DIN Certco stellte am 27. November 2000 ein neues Konzept zur Vertrauensbildung im E-Commerce durch Prüfung und Zertifizierung vor. "DIN Tested Website" ist ein modular aufgebautes Programm zur Prüfung von E-Commerce-Anwendungen, in dem die einschlägigen Forderungen aus drei international anerkannten Standards integriert sind. Die Prüfung der Software erfolgt auf der Grundlage von DIN ISO/IEC 12119. Für die nachweislich gleichbleibende Qualität und Zuverlässigkeit der Management- und IT-Prozesse sind Forderungen an ein Qualitäts- und IT-Sicherheits-Management-System zu erfüllen. Der Nachweis kann wahlweise durch Prozessaudits oder durch ein vollständig zertifiziertes Managementsystem erbracht werden, zum Beispiel nach ISO 9001 oder BS 7799. Nach erfolgreichem Abschluss erhält das Unternehmen ein Zertifikat sowie das Recht, seinen Webauftritt entsprechend zu kennzeichnen<sup>24</sup>.

<sup>21</sup> <http://www.cenorm.be/isss/Workshop/e-Trust/default.htm>

<sup>22</sup> <http://www.iso.ch/iso/en/prods-services/otherpubs/Consumerquestions.html>

<sup>23</sup> <http://www.din.de/>

<sup>24</sup> <http://www.dincertco.de/>

#### 4.4. Der weltweite Aktionsplan

Die Alliance for Global Business hat im Oktober 1999 Ihren zweiten "Global Action Plan for Electronic Commerce" veröffentlicht. Die Alliance ist ein Koordinationsgremium der führenden internationalen Unternehmensorganisationen, das sich zum Ziel gesetzt hat, in der Informationsgesellschaft und in Electronic Commerce die Privatinitiative und die Selbstregulierungsmechanismen sicherzustellen. Der Alliance gehören die folgenden fünf Gründungsmitglieder an:

- BIAC - Business and Industry Advisory Committee to the OECD<sup>25</sup>
- GIIC - Forum for the Global Information Infrastructure<sup>26</sup>
- ICC - International Chamber of Commerce<sup>27</sup>
- INTUG - International Telecommunication Users Group<sup>28</sup>
- WITSA - World Information Technology and Services Alliance<sup>29</sup>

Mit Ihrem globalen Aktionsplan statuiert die Alliance zehn fundamentale Prinzipien für den elektronischen Handel sowie eine Anzahl von Handlungsmaximen für einen sicheren und vertrauensvollen Internethandel. Dabei proklamiert sie insbesondere die Steigerung des Handelsvertrauens durch Massnahmen der Selbstregulierung zwischen Anbieter und Konsument. Der Konsumentenschutz, mit besonderer Berücksichtigung des Daten-, des Vertrauens- und des Inhaltsschutzes sollen dabei dank der Umsetzung verschiedener Massnahmen verstärkt werden. Dies geschieht mit dem Ziel, die staatlichen Interventionen auf gesetzlicher Ebene möglichst gering zu halten und nur dort einzusetzen, wo Eigenverantwortung und gegenseitige Selbstregulierung keinen ausgewogenen Schutz mehr für die beteiligten Vertragsparteien garantieren. Um weltweite Geltung zu erlangen, sollen sich die Massnahmen auf die OECD-Richtlinien sowie die umfangreichen Grundlagenarbeiten der ICC abstützen.

## 5. Internationale Vertrauensinitiative e-comtrust

### 5.1. Die Vertrauensinitiative

**Die Federation of European Direct Marketing FEDMA**, getragen von ihren 13 nationalen Organisationen und 600 Mitgliedern, die weltweit über 10'000 Firmen vertreten, hat neben einem **Code of Conduct** auch einen **Selbstregulierungsmechanismus** für den E-Commerce initiiert. Diese werden nun in Zusammenarbeit mit der Schweizerischen Normen-Vereinigung im Rahmen von CEN umgesetzt.

Der Aktionsplan der FEDMA hat folgende zwei Zielsetzungen:

- Das Vertrauen der Konsumenten in E-Commerce zu steigern.
- Das Wachstum des E-Commerce in Europa durch praktische Erfahrungen sicherzustellen.

Deshalb will die FEDMA über die sieben Kernelemente ihrer Vertrauensoffensive die Anbieter- und Konsumentenseite zu einem sicheren und vertrauensvollen E-Commerce zusammenführen. Sie will dies über folgende Aktivitäten erreichen:

- Europäische Standardisierung
- Ein europäisches Gütesiegel (e-comtrust)
- Verstärkungsmechanismen, Verhaltenskodex
- Begleitung und Überwachung
- Anbieten spezieller Software-Werkzeuge
- Aufklärungskampagnen
- Nutzensteigerungsleistungen

Anlässlich der GBDe-Konferenz (Global Business Dialogue e-Commerce im Rahmen des G8) am 25./26.9.2000 in Miami, haben sich die Teilnehmer klar für die Einführung von sogenannten ADR (Alternative Dispute Regulations) und die Vertrauensinitiative der FEDMA ausgesprochen. e-comtrust wurde im Bereich der Trust Marks als eine der idealen Lösungen angesehen, weil in der

---

<sup>25</sup> <http://www.biac.org>

<sup>26</sup> <http://www.giic.org>

<sup>27</sup> <http://www.iccwbo.org>

<sup>28</sup> <http://www.intug.net>

<sup>29</sup> <http://www.witsa.org>

Organisationsstruktur von e-comtrust die National und die International Association Hand in Hand zusammenarbeiten, um die besten Geschäftspraktiken für Online-Händler zu definieren und so den höchstmöglichen Schutz für Konsumenten zu generieren.

Die GBDe-Mitglieder, die sich aus den Regierungsvertretern der wichtigsten Industrieländer und rund 60 CEO's der wichtigsten Technologiekonzerne wie Time Warner, HP, Siemens, DASA, Toshiba, AOL, Walt Disney zusammensetzen, haben beschlossen, dass sowohl ADR als auch Trust Marks in die GBDe-Richtlinien aufgenommen werden sollen. Laut Carly Fiorina (CEO HP) würden die GBDe-Mitglieder "alles unternehmen, um diese Prinzipien in ihre zukünftige Geschäftspolitik aufzunehmen und dies würde zur Benchmark für die weltweiten Internetaktivitäten werden".

## 5.2. Das Pilotprojekt Schweiz

Die erste ecomtrust National Association (NA) ist am 1.11.2000 in der Schweiz in der Rechtsform eines Vereins konstituiert worden. Gründungsmitglieder sind je ein Vertreter folgender namhafter Verbände und Organisationen:

- Swiss ICT,
- Schweizerische Normen-Vereinigung SNV (CEN-Mitglied),
- economiesuisse (UNICE-Mitglied),
- Konsumentenforum kf.

Die Aufgabe dieser NA ist die Initialisierung, Unterstützung und Verbreitung aller Arbeiten, welche zur Vertrauensbildung im e-commerce beitragen.



Es ist geplant, Leitfäden für Konsumenten und Online-Anbieter herauszugeben, Anleitungen für Eltern bezüglich Umgang und Selbstkontrolle des Internet-Verhaltens der Kinder, Unterstützung der Aktivitäten des INB/TK191 national und international durch Sicherstellung des Informationsflusses in internationale Gremien (wie UNICE, BEUC, OECD etc.) und Ombudsstellen für Konsumenten (durch Konsumentenorganisationen) bereitzustellen.

## Zusammenfassung

Das Institut der Selbstregulierung ist seit den „Urzeiten“ des Internet ein systemimmanentes Grundprinzip geblieben und gegen verschiedene Versuche der Aufhebung erfolgreich verteidigt worden. Mit der Zeit sind die Elemente dieses Grundprinzips erweitert, ergänzt und verfeinert worden und haben zunehmend auch im Bereich des Datenschutzes Einzug gehalten. Heute erkennen wir im Bereich des Datenschutzes insbesondere die freiwillige Datenschutzerklärung (Privacy Policy) sowie das Datenschutzaudit als Elemente dieser Selbstregulierungselemente. Das Datenschutzaudit wird damit zum Mittel der Überprüfung und Verbindlichkeit der freiwilligen Datenschutzerklärung und verstärkt damit deren Wirkung nach aussen insbesondere auch gegenüber den betroffenen Eigentümer der Daten (Datenherren). Insbesondere der Konsument im Internet erhält dadurch ein zusätzliches Vertrauenskriterium, wenn beispielsweise ein Online-Shop neben seiner freiwilligen Datenschutzerklärung sich durch unabhängige Dritte nach einem transparenten und im voraus klar festgelegten Auditverfahren prüfen und begutachten lässt. In diesem Bereich haben vor allem die Standardisierungs- und Normungsorganisationen (CEN; ISO) grosse Erfahrung und stellen auch entsprechende Entwicklungsmethoden und Verfahren (CEN Workshop Agreement) für die Ausarbeitung von Standards oder Mindestqualitätsanforderungen bereit. Die Entwicklung hat auch hier auf breiter Front begonnen. Die Schweiz ist über die Vertrauensinitiative e-comtrust und die Standardisierungsarbeiten der Schweizerischen Normenvereinigung SNV an vorderster Front mit dabei.

Die Grundsätze der Selbstregulierung sind derart stark verankert und akzeptiert, dass selbst der Gesetzgeber an diesem Institut nicht mehr vorbeikommt. Der Europäische Gesetzgeber fordert selber in verschiedenen Richtlinien, dass die Privatwirtschaft, Organisationen oder Verbände dafür besorgt sein sollen, über die Selbstregulierung die notwendigen Mindestspielregeln im Zusammenwirken der Marktbeteiligten zu regeln. So wird in **Artikel 27 der Richtlinie 95/46/EG** des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (**Datenschutz-Richtlinie**) folgendes festgehalten:

*Die Mitgliedstaaten und die Kommission fördern die Ausarbeitung von Verhaltensregeln, die nach Maßgabe der Besonderheiten der einzelnen Bereiche zur ordnungsgemäßen Durchführung der einzelstaatlichen Vorschriften beitragen sollen, die die Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassen.*

In der **Richtlinie** des Europäischen Parlaments und des Rates **über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs** im Binnenmarkt (**E-Commerce Richtlinie**) führt der europäische Gesetzgeber zudem dazu aus:

### *Artikel 16 Verhaltenskodizes*

- (1) *Die Mitgliedstaaten und die Kommission ermutigen*
  - a) *die Handels-, Berufs- und Verbraucherverbände und -organisationen, auf Gemeinschaftsebene Verhaltenskodizes aufzustellen, die zur sachgemäßen Anwendung der Artikel 5 bis 15 beitragen;*
  - b) *zur freiwilligen Übermittlung der Entwürfe für Verhaltenskodizes auf der Ebene der Mitgliedstaaten oder der Gemeinschaft an die Kommission;*
  - c) *zur elektronischen Abrufbarkeit der Verhaltenskodizes in den Sprachen der Gemeinschaft;*
  - d) *die Handels-, Berufs- und Verbraucherverbände und -organisationen, die Mitgliedstaaten und die Kommission darüber zu unterrichten, zu welchen Ergebnissen sie bei der Bewertung der Anwendung ihrer Verhaltenskodizes und von deren Auswirkungen auf die Praktiken und Gepflogenheiten des elektronischen Geschäftsverkehrs gelangen;*
  - e) *zur Aufstellung von Verhaltenskodizes zum Zwecke des Jugendschutzes und des Schutzes der Menschenwürde.*
- (2) *Die Mitgliedstaaten und die Kommission ermutigen dazu, die Verbraucherverbände und Verbraucherorganisationen bei der Ausarbeitung und Anwendung von ihre Interessen berührenden Verhaltenskodizes im Sinne von Absatz 1 Buchstabe a zu beteiligen. Gegebenenfalls sind Vereinigungen zur*

*Vertretung von Sehbehinderten und allgemein von Behinderten zu hören, um deren besonderen Bedürfnissen Rechnung zu tragen.*

Damit ist das Prinzip der Selbstregulierung in der europäischen Union definitiv salonfähig geworden und nimmt – insbesondere auch im Bereich Datenschutz – eine bedeutende Position ein. Das „archaische“ Prinzip aus den Anfängen des Internets hat sich in die New Economy hinein weiterentwickelt und ist nicht mehr wegzudenken.

Zug, 14.6.2001

© Lic.iur. Lukas Fässler, Rechtsanwalt, Artherstrasse 23a, CH-6300 Zug

### **Anhang**

Abbildung 1: „Sichtweisen auf das Internet“; Strukturmodell

Abbildung 2: „Sichtweisen auf das Internet“; Domänen

Abbildung 3: „Prozess eines CEN Workshop Agreement CWA