Rechtliche und technische Aspekte von E-Commerce

Michael Sonntag

Johannes Kepler Universität Linz
Institut für Informationsverarbeitung und Mikroprozessortechnik
Wintersemester 2002/2003

Kontaktinformationen:

Mag. Dipl.-Ing. Dr. Michael Sonntag

E-Mail:
sonntag@fim.uni-linz.ac.at

Adresse:
Johannes Kepler Universität Linz
Institut für Informationsverarbeitung und Mikroprozessortechnik (FIM)
Altenbergerstr. 69
A - 4040 Linz

Fax:
++43 (732) 2468-8599

Telefon:
++43 (732) 2468-9330

Informationen zur LVA:

WWW:
http://www.fim.uni-linz.ac.at/staff/sonntag/LTAEC_Budapest/

Sprechstunden:
Montag 9-11 Uhr Raum T663 oder nach Vereinbarung

Zweite, aktualisierte und erweiterte Auflage
(Für LVA in Budapest gekürzt)

Inhaltsverzeichnis

I. Kryptographie

In diesem Kapitel werden ausgewählte Aspekte der Kryptographie behandelt, die in engem Zusammenhang mit E-Commerce stehen. Nach einer kurzen Erläuterung der Grundprinzipien und der Angriffsmöglichkeiten werden einige ausgewählte Verfahren ihrem Prinzip nach erläutert. Weiters wird das besondere Problem der Verwahrung von Schlüsseln dargestellt: Wie können Schlüssel einfach und bequem gespeichert werden, jedoch ohne daß fremde Personen Zugriff darauf erlangen können? Zum Abschluß wird das Problem der Verteilung von öffentlichen Schlüsseln untersucht, wobei besonders auf Zertifizierungsstellen eingegangen wird.

1. Allgemeines

In diesem Abschnitt wird kurz die Notwendigkeit von Verschlüsselung und der Verwendung von Signaturen erläutert und anschließend einige grundlegenden Begriffe definiert.

1.1. Notwendigkeit

Nicht immer sollen alle beliebigen Personen jede Kommunikation mithören können. Im persönlichen Bereich ist dies relativ einfach: Man begibt sich zu zweit in ein Zimmer mit guter Schalldämmung und kann eine private Unterhaltung führen. Bei elektronischer Kommunikation ist die viel schwieriger: Praktisch alle Kommunikationsmedien sind öffentlich zugänglich und ein Abhören ist mit geringem oder geringstem Aufwand möglich. Aus diesem Grund besteht ein starker Bedarf nach Technologie, welche eine geheime Kommunikation über einen öffentlichen Kanal ermöglicht. Als Analogon dazu kann ein versiegelter Brief dienen, der auch durch mehrere Hände wandert, bevor er beim Empfänger einlangt.

Genauso wie in unserem Beispiel soll es aber auch für den Staat möglich sein, in besonderen Fällen diese Geheimhaltung zu umgehen. In der Praxis erfolgt dies durch “Wanzen”, die es erlauben geheime Gespräche zu belauschen. Kryptographie ist in dieser Hinsicht viel problematischer für den Staat, da bei den meisten Systeme keine “Hintertür” existiert, die ein (autorisiertes) Entschlüsseln ohne Kenntnis des Schlüssels erlaubt. Vor diesem Hintergrund ist daher auch die Bestrebungen zur Eindämmung (Verwendungsverbot, Exportverbot) von starker Kryptographie zu sehen. Systeme mit solchen Hintertüren wurden zwar vorgeschlagen (“Key-Escrow-Systeme”, z. B. Clipper), doch konnten sie sich nicht durchsetzen.

Im Gegensatz zur Verschlüsselung unterliegen Signaturen keinen derartigen staatlichen Einschränkungen. Sie sollen eine elektronische Form der Unterschrift darstellen und so einen Text einer Person zuordnen, ohne daß diese bestreiten kann, daß sie ihn signiert (=unterschrieben) hat. Um E-Commerce zu fördern, wurden sogar rechtliche Rahmenbedingungen geschaffen, um ihre Verbreitung zu fördern (Siehe das Kapitel zum Signaturgesetz). Sie sollen dazu dienen, die (scheinbare) Anonymität im Internet in bestimmten wichtigen Fällen in eine sichere Identifikation zu verwandeln: Wichtigstes Anwendungsbeispiel ist der Kaufvertrag, bei dem beide Seiten nun ihre Identität beweisen können und daher im Rechtsverkehr viel weniger Unsicherheiten für beide Seiten bestehen. Sowohl der Kunde kann feststellen, bei wem er wirklich einkauft, wie auch der Händler, an wen er sich halten kann, um den Kaufpreis einzufordern.

1.2. Symmetrische / Asymmetrische Verschlüsselung

Bei symmetrischen Verschlüsselungssystemen ist der Schlüssel zur Verschlüsselung gleich dem zur Entschlüsselung während bei asymmetrischen Verfahren zwei verschiedene Schlüssel verwendet werden.[1]

1.2.1. Symmetrische Kryptosysteme

Ein symmetrisches Kryptosystem besteht aus dem Tupel (X, Y, K, $f_{encrypt}$, $f_{decrypt}$).

X: Originaldaten Y: Verschlüsselte Daten

K: Schlüssel (Secret key)

$f_{encrypt:}$: K x X $\rightarrow$ Y $f_{decrypt:}$: K x Y $\rightarrow$ X

Es müssen die folgenden Bedingungen gelten:

1. $f_{encrypt}$(k,*) und $f_{decrypt}$(k,*) müssen für alle k effizient zu berechnen sein. Unter effizient ist hier eine Berechnung in polynomialer Zeit zu verstehen, um eine schnelle Codierung und Decodierung zu gewährleisten.
2. Für alle Schlüssel k und alle Originaldaten x muß gelten: $f_{decrypt}$(k, $f_{encrypt}$(k, x)=x. Die Decodierung der verschlüsselten Daten mit dem Originalschlüssel muß wieder die Eingabe ergeben.
3. Für alle Schlüssel k muß es “schwierig” sein (d. h. nur in nicht-polynomialer Zeit), aus der Kenntnis von (X, Y, K, $f_{encrypt}$, $f_{decrypt}$) und einer beliebigen Anzahl von Paaren (x, $f_{encrypt}$(k, x)) den Schlüssel k zu berechnen. Die erste Bedingung soll sicherstellen, daß der Algorithmus veröffentlicht werden kann, ohne die Sicherheit zu gefährden. Die zweite Bedingung stellt den sogenannten “known plaintext attack” dar, bei dem sowohl die Originaldaten wie auch die verschlüsselten Daten bekannt sind.
4. Für alle Schlüssel k und alle Originaldaten x muß es “schwierig” sein, aus der Kenntnis von (X, Y, K, $f_{encrypt}$, $f_{decrypt}$) und der Kenntnis von $f_{encrypt}$(k, x) die Originaldaten x zu berechnen, ohne den Schlüssel k zu kennen. Dies ist der klassische “ciphertext only attack”, bei dem nur der Algorithmus und die verschlüsselten Daten zur Verfügung stehen und sowohl der Schlüssel als auch damit die Originaldaten berechnet werden sollen.

1.2.2. Asymmetrische Kryptosysteme

Ein asymmetrisches Kryptosystem besteht aus dem Tupel (X, Y, P, S, $f_{encrypt}$, $f_{decrypt}$).

X: Originaldaten Y: Verschlüsselte Daten

P: Öffentlicher Schlüssel (public key) S: Geheimer Schlüssel (private key)

$f_{encrypt:}$: P x X $\rightarrow$ Y $f_{decrypt:}$: S x Y $\rightarrow$ X

Es müssen die folgenden Bedingungen gelten:

1. $f_{encrypt}$(p,*) und $f_{decrypt}$(s,*) müssen für alle Schlüsselpaare p und s effizient zu berechnen sein. Unter effizient ist hier wieder eine Berechnung in polynomialer Zeit zu verstehen.

[1] Nach [Pfaff 96]

2. Für jeden öffentlichen Schlüssel p existiert ein privater Schlüssel s=s(p) sodaß für alle Originaldaten x gilt: $f_{decrypt}(s, f_{encrypt}(p, x))=x$. Die Decodierung mit dem privaten Schlüssel der verschlüsselten Daten muß wieder die Eingabedaten ergeben und zu jedem öffentlichen Schlüssel muß ein passender privater Schlüssel existieren (der vom Öffentlichen abhängt).
3. Für alle öffentlichen Schlüssel p muß es "schwierig" sein (d. h. nur in nicht-polynomialer Zeit), aus der Kenntnis von (X, Y, P, S, $f_{encrypt}$, $f_{decrypt}$) und einer beliebigen Anzahl von Paaren (x, $f_{encrypt}(p, x)$) den geheimen Schlüssel s=s(p) zu berechnen. Diese Bedingung ist nicht in den üblichen Definitionen enthalten[2], muß jedoch vorausgesetzt werden, da bei einem asymmetrischen Verfahren der öffentliche Schlüssel üblicherweise wirklich "öffentlich" bekannt ist und daher beliebig viele solcher Paare berechnet werden können!
4. Für alle öffentlichen Schlüssel p und alle Originaldaten x muß es "schwierig" sein, aus der Kenntnis von (X, Y, P, S, $f_{encrypt}$, $f_{decrypt}$), der Kenntnis von p und der Kenntnis von $f_{encrypt}(p, x)$ die Originaldaten x zu berechnen, ohne den privaten Schlüssel s zu kennen.
5. Die Berechnung des privaten Schlüssels s=s(p) aus der Kenntnis des öffentlichen Schlüssels p muß "schwierig" sein, also exponentielle Zeit benötigen.

1.2.3. Vergleich symmetrischer und asymmetrischer Verfahren

Symmetrische Verfahren sind gegenüber asymmetrischen meist um den Faktor 10 bis 100 schneller. Aus diesem Grund werden asymmetrische Verfahren nur dann eingesetzt, wenn dies unbedingt notwendig ist. Die Länge der zu verarbeiteten Daten wird so gering wie möglich gehalten.

Symmetrische Algorithmen besitzen Schlüssellängen zwischen 56 und 128 Bit, während asymmetrische Algorithmen heute sinnvollerweise bei einer Untergrenze von 768 Bit beginnen. Dies hat vor allem den Grund, daß bei asymmetrischen Systemen viel weniger Zahlen als Schlüssel in Frage kommen (DES: Alle Zahlen bis auf genau 16, also 2^{56}-16; RSA: nur Primzahlen, diese werden bei steigender Zahlengröße aber immer seltener).

1.3. Verschlüsselung ⇔ Hash-Funktionen

Es ist wichtig, zwischen einer Verschlüsselungs- und einer Hash-Funktion zu unterscheiden, da diese einen wichtigen Unterschied in Bezug auf die Wahrung der Information besitzen:

1.3.1. Verschlüsselungsfunktionen

Verschlüsselungsfunktionen sind Funktionen, zu denen eine inverse Funktion existiert, d. h. $f_{decode}(f_{encode}(x))=x$, wobei die beiden Funktionen bei symmetrischen Systemen gleich sind und bei asymmetrischen Funktionen unterschiedlich. Die Information ist in der codierten Form immer noch vollständig enthalten, auch wenn eventuell Redundanzen entfernt worden sind (z. B. bei Komprimierung) und kann daher durch die Decodierung vollständig wiederhergestellt werden. Solche Funktionen werden für alle Arten von Verschlüsselungen und Komprimierungen verwendet.

Bei symmetrischen Verschlüsselungssystemen muß es "schwierig" sein, aus der Kenntnis von $f_{encode}(x)$ wieder x zu berechnen (Der Schlüssel ist hier in der Funktion enthalten). Bei asymmetrischen Systemen kann auch noch die Funktion f_{encode} bekannt sein, ohne daß daraus f_{decode} oder x zu berechnen sein dürfen.

---

[2] So etwa nicht in der ursprünglichen Definition von Diffie und Hellmann. Wahrscheinlich als selbstverständlich vorausgesetzt.

1.3.2. Hash-Funktionen

Hash-Funktionen oder Einwegfunktionen besitzen keine Rücktransformation, d. h. es existiert keine Funktion $f_{decode}(x)$, sodaß $f_{decode}(f_{encode}(x))=x$ ist. Dies bedeutet, daß durch ihre Anwendung ein Informationsverlust auftritt. Die ursprünglichen Daten können daher niemals wiederhergestellt werden. Ihr Anwendungsbereich liegt unter Anderem bei Prüfsummen und Signaturen sowie bei der Speicherung von Paßworten oder bei der Generierung von Zufallszahlen.

Bei Sicherheitssystemen kommt es darauf an, daß aus der Kenntnis von $f_{encode}(x)$ es "schwierig" sein muß, ein y zu finden, sodaß $f_{encode}(x) = f_{encode}(y)$ ist. Bei einer Speicherung von Paßwörtern in codierter Form würde dieses y ein äquivalentes Paßwort darstellen, welches an Stelle des echten (x) akzeptiert werden würde.

1.4. Angriffsarten und Sicherungsmaßnahmen

Folgende Angriffsarten sind grundsätzlich auf ein System öffentlicher Datenübertragung möglich und müssen daher verhindert werden (Nach [Schaumüller 99] und [Pfaff 96] mit Ergänzungen):

- Abhören: Der Versuch, Daten während der Übertragung zu kopieren um diese dann selbst nutzen zu können. Beispiel: Mitschreiben von Kreditkartennummern, um mit diesen dann Mißbrauch betreiben zu können.
- Manipulation: Die Veränderung von Daten während der Übertragung, sodaß die Änderung nicht bemerkt wird und die Daten in abgewandelter Form akzeptiert werden. Beispiel: Ändern der Kontonummer einer Überweisung.
- Wiedereinspielen: Die Wiederholung einer Original-Nachricht in unveränderter Form. Beispiel: Senden fremder E-Cash Daten zur Begleichung einer eigenen Schuld.
- Vortäuschen einer falschen Identität: Zugriff auf einen Rechner erlangen, indem man sich als eine andere Person/Rechner/Programm ausgibt, als man tatsächlich ist. Beispiel: Benutzen fremder Paßwörter um eingeschränkt verfügbare Dienste nutzen zu können.
- Abstreiten: Das Bestreiten des Empfangs oder des Absendens einer Nachricht, obwohl dies tatsächlich von dieser Person/Rechner/Programm erfolgte. Beispiel: Bestreiten des Empfangs der Zahlung.
- Serviceverhinderung: (Be-)Hinderung anderer Personen/Rechner/Programme daran, bestimmte Dienste in Anspruch zu nehmen. Beispiel: Abschicken großer Datenmengen, um einen anderen Rechner zum Absturz zu bringen oder so zu blockieren.
- Verkehrsanalyse: Beobachtung des Kommunikationsmusters, um daraus Schlüsse zu ziehen. Beispiel: Beobachtung welche Internet-Shops eine Person besucht bzw. wo sie einkauft.

Gegen diese Angriffsmöglichkeiten sind die folgenden Sicherungsmaßnahmen möglich. Diese können einzeln, aber auch in Kombination eingesetzt werden:

- Authentisierung: Der Nachweis einer angegebenen Identität einer Person, eines Rechners oder eines Programmes.
- Isolation: Zuordnung von bestimmten Rechten auf Objekte zu Identitäten und die Verhinderung des unerlaubten Zugriffs.
- Verschlüsselung: Kodierung von Daten, sodaß Personen ohne die zugehörigen geheimen Informationen nicht an die enthaltenen Daten gelangen können.

- Integritätsprüfung: Prüfung, ob die Daten nicht absichtlich verändert wurden (Checksummen: Sicherung gegen zufällige Fehler).
- Signaturen: Zuordnung von Identitäten zu von ihnen approbierten Nachrichten (Notwendige Eigenschaften: Personenabhängigkeit, Dokumentenabhängigkeit, Überprüfbarkeit, Fälschungssicherheit und Dokumentenechtheit; Siehe dazu das Kapitel zum Signaturgesetz)
- Steganographie: Das Verstecken einer Nachricht in anderen Daten, sodaß ihre Existenz nicht klar sichtbar ist.

In der folgenden Tabelle ist aufgelistet, welche Sicherungsmaßnahmen zur Verhinderung welcher Angriffsarten eingesetzt werden können. Zusätzlich wird noch zwischen detektiven (D) und präventiven (P) Methoden unterschieden. In Klammern gesetzte Buchstaben sind dazu nur eingeschränkt verwendbar.

Detektive Methoden erlauben es, im Nachhinein zu erkennen, daß ein Angriff stattgefunden hat, können ihn aber nicht verhindern. Im Gegensatz dazu verhindern präventive Methoden einen erfolgreichen Angriff, führen aber nicht automatisch zur Entdeckung eines Versuches.

Angriffsart	**Sicherungsmaßnahmen**					
	Authenti-sierung	Isolation	Verschlüs-selung	Integritäts-prüfung	Signaturen	Steganograph. (wenn geheim)
Abhören		(D, P)	P			P
Manipulation	(D)	(D, P)	D	D	D	P
Wiedereinspielen	(D)			D	D	P
Vortäuschen einer falschen Identität	P	D, P	(D)	(D)	D	
Abstreiten				D	P	
Serviceverhinderung	D	D, (P)				
Verkehrsanalyse			(P)			P

2. Ausgewählte kryptographische Verfahren

In diesem Abschnitt werden wichtige Elemente beschrieben, die bei der Implementierung von kryptographischen Systemen von Bedeutung sind. Dies sind einerseits Algorithmen, andererseits auch Signaturen und Zertifikate.

2.1. Diffie-Hellman Key Agreement

Der DH-Key-Agreement Algorithmus ([PKCS]: PKCS #3) erlaubt es, daß zwei oder mehrere Personen einen gemeinsamen Schlüssel vereinbaren, obwohl sie nur über einen ungesicherten Kanal kommunizieren können. Es handelt sich um ein asymmetrisches Verfahren, welches nicht nur für zwei beteiligte Parteien sondern auch beliebig große Gruppen möglich ist. Das Verfahren setzt voraus, daß die Daten während der Übertragung nicht verändert werden (d. h. Signaturen beim Austausch verwenden!).

Die Schlüsselvereinbarung läuft folgendermaßen ab, wobei mehr als zwei Parteien die Daten an entsprechend mehr Partner zu übermitteln sind und mehrfache Exponentiationen durchgeführt werden müssen:

1. Eine zentrale Autorität (meist eine der beteiligten Parteien) bestimmt eine Primzahl p und eine ganze Zahl g für die gilt: $0 < g < p$. Diese Daten werden an beide Parteien übermittelt.
2. Jede Partei i berechnet eine eigene Zufallszahl x_i mit der Eigenschaft $0 < x_i < p-1$. Aus diesem privaten Wert wird ein öffentlicher Wert y nach folgender Formel berechnet: $y= (g^{xi}) \bmod p$. Dieser Wert y wird dann an die andere Partei versendet.
3. Jede der Parteien berechnet sich aus der von der anderen Partei erhaltenen Zahl y' den gemeinsamen geheimen Wert $z = (y'^{xi}) \bmod p$. Dieser Wert ist bei beiden Parteien gleich:

$$z = g^{x_i x_j} \bmod p = g^{x_j x_i} \bmod p = g^{x_i * x_j} \bmod p$$

Eine Partei, die alle Nachrichten kennt (g, p und beide y), kann dennoch z nicht berechnen. Dieses Protokoll beruht darauf, daß in einem Primzahlenkörper eine Exponentiation zwar relativ einfach durchzuführen ist, die Berechnung des diskreten Logarithmus jedoch äußerst schwierig und langsam ist.

Dieses Protokoll findet immer dann Anwendung, wenn zwei Rechner einen gemeinsamen Schlüssel vereinbaren wollen, sich jedoch gegenseitig nicht kennen (und daher keinen gemeinsamen geheimen Schlüssel besitzen). In diesem Fall erfolgt nach einer Authentisierung mittels asymmetrischer Algorithmen (Zertifikate) die Vereinbarung eines sogenannten "session key" mit dem DH-Protokoll für die Kommunikation mittels symmetrischer Verschlüsselung. Um einen Angriff einer dazwischenliegenden Instanz zu verhindern (man-in-the-middle attack) muß der Nachrichtenaustausch mittels Signaturen gesichert werden.

2.2. Passphrase Based Encryption

Ein großes Problem ist bei allen Sicherheitssystemen, wie der Schlüssel gespeichert wird: Einfache Schlüssel sind unsicher und komplexe (z. B. eine 1024 Bit Zahl als RSA-Schlüssel) können normale Menschen sich nicht merken. Da jede Person auch mehrere Schlüssel verwendet (für verschiedene Anwendungen, unterschiedliche Algorithmen und als Sicherheitvorkehrung), muß daher eine Möglichkeit geschaffen werden, diese zu speichern. Dies kann einerseits extern des Rechners erfolgen (Beispielsweise auf einer Chipkarte) oder intern als Datei. Die interne Speicherung bedingt jedoch, daß die Datei vor unbefugtem Zugriff geschützt sein muß. Dies muß insbesondere auch gegenüber dem Administrator des Rechners und allen anderen sonst privilegierten Personen gegenüber gelten. Die Möglichkeit, die Schlüssel-Datei zu lesen soll noch zu keinem Sicherheitsverlust führen. Es ist also nötig, diese Schlüssel-Sammlungen wiederum zu verschlüsseln. Dazu wird jedoch ein Schlüssel benötigt, welcher irgendwo zu speichern ist....

Dieses Henne-Ei Problem kann mit der sogenannten "Passphrase based encryption"[3] gelöst werden. Hier wird aus einer Menschen-lesbaren (und merkbaren) Phrase, also einem längeren Satz, ein Schlüssel berechnet, der dann zur Verschlüsselung verwendet werden kann. Dies erfolgt mittels einer Hash-Funktion. Es gelten für die Phrase die selben Anforderungen wie für Paßwörter, doch sollte sie

[3] Siehe dazu PKCS #5: Password-based Cryptography standard: http://www.rsa.com/rsalabs/pubs/PKCS

länger sein, um eine Wörterbuch-Attacke zu verhindern (>20 Zeichen). Dennoch ist diese Methode nur mittelmäßig sicher. Um die Sicherheit zu erhöhen, werden zwei zusätzliche Punkte eingeführt:

1. Salz: Hierbei handelt es sich um eine Zufallszahl (typischerweise 64 Bits lang). Diese wird an die Paß-Phrase angehängt, bevor dieses in die Hash-Funktion eingegeben wird. Es kann im Klartext gepeichert oder weitergegeben werden. Es dient einerseits dazu, den Schlüsselraum zu erweitern (für jedes Paßwort gibt es nun 2^{64} verschiedene Schlüssel), sodaß ein Angreifer kein Wörterbuch mehr erstellen kann, sondern mit dem nur ab dem tatsächlichen Einsatz bekannten Salz nun alle möglichen Pass-Phrasen durchprobieren kann. Weiters verhindert es, daß bei zwei Verwendungen des selben Paßwortes der gleiche Schlüssel verwendet wird. Steht kein oder kein guter Zufallszahlengenerator zur Verfügung, kann auch die Anwendung einer Hash-Funktion auf die zu übertragende Nachricht zur Produktion des Salzes verwendet werden.
2. Um die Berechnung einer Tabelle durch einen Angreifer zu erschweren, wird ein Wiederholungszähler eingebaut. Dieser bewirkt, daß das Paßwort nicht nur einmal, sondern n-Mal durch die Hash-Funktion geschickt wird: T_1 = Hash(Salz +Pass-Phrase), T_2 = Hash(T_1), ... T_n = Hash(T_{n-1}). Diese Iteration sollte mindestens 1000 mal durchgeführt werden (Praxis: 2000). Dies bedeutet für den echten Verwender kein Problem, da Hash-Funktionen sehr schnell berechnet werden können. Ein Angreifer benötigt jedoch dann die n-fache Zeit um ein Wörterbuch aufzustellen.

Sowohl Salz wie auch der Iterations-Zähler können gefahrlos unverschlüsselt übertragen werden. Durch ihre Kenntnis ergibt sich keine neue Angriffsmöglichkeit.

2.3. Signaturen

Eine Signatur stellt gleichzeitig zwei Sicherheitsmechanismen zur Verfügug: Einerseits kann die Identität einer Person überprüft werden, indem die Kenntnis des privaten Teils eine Schlüsselpaares überprüft wird. Signaturen sind daher nur mit asymmetrischen Verschlüsselungssystemen möglich[4]. Andererseits kann auch überprüft werden, ob die Nachricht zwischen dem Zeitpunkt des Signierens und des Prüfens der Signatur verändert wurde.

Eine Signatur ist daher im Endeffekt wie eine Unterschrift: Auch diese identifiziert eine bestimmte Person und verhindert (großteils) nachträgliche Veränderungen. Signaturen bieten jedoch keinerlei Vertraulichkeit. Es ist ihre Eigenschaft, daß sie eben von jeder Person (mit Kenntnis des öffentlichen Schlüssels) überprüft werden kann.

Ein System zur Erstellung digitaler Signaturen besteht aus dem Tupel (X, Y, P, S, f_{sign}, f_{verify}).

X: Originaldaten Y: Signatur

P: Öffentlicher Schlüssel (public key) S: Geheimer Schlüssel (private key)

f_{sign}: $S \times X \rightarrow Y$ f_{verify}: $P \times (X \times Y) \rightarrow \{OK, falsch\}$

Es müssen die folgenden Bedingungen gelten:

[4] Achtung: Nicht alle Signatursysteme lassen sich auch zur Verschlüsselung einsetzen! RSA ermöglicht sowohl Verschlüsselung wie auch Signaturen, während DSA (Digital Signature Algorithm) nur Signaturen erlaubt (und daher auch mit beliebiger Schlüssellänge aus Amerika exportiert werden darf!).

1. $f_{sign}(s,*)$ und $f_{verify}(p,*,\#)$ müssen für alle Schlüsselpaare p und s effizient zu berechnen sein. Unter effizient ist hier wieder eine Berechnung in polynomialer Zeit zu verstehen.
2. Für jeden öffentlichen Schlüssel p existiert ein privater Schlüssel s=s(p) sodaß für alle Originaldaten x gilt: $f_{verify}(p, x, y)$ = OK dann und nur dann, wenn $y = f_{sign}(s, x)$. Die Überprüfung der Signatur der Daten mit dem öffentlichen Schlüssel darf immer nur dann (und dann immer) erfolgreich sein, wenn die Signatur mit dem zugehörigen privaten Schlüssel erzeugt wurde. Zu jedem öffentlichen Schlüssel muß ein passender privater Schlüssel existieren (der vom öffentlichen Schlüssel abhängt).
3. Für alle öffentlichen Schlüssel p muß es "schwierig" sein (d. h. nur in nicht-polynomialer Zeit), aus der Kenntnis von (X, Y, P, S, f_{sign}, f_{verify}) und einer beliebigen Anzahl von Paaren (x, $f_{sign}(s, x)$) den geheimen Schlüssel s=s(p) zu berechnen. Selbst aus einer großen Anzahl von signierten Dokumenten (bei denen der Klartext bekannt ist; d. h. known-plaintext attack!) darf der private Schlüssel nicht ableitbar sein.
4. Für alle öffentlichen Schlüssel p und alle Originaldaten x muß es "schwierig" sein, aus der Kenntnis von (X, Y, P, S, f_{sign}, f_{verify}), der Kenntnis von p und der Kenntnis von x, aber ohne die Kenntnis von s=s(p) die Signatur $y=f_{sign}(s, x)$ zu berechnen.
5. Die Berechnung des privaten Schlüssels s=s(p) aus der Kenntnis des öffentlichen Schlüssels p muß "schwierig" sein, also exponentielle Zeit benötigen.

2.4. Zertifikate nach X.509v3

Zertifikate kann man sich als eine Art "digitaler Ausweis" vorstellen. Sie dienen dazu, eine eindeutige Verbindung zwischen einer Person und einem öffentlichen Schlüssel (und damit auch zu einem privaten Schlüssel!) herzustellen. Zertifikate werden immer von einer bestimmten Instanz ausgestellt, einer sogenannten "Zertifizierungsstelle" (Certificate Authority, CA). Ein Zertifikat hat jedoch nur dann irgendeine Bedeutung, wenn der Verwender des Zertifikats, der dessen Echtheit überprüfen möchte, Vertrauen zu dieser Ausgabestelle hat. Eine wichtige Voraussetzung dafür ist, daß die Zertifizierungsstelle genau bekanntgibt, welche Angaben überprüft werden, bevor ein Zertifikat ausgestellt wird: Nur auf diese kann man sich verlassen, wenn eine Überprüfung erfolgreich ist.

Um ein Zertifikat problemlos öffentlich übertragen zu können und die Unverändertheit der bestätigten Informationen zu garantieren, werden die Daten bei der Zertifizierungsstelle eingereicht, diese überprüft sie und versieht diese anschließend mit einer elektronischen Signatur, wozu ihr eigener privater Schlüssel verwendet wird. Um die Gültigkeit zu überprüfen, ist daher die Kenntnis des öffentlichen Schlüssels der Zertifizierungsstelle notwendig (Siehe dazu Abschnitt 2.4.2).

2.4.1. Bestandteile von Zertifikaten nach X.509v3

Zertifikate bestehen aus folgenden Elementen:

1. Der X.509 Standard hat mehrere Versionen hinter sich. Daher muß bei jedem Zertifikat angegeben werden, welcher Version es entspricht.
2. Um ein Zertifikat eindeutig identifizieren zu können (Eine Person kann mehrere Zertifikate des selben Schlüssels von der selben Zertifizierungsstelle besitzen; z. B. für verschiedene Verwendungszwecke in verschiedenen Qualitäten), muß jede CA eine eindeutige Seriennummer vergeben.

3. Da ein Zertifikat immer nur in Zusammenhang mit einer Zertifizierungsstelle und ihren Prüfungs-Richtlinien eine Bedeutung hat, muß diese im Zertifikat eindeutig gekennzeichnet werden (Idealerweise Klartext und URL).
4. Ein Zertifikat ist immer nur während einer beschränkten Zeit gültig. Dies soll verhindern, daß ein einmal gebrochenes Zertifikat (einem Angreifer gelang es, an den privaten Schlüssel heranzukommen) zu große Folgen nach sich zieht: Nach seiner Ablaufzeit ist es jedenfalls ungültig. Dies erfolgt durch die Angabe von einem Beginn- und einem Endedatum.
5. Die eine Hälfte des wichtigsten Teils ist das "Subjekt": Für wen das Zertifikat ausgestellt wird, also wem der angegebene öffentliche Schlüssel zugeordnet wird.
6. Die andere Hälfte ist der öffentliche Schlüssel, der dem Subjekt zugeordnet ist. Er ist in einer Algorithmus-spezifischen Form codiert.
7. Bei einem Zertifikat der Version 3 können noch Erweiterungen angebracht werden: Ein Beispiel dafür ist, wozu das zertifizierte Schlüsselpaar verwendet werden darf: z. B. nur zur Signatur oder auch zur Verschlüsselung von Nutzdaten oder zur Verschlüsselung von anderen Schlüsseln.

Um ein Zertifikat auf allen Plattformen verwenden zu können, muß eine eindeutige Repräsentation erfolgen. Diese muß bis auf das letzte Bit genau festlegen, wie die einzelnen Element gespeichert werden. Dazu wird die ASN.1 - Notation (Abstract Syntax Notation One)[5] mit DER-Kodierung verwendet. Ein X.509v3 Zertifikat ist als ASN.1 Sequenz definiert:

```
Certificate ::= SEQUENCE
{
   tbsCertificate       TBSCertificate,
   signatureAlgorithm   AlgorithmIdentifier,
   signature            BIT STRING
}
```

Es enthält also das eigentliche Zertifikat, eine Kennzeichnung des zur Signierung verwendeten Algorithmus und die eigentlichen Signaturdaten, an Hand derer das Zertifikat überprüft werden kann. Der eigentliche Zertifikats-Inhalt ist definiert als:

```
TBSCertificate ::= SEQUENCE
{
   version         [0]  EXPLICIT Version DEFAULT v1,
   serialNumber         CertificateSerialNumber,
   signature            AlgorithmIdentifier,
   issuer               Name,
   validity             Validity,
   subject              Name,
   subjectPublicKeyInfo SubjectPublicKeyInfo,
   issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                        -- If present, version must be v2 or v3
   subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                         -- If present, version must be v2 or v3
   extensions      [3]  EXPLICIT Extensions OPTIONAL
                        -- If present, version must be v3
}
```

[5] Definiert in dem ITU-T X.208 Standard. (International Telecommunications Union; früher CCITT). X.509 Zertifikate werden nach den Distinguished Encoding Rules (DER) kodiert (Eine der Möglichkeiten, ASN.1 Strukturen in Bitfolgen umzuwandeln).

2.4.2. Zertifikats-Hierarchien

Zertifizierungsstellen sind üblicherweise in einer baumartigen Struktur angeordnet: Das Zertifikat einer CA, mit dessen zugehörigen privaten Schlüssel die Zertifikate von Kunden signiert werden, wird von der Zertifizierungsstelle höherer Instanz signiert. Die oberste Zertifizierungsstelle wird "Oberste Zertifizierungsstelle" (Root-CA) genannt. Ihr Schlüssel muß besonders sicher und sehr gut geschützt werden: Wird ihr privater Schlüssel bekannt, sind **alle** mit diesem Schlüssel ausgestellten Zertifikate plötzlich wertlos. Ihr Zertifikat wird mit dem eigenen Schlüssel signiert, daher ist es mit dem Schlüssel, der darin enthalten ist, überprüft werden (self-signed certificate). Ob ein solches Zertifikat gültig ist, kann innerhalb des Systems nicht festgestellt werden. Dies hat extern zu erfolgen, z. B. mit der Veröffentlichung einer Prüfsumme in Zeitungen oder einer Verteilung übere sichere Kanäle (z. B. bei Behörden abzuholen).

2.4.3. Widerrufs-Listen

Da Zertifikate auch kompromittiert werden können oder auch der Grund ihrer Ausstellung nicht mehr existiert (Beispielsweise eine darin zertifizierte Kreditkartennummer ist wegen mangelnder Bonität nicht mehr gültig), muß es eine Möglichkeit geben, Zertifikate vor ihrem Ablaufdatum für ungültig zu erklären. Dazu werden Widerrufs-Listen verwendet, in denen die ungültigen Zertifikate aufgelistet sind. Leider existieren zur Zeit noch keine Standards, wie dies geschehen soll, sondern lediglich Vorschläge. Diese Listen müßten entweder von jeder Zertifizierungsstelle für ihre Zertifikate oder von einer Root-CA für alle Zertifikate zur Verfügung gestellt werden. Auch bei ihnen muß darauf geachtet werden, daß sie während der Übertragung nicht verändert werden können, daher sind diese Listen ebenfalls zu signieren (unter anderem auch, um ein späteres Abstreiten durch die Zertifizierungsstelle zu verhindern).

2.4.4. Beispiel eines Zertifikates

```
 [ [  Version: V1
  Subject: CN="Server Certificate, RSA (self-signed)", OU=FIM, O=Uni-Linz, C=AT
  Signature Algorithm: MD5withRSA, OID = 1.2.840.113549.1.1.4

  Key:  public exponent: 3
modulus:
8ecbd113a02932ed0b04199eecd84f12ea076378ae7c24ba9a60c02adbf29a5bacb1bc39aaf9475e24e713
1781c49b7a900bb9bda7ef09037a7c357ad62d20dbce969c1017cb5549007820cf8b8e1fa916dd49b61d58
3c25876289b3e2f8bc3337ddc9714
7e50f2030bf563486db8371bb1f00b8d62b3b06a87de776cf79a729

  Validity: [From: Wed Oct 20 23:11:37 GMT+02:00 1999,
              To: Sat Nov 20 23:11:37 GMT+01:00 1999]
  Issuer: CN=FIM Test CA, OU=FIM, O=Uni-Linz, C=AT
  SerialNumber: [    01]

]
  Algorithm: [MD5withRSA]
  Signature:
0000: 7E C4 DD C5 05 D0 54 40   09 D8 AF 3A 1B 29 F1 7F  ......T@...:.)..
0010: 74 36 05 B5 2D D3 9C D7   63 F3 64 D9 71 D1 86 F4  t6..-...c.d.q...
0020: 9A 5C BE 9E EE 01 B5 0F   AB 1E 1F DC FE CC 68 84  .\............h.
0030: DF 6D 7F 8F 03 28 7E 4D   F4 E8 12 42 C5 1C 40 54  .m...(.M...B..@T
0040: 71 4A 01 B0 68 66 6A FE   FC B6 D3 D6 07 CE 5C A4  qJ..hfj.......\.
0050: 7E DF 4B 13 3F 84 C8 4F   15 9A 04 F3 98 21 AF 49  ..K.?..O.....!.I
0060: 0A 90 4A 2D D2 3E 2D 3B   6F A2 40 19 21 B6 7A D6  ..J-.>-;o.@.!.z.
0070: 45 34 8C B1 5A 07 74 3D   16 18 97 BD 52 3D 2C 6E  E4..Z.t=....R=,n
]
```

Das selbe Zertifikat in Base64-Codierung zur Übertragung:

```
-----BEGIN CERTIFICATE-----
```

```
MIICDzCCAXgCAQEwDQYJKoZIhvcNAQEEBQAwRDELMAkGA1UEBhMCQVQxETAPBgNV
BAoTCFVuaS1MaW56MQwwCgYDVQQLEwNGSU0xFDASBgNVBAMTC0ZJTSBUZXN0IENB
MB4XDTk5MTAyMDIxMTEzN1oXDTk5MTEyMDIyMTEzN1owXjELMAkGA1UEBhMCQVQx
ETAPBgNVBAoTCFVuaS1MaW56MQwwCgYDVQQLEwNGSU0xLjAsBgNVBAMTJVNlcnZl
ciBDZXJ0aWZpY2F0ZSwgUlNBIChzZWxmLXNpZ25lZCkwgZ0wDQYJKoZIhvcNAQEB
BQADgYsAMIGHAoGBAI7L0ROgKTLtCwQZnuzYTxLqB2N4rnwkuppgwCrb8ppbrLG8
Oar5R14k5xMXgcSbepALub2n7wkDenw1etYtINvOlpwQF8tVSQB4IM+Ljh+pFt1J
th1YPCWHYomz4vi8MzfdyXFH5Q8gML9WNIbbg3G7HwC41is7Bqh953bPeacpAgED
MA0GCSqGSIb3DQEBBAUAA4GBAH7E3cUF0FRACdivOhsp8X90NgW1LdOc12PzZNlx
0Yb0mly+nu4BtQ+rHh/c/sxohN9tf48DKH5N9OgSQsUcQFRxSgGwaGZq/vy209YH
zlykft9LEz+EyE8VmgTzmCGvSQqQSi3SPi07b6JAGSG2etZFNIyxWgd0PRYYl71S
PSxu
-----END CERTIFICATE-----
```

2.5. Secure Socket Layer (SSL)

SSL ist ein Protokoll das dazu dient, eine sichere Verbindung über das Internet aufzubauen. Es ist unabhängig von dem darüberliegenden Protokoll und ist daher für jede Applikation einsetzbar. Als Basis wird nur ein verläßliches Transportprotokoll vorausgesetzt (typischerweise TCP/IP). Es verhindert:

- Abhören: Die Kommunikation wird verschlüsselt
- Manipulation: Es werden kryptographische Prüfsummen verwendet.
- Wiedereinspielen: Es werden die Pakete durchnumeriert.
- Vortäuschen einer falschen Identität (Standardmäßig nur des Servers, aber auch für den Client möglich): Es werden Zertifikate ausgetauscht und die Kenntnis des entsprechenden privaten Schlüssels überprüft. Als Standard wird nur der Server authentifiziert, es kann jedoch auch vom Client ein Zertifikat verlangt werden oder das des Servers wegfallen (In diesem Fall ist keine Sicherheit gegenüber man-in-the-middle Attacken mehr gegeben!).
- Abstreiten: Da derjenige, der ein Zertifikat anbietet, auch die Kenntnis des privaten Schlüssels beweisen muß, kann er später die Verbindung nicht mehr ableugnen.

Es erfolgt eine automatische Vereinbarung der verwendeten Algorithmen, daher ist auf eine richtige Konfiguration zu achten, damit nicht eine kryptographisch schwache Version gewählt wird. Da Daten nach einer Verschlüsselung nicht mehr komprimierbar sind, ist auch die Möglichkeit, die Date vorher zu komprimieren, enthalten.

Der Verbindungsaufbau bei SSL sieht folgendermaßen aus:

Client		**Server**
ClientHello	⇒	
		ServerHello
		ServerCertificate*
		ServerKeyExchange*
		CertificateRequest*
	⇐	ServerHelloDone
ClientCertificate*		
ClientKeyExchange		
CertificateVerify*		
(Umschalten auf Verschlüsselung)		
Finished	⇒	

		(Umschalten auf Verschlüsselung)
	⇐	Finished
Anwendungsdaten	⇔	Anwendungsdaten

*: Optional

Während der Übertragung von Anwendungsdaten können die verwendeten Schlüssel transparent gewechselt werden, indem Teile des obigen Protokolls wiederholt werden. Im Einzelnen zu den oben enthaltenen Schritten:

1. Client- und Server-Hello: Der Client schickt eine Zufallszahl und seine Möglichkeiten zur Verschlüsselung und Komprimierung an den Server, der darauf mit seiner Zufallszahl und einer Auswahl aus den Verschlüsselungs- und Komprimierungsalternativen antwortet. Unterstützt er keine der Methoden oder sind sie ihm zu unsicher, antwortet er mit einer Fehlermeldung und das Protokoll ist beendet. Die Zufallszahl wird dafür benötigt, um Wiedereinspielen zu vermeiden. Da diese Nachricht in verschiedenen Hash-Werten enthalten ist (Siehe unten bei Punkt 3 und 8), kann dadurch kein Wiedereinspielen erfolgen, da die andere Seite jedesmal einen neuen Wert wählt und alte Nachrichten daher nicht wiederverwendet werden können.
2. ServerCertificate: Der Server schickt sein Zertifikat und die gesamte Zertifikatsliste bis zur höchsten Zertifizierungsstelle an den Client.
3. ServerKeyExchange: Besitzt der Server kein Zertifikat oder kann es nur zum Signieren aber nicht zum Verschlüsseln verwendet werden, so werden hiermit die Daten zur Schlüsselgenerierung an den Client geschickt. Die Schlüsselgenerierung erfolgt typischerweise nach dem Diffie-Hellman Protokoll[6]. Um eine Manipulation zu verhindern, werden sowohl die Parameter zur Schlüsselgenerierung als auch die Zertifikate (voriger Punkt) mit dem privaten Schlüssel des Servers signiert.
4. CertificateRequest: Ein nicht-anonymer Server kann vom Client ein Zertifikat verlangen. Der Server schickt sowohl die Typen der akzeptierten Zertifikate, als auch die anerkannten Zertifizierungsstellen mit, um dem Client eine passende Auswahl zu ermöglichen.
5. ServerHelloDone: Diese Nachricht dient nur dazu, dem Client zu signalisieren, daß nun er an der Reihe ist, Daten zu übermitteln.
6. ClientCertificate: Der Client sendet ein passendes Zertifikate, sofern er eines besitzt bzw. eine Fehlermeldung, worauf die Verbindung beendet wird.
7. ClientKeyExchange: Der Client sendet entsprechend dem ausgewählten Protokoll die Daten für seinen temporären Schlüssel zur Kommunikationsverschlüsselung (der eigene Teil der Diffie-Hellman-Parameter, ein eigener temporärer RSA-Schlüssel bzw. FORTEZZA-Parameter).
8. CertificateVerify: Mit dieser Nachricht beweist der Client, daß er den zugehörigen Schlüssel zu seinem Zertifikat besitzt (Wird nur bei Client-Authentifizierung an den Server geschickt). Es werden ein SHA und ein MD5-Hashwert aus den bisherigen SSL-Nachrichten und dem gemeinsamen Schlüssel signiert.

[6] Weiters unterstützt: FORTEZZA (Hardware-basiertes Verfahren) und RSA: RSA-Zertifikate mit langem Schlüssel dürfen teilweise wegen Exportkontroll-Vorschriften nur zum Signieren verwendet werden. In diesem Fall wird ein temporärer kurzer RSA-Schlüssel (public key) an den Client geschickt, welcher nur für diese eine Verbindung verwendet wird. Es wird ein regelmäßiger Wechsel empfohlen, um die Sicherheit dadurch nicht zu stark zu beeinträchtigen.

9. Finished (Client und Server): Diese Nachricht ist die erste, die verschlüsselt ausgetauscht wird. Sie enthält die kryptographische Prüfsumme aller vorhergegangenen SSL-Nachrichten, um eine nochmalige Überprüfung zu ermöglichen.

Die Applikationsdaten werden daher insgesamt folgendermaßen geschützt:

- Zu versendende Daten werden mit einer kryptographischen Prüfsumme geschützt, in welche die Daten, die Seriennummer des Paketes und die Länge der Daten eingeht. Da sowohl der Server wie auch der Client einen eigenen Schlüssel dafür verwenden, kann eine Nachricht auch nicht in die andere Richtung eingefügt werden. Die Seriennummern verhindern das Unterdrücken oder Wiedereinspielen von Paketen.
- Die Daten werden bei der Übertragung verschlüsselt. Auch hier sind der Server und der Client-Schlüssel unterschiedlich, daher kann auch keine der Parteien gefälschte Nachrichten des anderen (angeblich empfangene) erzeugen.
- Die Übertragung der Schlüssel für die Prüfsumme erfolgt verschlüsselt, daher ist eine Modifikation nur dann möglich, wenn auch die Verschlüsselung gebrochen werden kann. Da es für diese Schlüssel keine Export-Restriktionen gibt, können sie länger als die Verschlüsselungs-Schlüssel sein. Selbst wenn daher die Verschlüsselung gebrochen werden kann, ist trotzdem die Garantie der Unveränderthеit der Kommunikation möglich.

3. Prinzipien der Schlüsselverwaltung

Bei dem Einsatz kryptographischer Schlüssel ist während deren Lebenszyklus auf folgende Punkte besonderer Bedacht zu nehmen, um eine Kompromittierung zu vermeiden:

1. **Erzeugung:** Die Erzeugung sollte nach Möglichkeit einen "echten" Zufall verwenden, also physikalische Zufallsgeneratoren[7] (RNG = Random Number Generator). Für einfachere Anwendungen genügen gute Pseudozufallszahlengeneratoren (PRNG = Pseudo-RNG), welche eine lange Periode aufweisen müssen und nicht manipulierbar sind (Startwert!).
2. **Verteilung:** Bei asymmetrischen Systemen wird nur der öffentliche Schlüssel verteilt, der private ist geheim zu halten. Bei symmetrischen Systemen ist es jedoch nötig, den geheim zu haltenden Schlüssel zu verteilen, weshalb eine sichere Übertragung notwendig ist. Siehe dazu das nächstes Kapitel!
3. **Speicherung:** Schlüssel sind so zu speichern, daß unbefugte Personen keinen Zugriff darauf erlangen und daß die Person, welche sie verwenden möchte, vorher ihre Identität nachweist, bevor kryptographische Operationen mit privaten oder geheimen Schlüsseln stattfinden. Dies erfolgt meist durch PINs oder Paßwörter. Die Speicherung kann einerseits in einem physikalisch sicheren Behältnis erfolgen (welches nur sehr schwer ohne Zerstörung zu öffnen ist), oder indem die Schlüssel selbst wieder verschlüsselt werden. Siehe als Beispiele hierzu die Abschnitte 3.1 und 3.2.
4. **Verwendung:** Da Schlüssel umso angreifbarer werden, je mehr mit ihnen verschlüsselte Daten zur Verfügung stehen, sollten sie möglichst oft gewechselt werden (z. B. Session-keys die jeweils nur für eine Kommunikation gelten). Ebenso sollten für verschiedene Tätigkeiten verschiedene

[7] Diese verwenden üblicherweise das Rauschen in Widerständen, welches verstärkt und anschließend zur Generierung einer Bitfolge verwendet wird.

Schlüssel verwendet werden, sodaß die Kompromittierung eines davon nicht alle Bereiche betrifft. Typischerweise werden verschiedene Schlüssel für die Verschlüsselung von E-Mails, deren Signierung, den Aufbau von Kommunikationsbeziehungen, etc. verwendet. Insbesondere bei der Verwendung von physikalischen Schlüsselspeicherungsmethoden oder dem Einsatz von Fremd-Software muß darauf geachtet werden, ob auch genau das angezeigt wird, was dann später mit dem Schlüssel verschlüsselt oder signiert wird (secure viewer).

5. **Verwaltung:** Es ist darauf zu achten, daß dem Benutzer immer klar angezeigt wird, welche Sicherheitsstufe zur Zeit verwendet wird, bzw. welchen Schlüssel er gerade verwendet. Dazu müssen Schlüssel und Zertifikate mit einem kurzen, aussagekräftigen Namen versehen werden. Da private und geheime Schlüssel nicht in Zertifikaten gespeichert werden (wo immer auch ein Name enthalten ist), ist bei ihnen beim Ablegen besonders darauf zu achten.
6. **Entsorgung:** Um ein nachträgliches Entschlüsseln zu verhindern, müssen Schlüssel am Ende ihres Einsatzes sicher zerstört werden. Bei physikalischer Speicherung ist auf eine tatsächliche Zerstörung zu achten, bei Speicherung in elektronischer Form ist ein tatsächliches Überschreiben (im Speicher bzw. auf einem Datenträger; Achtung: Buffer!) notwendig. Unter Umständen ist auch eine sichere Speicherung notwendig, um die spätere zufällige Generierung und Verwendung des selben Schlüssels zu vermeiden.

3.1. Externe Speicherung am Beispiel von Smartcards

Eine sehr sichere Möglichkeit zur Speicherung von Schlüsseln sind Smartcards (Plastikkarten mit integriertem Microchip). Aufgrund ihrer Bauweise ist es extrem schwer, physisch an die Daten heranzukommen, ohne sie zu beschädigen/löschen. Da auch Protokolle und Algorithmen verwendet werden, welche ohne Übertragung des Schlüssels aus der Karte hinaus auskommen, verläßt der Schlüssel niemals diesen relativ gut gesicherten Hardwarebereich[8]. Sie haben weiters den Vorteil, daß sie die Daten mit einer physischen Instanz verbinden: Ein Diebstahl wird relativ schnell bemerkt. Ihr Nachteil ist, daß solche Karten einerseits nicht ganz billig sind, und daß unbedingt ein zusätzliches Hardwaregerät (Kartenleser) notwendig ist. Weiters stellt sich natürlich noch das Problem, wie die Karte ihren rechtmäßigen Besitzer erkennt: Dies erfolgt üblicherweise über eine Geheimnummer (PIN), doch existieren auch schon Karten, welche ein Feld zur Überprüfung des Fingerabdrucks eingebaut haben.

3.2. Interne Speicherung am Beispiel Java Keystore

Im Gegensatz zu einer Chipkarte können die Schlüssel bei interner Speicherung nicht physikalisch geschützt werden: Es muß immer damit gerechnet werden, daß jemand Zugriff auf die Datei erhält. Aus diesem Grund werden Schlüssel, die in einem Java Keystore (Speichert Zertifikate und Schlüssel; dient u. A zum Signieren von jar-Dateien, also dem Signieren von Programmen) abgelegt sind, verschlüsselt. Darüberhinaus wird auch noch die gesamte Datei ein zweites Mal verschlüsselt. Wenn es also gelingt, die Datei zu entschlüsseln, so sind die privaten Schlüssel (Zertifikate nicht!) immer noch mit einem jeweils anderen Paßwort geschützt (sofern unterschiedliche Paßworte verwendet werden!). Ein Im- und Export von Zertifikaten und damit öffentlichen Schlüsseln ist zwar möglich, doch können private Schlüssel weder eingebracht werden noch ist ein Export möglich. Nur intern erzeugte Schlüsselpaare können verwendet werden. Da der Schlüssel keine Verkörperung besitzt, bleibt ein Diebstahl unbemerkt. Erst eine etwaige mißbräuchliche Verwendung kann (nicht

[8] Die Chips sind auch so konstruiert, daß ein Auslesen der Schlüssel mit einem falschen oder manipulierten Lesegerät gar nicht möglich ist: Die entsprechenden Daten können niemals auf einen externen Bus gelangen, da sie in einem separaten Speicher abgelegt sind: Lediglich der interne Prozessor kann darauf zugreifen.

immer sofort!) entdeckt werden, weshalb in vielen Fällen der Schaden schon entstanden ist, wenn das Sicherheitsproblem entdeckt wird.

Die Sicherheit der Schlüssel hängt bei einem Keystore hauptsächlich von den verwendeten Paßwörtern ab. Da Java von der Firma Sun entwickelt ist und das zugehörige Programm "keytool" daher aus Amerika exportiert wird, können für die Verschlüsselung nur kryptographisch schwache Algorithmen bzw. Schlüssellängen verwendet werden. Die Sicherheit ist daher auch aus diesem Grund als nicht besonders hoch anzusehen.

4. Schlüsselverteilung

Ein großes Problem bei der Verwendung von Kryptographie stellt immer die Verteilung der Schlüssel dar: Wie gelangt dieser sicher in den Besitz der Person, welche die Nachricht entschlüsseln/verschlüsseln soll?

4.1. Externer Versand

Eine immer mögliche und sehr nützliche und verläßliche Möglichkeit ist es, den Schlüssel auf einem anderen (sicheren!) Weg zu übertragen. Beispiele hierfür wären, die Schlüssel bei einem persönlichen Treffen auszutauschen oder mit sicherer Post (Kurier, Diplomatenpost, gut versteckt) zu übertragen. Alle diese Übertragungsarten haben jedoch den Nachteil, daß sie einerseits nur für kleine Gruppen geeignet sind, die sich auch schon im Vornherein kennen müssen und andererseits immer eine relativ große Verzögerung und einen Medienbruch bedeuten.

Für den E-Commerce, wo viele (vorher dem Verkäufer unbekannte) Kunden eine sichere Datenübertragung wünschen bzw. die Kunden nicht von allen Geschäften vorher Schlüssel einfordern können, ist diese Art der Schlüsselverteilung ungeeignet.

4.2. Certificate Authorities (CA)

Zertifizierungsstellen stellen eine Verbindung zwischen einem Zertifikat und einer bestimmten Person her. Da Zertifikate nur für öffentliche Schlüssel sinnvoll sind, kann dieses Verfahren nur bei asymmetrischen Systemen eingesetzt werden. Da grundsätzlich jede Person eine solche Stelle einnehmen kann, indem sie Zertifikate von anderen Personen signiert, ist bei der Prüfung eines Zertifikates immer genau zu untersuchen, wer dieses bestätigt.

Ein Zertifikat selbst hat grundsätzlich keinerlei Bedeutung für die Bestätigung einer Identität. Erst die Verbindung des Zertifikates mit dem privaten Schlüssel einer Person, von der man annimmt, daß sie ihn nur zu bestimmten Zwecken verwendet, bedeutet eine Erhöhung der Sicherheit. Ein besonders wichtiger Punkt ist daher das Vertrauen der Benutzer in die Zertifizierungsstelle: Ein Zertifikat hat höchstens das gleiche Vertrauen wie die Zertifizierungsstelle (Kein Vertrauen in die Zertifizierungsstelle, weil diese z. B. unbekannt ist, bedeutet, daß deren Zertifikate wertlos sind!).

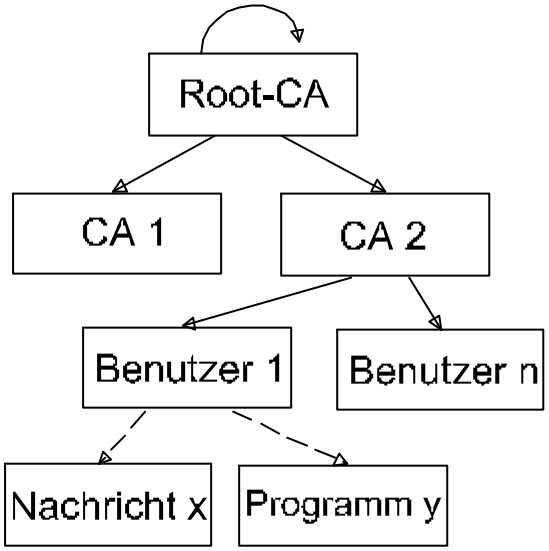
Für eine Zertifizierungsstelle ist es daher besonders wichtig, daß ihre Richtlinien (Policies = wann sie wem ein Zertifikat ausstellt) möglichst weit bekannt sind und daß die Endbenutzer ein hohes Vertrauen haben, daß diese Richtlinien auch tatsächlich eingehalten werden. Um dieses Vertrauen zu erhöhen, gibt es oft auch eine staatliche Aufsicht, welche die Einhaltung der selbst aufgestellten, bzw. vorgeschriebenen Richtlinien überprüft (Näheres im Kapitel zum Signaturgesetz). Dies insbesondere auch deshalb, da der Staat im elektronischen Rechtsverkehr (z. B. Einreichungen bei Ämtern) selbst auf die Akzeptierung von Zertifikaten fremder Anbieter angewiesen ist, will er nicht selbst eine große

Zertifizierungsstelle einrichten. Um dies zu ermöglichen, muß es zumindest eine Zertifikatskategorie geben, die staatlicherseits akzeptiert wird und daher staatlichen Mindestbedingungen entsprechen muß.

4.2.1. Darstellung einer Zertifizierungshierarchie

Im folgenden ist eine Zertifizierungshierarchie schematisch dargestellt. Außer auf der obersten Ebene können natürlich noch viele weitere Instanzen vorhanden sein, egal ob dies andere Zertifizierungsstellen oder Benutzer sind (Diese können auch gemischt auftreten: Eine CA kann sowohl andere Zertifizierungsstellen als auch Endbenutzer zertifizieren).

In der Praxis ist die Hierarchie jedoch ziemlich flach (wie im Bild dargestellt) und es erfolgt keine Mischung von Zertifizierungsobjekten: Es werden entweder CA's oder Benutzer aber nicht beide von einer Stelle zertifiziert.



Root-CA: Die oberste Zertifizierungsstelle muß sich selbst zertifizieren, da es keine übergeordnete Instanz mehr geben kann. Ihr Zertifikat ist daher mit dem privaten Schlüssel signiert, der zu dem im Zertifikat enthaltenen öffentlichen Schlüssel paßt ("self-signed certificate").

CA x: Die Zertifikate der einzelnen Zertifizierungsstellen sind mit dem privaten Schlüssel der obersten Zertifizierungsstelle signiert und enthalten den eigenen öffentlichen Schlüssel. Es können auch mehrere solcher CA's untereinander existieren, die Kette kann also so aussehen: Root-CA → CA Stufe 1 → CA Stufe 2 → CA Stufe 3 → Benutzer.

Benutzer x: Die Zertifikate der einzelnen Benutzer stellen das untere Ende der Zertifizierungshierarchie da. Natürlich können auch sie wiederum selbst Zertifikate ausstellen, doch wird diesen vermutlich nur ein geringer Wert beigemessen werden[9].

Nachricht x: Einzelne Nachrichten werden von den Benutzern signiert. Hier ist jedoch ein signifikanter Unterschied zu den oberen Verhältnissen zu beachten: Der Benutzer bestätigt hier nicht mehr die Identität der Nachricht (wie es CAs mit Benutzern tun), sondern stellt nur mehr eine besondere Verbindung mit sich selbst her: Die Nachricht ist keine eigene "Person", sondern wird lediglich dem Signator zugerechnet.

Programm x: Ähnliches ist bei Programmen der Fall: Auch sie erhalten keine eigentliche Persönlichkeit sondern sind nur "Erweiterungen" dessen, der sie signiert hat. Dies ist insbesondere deshalb wichtig zu beachten, da CA's bestimmte Eigenschaften der von ihnen zertifizierten Personen garantieren (z. B. den Namen), während Endbenutzer üblicherweise keine explizite Garantie

[9] Siehe dazu aber PGP: Dieses System baut darauf auf, daß jede Person die Schlüssel von anderen Personen bestätigt (also ihnen ein Zertifikat ausstellt). Vertraut man nun einer bestimmten Person, so wird man auch den von ihr zertifizierten Schlüsseln vertrauen. Dies ist natürlich für kleine oder geschlossene Gruppen gut geeignet, jedoch für offene Systeme wie etwa bei E-Commerce ungeeignet: Wie sollte ein Händler je die Schlüssel aller möglicher Kunden erhalten und ihnen auch vertrauen können? Näheres zu PGP unter http://www.pgp.com

abgeben. Aus der Tatsache der Zertifizierung läßt sich der Urheber zurückverfolgen, etwaige Garantien können jedoch in jedem Fall anders sein oder auch gar nicht existieren.

4.2.2. Liste von anerkannten CA's

Die folgenden Zertifizierungsstellen sind allgemein anerkannt. Insbesondere von denjenigen, die international tätig sind, werden die Root-Zertifikate in den am meisten verwendeten Browsern (Netscape Navigator und Microsoft Internet Explorer) standardmäßig als vertrauenswürdig inkludiert.

Bei praktisch allen CAs gibt es verschiedene Klassen von Zertifikaten: Einerseits solche für Server, andererseits Zertifikate für Einzelpersonen. Es werden auch meist mehrere Stufen angeboten: Von einfachsten Zertifikaten, die lediglich das Vorhandensein einer funktionierenden E-Mail Adresse bestätigen (zum Zeitpunkt der Ausstellung!) bis hin zu sehr vertrauenswürdigen Zertifikaten, die ausschließlich mit notariell beglaubigten Urkunden als Nachweis erhältlich sind. Entsprechend der Sicherheit bemißt sich auch die einmalige und die regelmäßig wiederkehrende Gebühr.

International:

1. Verisign: http://www.verisign.com
2. Thawte: http://www.thawte.com
3. GTE: http://www.gte.com/cybertrust/index.html

Österreich:

Telekom Control Kommission: http:/www.tkc.at/

1. a-sign (Datakom): http://a-sign.datakom.at (Elektronische Zertifikate und Smartcards)
2. e-sign (A-Trust): http://www.e-sign.at (Smartcards)
3. A-Cert (Arge Daten): https://a-cert.argedaten.at , http://www.a-cert.at (Zertifiziert nur PGP-Schlüssel; führt vorher eine Identitätsüberprüfung durch)
4. net.surance Security (EA Generali): http://www.generali.co.at/security (Elektronische Zertifikate)

5. Literatur

Pfaff, Oliver: Sicherheit in Netzen und Systemen. Skriptum zur Spezialvorlesung aus Systemwissenschaften SS 96. Universität Linz 1996

Schaumüller-Bichl, Ingrid: Datenschutz und Informationsrecht. Vorlesung SS 99. Universität Linz 1999

Knudsen, Jonathan: Java Cryptography. Cambridge: O'Reilly 1998

Public-Key Cryptography Standards: Specifications by RSA Laboratories. http://www.rsa.com/rsalabs/pubs/PKCS

Sterbenz, Andreas: Digitale Signaturen - Eine Einführung. Institut für Angewandte Informationsverarbeitung und Kommunikationstechnik, TU Graz. http://akitsicherheit.iaik.tu-graz.ac.at/DiGSig-prinzip.htm

Garfinkel, Simon, Spafford, Gene: Web Security & Commerce. Cambridge: O´Reilly 1997

Oaks, Scott: Java Security. Cambridge: O´Reilly 1998

The European Electronic Signature Standardization Initiative http://www.ict.etsi.org/eessi/EESSI-homepage.htm

II. Rechtliche Rahmenbedingungen elektronischer Signaturen

In diesem Kapitel wird das österreichische Signaturgesetz (SigG) besprochen, welches in Durchführung der Signatur-Richtlinie (SigRL) der Europäischen Union beschlossen wurde. Teilweise wird auch Bezug auf die Signatur-Verordnung (SigVO) genommen. Neben den verschiedenen einzelnen rechtlichen Aspekten wird einerseits besprochen, worauf sich diese Vorschriften genau beziehen, andererseits welche Rechtsfolgen sich aus sicheren Signaturen ergeben. Ein besonderes Augenmerk wird auch noch auf die Akkreditierung gelegt, mit der ein Anbieter von Zertifizierungsdiensten eine besonders überprüfte Qualität nachweisen kann. Weiters wird auch noch kurz der Electronic Signatures Act aus den USA besprochen.

Die rechtliche Anerkennung von Signaturen ist für E-Commerce besonders wichtig, da nur dann die sichere Beweisbarkeit vor Forderungen, beispielsweise aus Kaufverträgen, gegeben ist. Weiters ermöglichen sie die sichere Erkennung des Inhabers eines Geschäftes (über dessen Zertifikat), was dazu beiträgt, das Vertrauen der Konsumenten zu erhöhen und daher den elektronischen Handel fördert. Dies ist insbesondere ein Anliegen der europäischen Union, da auf diese Weise der freie Waren- und Dienstleistungsverkehr verstärkt wird. Aus diesem Grund wurde auch eine Signatur-Richtlinie geschaffen, sodaß in der gesamten Union einheitliche Regelungen bestehen und grenzüberschreitende Transaktionen problemlos möglich sind.

1. Einleitung

Elektronische Signaturen sollen es ermöglichen, daß Dokumente nicht nur in physischer Form sondern auch elektronisch unterschrieben (=signiert) werden können. Dadurch soll es möglich werden, sowohl die Beweisbarkeit von Rechtsgeschäften zu verbessern wie auch den Anwendungsbereich von E-Commerce zu vergrößern. Grundsätzlich kann nach der SigRL jedes Rechtsgeschäft, welches die einfache Schriftform (=Unterschrift) erfordert nun auch elektronisch abgeschlossen werden. Höherwertige Formen (Notarielle Beurkundung, Notariatsakt, gerichtliche Beglaubigung, ...) werden nicht erfaßt und können weiterhin nur durch physische Unterschrift (in Zusammenwirkung mit oder vor der entsprechenden Stelle) auf Papier erfolgen. Insbesondere ist kein “elektronischer Notariatsakt” vorgesehen, bei dem z. B. zusätzlich auch der Notar seine Signatur anbringen müßte.

Digitale Signaturen sind physischen sehr ähnlich, doch gibt es einen besonderen Unterschied: Elektronische Signaturen besitzen ein “Ablaufdatum”: Durch den technischen Fortschritt ist eine Signatur, die heute noch unfälschbar ist, in einigen Jahren wahrscheinlich ohne großen Aufwand zu brechen. Da Unterschriften mit rechtlicher Bedeutung aber oft viel länger gültig sein müssen (3-40 Jahre Verjährung), kann es notwendig sein, später eine erneute (Nach-)Signierung durchzuführen. Dies hat aber natürlich nur dann einen Sinn, wenn mit der Nachsignierung ein Zeitstempel (signiert von einem Zert.-Anbieter) verbunden ist, der den tatsächlichen Zeitpunkt der Nachsignierung bestätigt (Dieser muß innerhalb der Gültigkeitszeit des ursprünglichen Schlüssels liegen).

In geschlossenen Gruppen können weiterhin beliebige Signaturen und Verfahren verwendet werden. Diese werden aber rechtlich anerkannt, wenn sie die entsprechenden Eigenschaften besitzen, und haben dann auch Beweiswert vor Gericht (der jedoch an Hand der Ausgabe, der Sicherheitsvorkehrungen, etc. individuell zu beurteilen ist). Es kann daher im gegenseitigen Übereinkommen jederzeit eine andere Signatur vereinbart und verwendet werden.

Wichtig ist zu bemerken, daß durch das Signaturgesetz **nicht** die allgemeine Zulässigkeit elektronischer Kommunikation mit irgendjemandem, insbesondere nicht mit Behörden, festgelegt wird. In diesem Bereich ergeben sich keine Änderungen. Nur wenn el. Kommunikation erlaubt ist, dann ermöglichen Signaturen eine besondere Qualität der Eingaben und daher eventuell einen größeren Anwendungsbereich. Im Gegenzug ist es aber so, daß ohne Signaturen el. Kommunikation immer eine unsichere und daher seltene Ausnahme bleiben würde. Grundsätzlich wird davon ausgegangen, daß qualifizierte Signaturen (soweit die Kommunikation vorgesehen ist) auch für den Verkehr mit Behörden sicher genug sind. In besonders zu begründenden Fällen könnten jedoch auch besondere Vorkehrungen gefordert werden (so etwa nur Signaturen, die auf Chipkarten mit Fingerabdruck zur Autorisierung basieren und keine rein el. Signaturen; zur Zeit sind jedoch keine solchen Zusatzerfordernisse vorgesehen).

In der SigRL ist explizit festgelegt, daß die Aufnahme des Betriebes eines Zertifizierungsdiensteanbieters nicht von einer Genehmigung abhängig gemacht werden darf (d. h. kein Konzessionssystem). Werden die Vorschriften erfüllt, was im Laufe der Zeit und wiederholt überprüft wird, so kann sofort mit der Tätigkeit begonnen werden. Hierdurch wird nur eine Mindestqualität garantiert, die bei Betriebsbeginn noch nicht unbedingt gegeben sein muß. Um daher das Vertrauen der Konsumenten zu erhöhen, steht es einem Anbieter frei, sich einer besonderen Prüfung (→Akkreditierung) zu unterziehen, wodurch von staatlicher Seite aus eine besondere Qualität bestätigt wird. Dies darf jedoch nicht verpflichtend vorgesehen sein und auch zu keiner Wettbewerbsverzerrung führen.

1.1. Anforderungen an eine elektronische Unterschrift

Handschriftliche Unterschriften entsprechen in den meisten Fällen den folgenden Anforderungen. Eine äquivalente Unterschrift auf elektronischem Wege muß auch alle diese Punkte erfüllen (und ist daher in vielen Fällen sogar sicherer!):

- **Personenabhängigkeit:** Die Unterschrift ist eindeutig mit einer bestimmten Person verbunden, welcher der Inhalt deshalb zugerechnet wird.
- **Dokumentenabhängigkeit:** Die Unterschrift ist untrennbar mit dem Dokument verbunden und kann nicht auf ein anderes übertragen werden.
- **Überprüfbarkeit:** Die Unterschrift kann durch jeden überprüft werden, insbesondere ob sie von einer bestimmten Person stammt oder nicht.
- **Fälschungssicherheit:** Die Unterschrift kann nur durch eine einzige Person erzeugt werden. Fälschung sind daher nicht möglich, genauso wie der echte Unterzeichner nicht abstreiten kann, selbst unterschrieben zu haben.
- **Dokumentenechtheit:** Das Dokument kann nach der Unterschrift nicht mehr verändert werden. Die Unterschrift bildet einen Abschluß des Dokumentes.

2. Begriffsbestimmungen

In diesem Abschnitt werden die verwendeten Begriffe definiert, und zwar wie sie nach der SigRL und dem SigG (entspricht weitgehend der SigRL) zu verstehen sind. Diese Definitionen können sich von technischen unterscheiden und dienen der einheitlichen Auslegung der Vorschriften (Umfang: Was ist alles betroffen; Erläuterung: Welche Eigenschaften sind genau mit einem Begriff zu verbinden).

2.1. Elektronische Signatur

Eine Definition ist in § 2 Z 1 SigG und in Art 2 Z 1 SigRL enthalten.

Eine elektronische Signatur sind elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung, also der Feststellung der Identität des Signators dienen.

Die Beschränkung auf el. Daten hat den Grund, daß ein Ausdruck unter Umständen nicht mehr unverändert in die Originaldaten zurückgewandelt werden kann: Nicht-druckbare Zeichen, Zeilenumbrüche, Elemente der Codierung, redundante Elemente in den Daten die beim Ausdruck wegfallen, etc. Dies würde dazu führen, daß original-signierte Daten ohne Veränderung des Inhalts als unecht festgestellt werden könnten. Selbst wenn daher ein unverwechselbare Codierung vorliegt (z. B. Ausdruck als Byte-Codes), kann nicht mehr von einer el. Signatur gesprochen werden, (obwohl dann eine solche wiederhergestellt werden kann). Hier nicht besonders wichtig, wenn auch für den Umfang des Gesetzes sinnvoll; Bei sicheren Signaturen jedoch ein unbedingt notwendige Voraussetzung.

Die Beifügung entspricht einer externen Signierung (=Verlängerung des Textes), während die logische Verknüpfung auf eine Signierung ohne Verlängerung hinweist (interne Signatur), wobei die Daten mit dem privaten Teil des Schlüssels verschlüsselt werden (Nachteil: Entschlüsselung ist immer nötig, um den Text zu erhalten; bei externer Signierung kann die Prüfung auf Zweifelsfälle beschränkt werden).

Da die Daten der Identifizierung des Signators (Siehe 2.3) dienen, ist es mit einer (technischen) Signatur alleine nicht getan: Es muß auch ein Zertifikat beigefügt werden, aus dem dann die Identität feststellbar ist, wenn auch nicht unbedingt der Name (so bei Pseudonymen). Dieses Zertifikat ermöglicht auch die Prüfung der Signatur bzw. die Entschlüsselung des Textes. Alternativ würde dem Gesetztestext auch ein eindeutiger Hinweis entsprechen, welches Zertifikat zu verwenden ist. Dieser Vermerk muß jedoch allgemein verständlich sein, sodaß potentiell jeder dieses Zertifikat ausheben kann (Achtung: Qualifizierte Zertifikate sind nur mit Zustimmung des Inhabers öffentlich abrufbar: § 7 Abs 2 SigG; Dies ist kein Widerspruch: Gerichte und Behörden können diese Einschränkung umgehen und sind daher in der Lage, das notwendige Zertifikat festzustellen: § 22 Abs 2, 3).

Es muß sich hierbei nicht unbedingt um Zertifikate handeln, sondern auch eine rein textuelle Angabe des Namens des Signators erfüllt die Anforderungen an eine (einfache!) elektronische Signatur (natürlich mit geringer Sicherheit!).

2.2. Fortgeschrittene/Sichere elektronische Signatur

Eine Definition ist in § 2 Z 3 SigG und in Art 2 Z 2 SigRL enthalten.

Eine elektronische Signatur, die
a) ausschließlich dem Signator zugeordnet ist,
b) die Identifizierung des Signators ermöglicht,
c) mit Mitteln erstellt wird, die der Signator unter seiner alleinigen Kontrolle halten kann,
d) mit den Daten, auf die sie sich bezieht, so verknüpft ist, daß jede nachträgliche Veränderung der Daten festgestellt werden kann, sowie
e) auf einem qualifizierten Zertifikat beruht und unter Verwendung von technischen Komponenten und Verfahren, die den Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen entsprechen,
erstellt wird.

Eine sichere elektronische Signatur ist gegenüber einer normalen Signatur um einige Punkte erweitert. So wird vorausgesetzt, daß der Signator die Mittel zur Erstellung unter seiner alleinigen Kontrolle halten kann. Dies ist notwendig, da sonst keine Rechtsfolgen an eine sichere Signatur geknüpft werden könnten: Jeder könnte behaupten, daß er nicht in der Lage ist, eine Fälschung zu verhindern und daher die Signatur ihm nicht zugerechnet werden darf, da sie auch genauso von jemand anderem stammen könnte. Dies bedeutet jedoch keinen Ausschluß dieser Möglichkeit: Wurde das Mittel (z. B. die Smartcard und der PIN-Code) tatsächlich von jemand anderem verwendet, so kann darüber ein Beweis geführt und die Rechtswirkungen abgewendet werden.

Jegliche nachträgliche Veränderung der Daten muß erkennbar sein, um die Dokumentenechtheit zu gewährleisten. Dies erfolgt bei externen Signaturen dadurch, daß sich bei der Überprüfung ein anderer Hashwert ergibt, als der Signatur entspricht, während bei internen Signaturen die Entschlüsselung nicht mehr möglich ist.

Daß ein qualifiziertes Zertifikat (Siehe 2.5) verwendet werden muß, ist nur im SigG, aber nicht in der SigRL enthalten. Dies ist jedoch kein Widerspruch, da die Richtlinie sich nirgends auf eine fortgeschrittene Signatur alleine ohne qual. Zertifikat bezieht. Für sichere el. Signaturen kommen daher nur public-key-Systeme in Frage, wobei die Verknüpfung einer Person mit einem öffentlichen Schlüssel durch Zertifikate erfolgt.

2.3. Unterzeichner/Signator

Eine Definition ist in § 2 Z 2 SigG und in Art 2 Z 3 SigRL enthalten.

Eine natürliche Person, der Signaturerstellungsdaten und die entsprechenden Signaturprüfdaten zugeordnet sind und die entweder im eigenen oder im fremden Namen eine el. Signatur erstellt, oder ein Zertifizierungsdiensteanbieter, der Zertifikate für die Erbringung von Zertifizierungsdiensten verwendet.

Unter Signaturerstellungsdaten ist der private Schlüssel zu verstehen, während Signaturprüfdaten den öffentlichen Schlüssel bezeichnet. Diese Benennung wurde gewählt, um eine technik-indifferente Fassung zu ermöglichen, sodaß auch etwaige andere Systeme darunter subsumiert werden können.

Ein Signator kann sowohl im eigenen Namen, wie auch in anderem Namen handeln (Vollmacht, Auftrag, Geschäftsführung, ...), ebenso wie bei händischen Unterschriften.

Im Gegensatz zur SigRL spricht das SigG ausdrücklich nur von natürlichen Personen (Siehe dazu Kapitel 8: Widerspruch zwischen SigRL und SigG). Juristische Personen können daher keine Signatoren sein. Von diesem Grundsatz wird eine Ausnahme gemacht: Zertifizierungsdiensteanbieter können als Person im Zertifikat ihre Firma führen, besitzen also ein Zertifikat für ihre juristische Person. Dies hat den Grund, daß sonst bei jedem Wechsel des für die Ausstellung von Zertifikaten zuständigen Mitarbeiters alle von diesem signierten Zertifikate unter dem neuen Root-Zertifikat (das auf den neuen Mitarbeiter ausgestellt werden müßte) nicht mehr gültig wären. Dies würde dazu führen, daß alle Benutzer bei einem solchen Personenwechsel ein neues Zertifikat der Zertifizierungsstelle installieren müßten, um sowohl alte wie auch neue Zertifikate als gültig zu erkennen.

2.4. Zertifikat

Eine Definition ist in § 2 Z 8 SigG und in Art 2 Z 9 SigRL enthalten.

Eine elektronische Bescheinigung, mit der Signaturprüfdaten einer bestimmten Person zugeordnet werden und deren Identität bestätigt wird.

Diese Definition entspricht der technischen Definition: Es wird eine Verbindung zwischen einem öffentlichen Schlüssel und einer bestimmten Person hergestellt. Die Identifizierung der Person erfolgt über einen Namen, welcher der Person eindeutig zugeordnet sein muß (Pseudonyme sind aber möglich).

Im Gegensatz zu den Bestimmungen beim Signator können Zertifikate für alle Personen ausgestellt werden, insbesondere auch für juristische Personen. Diese können daher auch als Unterzeichner auftreten, lösen aber nicht die Rechtswirkungen aus, die mit dem Begriff eines "Signators" verbunden sind (da sie keine sichere elektronische Signatur erstellen können; dies ist nur Signatoren möglich).

2.5. Qualifiziertes Zertifikat

Eine Definition ist in § 2 Z 9 SigG iVm § 5, 7 SigG und in Art 2 Z 10 SigRL iVm Anhang I, II SigRL enthalten.

Ein Zertifikat, das zumindest die folgenden Angaben enthält und von einem Zertifizierungsdiensteanbieter für qualifizierte Zertifikate ausgestellt wird und mit der sicheren elektronischen Signatur des Zertifizierungsdiensteanbieters versehen ist:

a) den Hinweis darauf, daß es sich um ein qualifiziertes Zertifikat handelt,
b) den unverwechselbaren Namen des Zertifizierungsdiensteanbieters und den Staat seiner Niederlassung,
c) den Namen des Signators oder ein Pseudonym, das als solches bezeichnet sein muß,
d) gegebenenfalls auf Verlangen des Zertifikatswerbers Angaben über eine Vertretungsmacht, eine andere rechtlich erhebliche Eigenschaft des Signators oder weitere rechtlich erhebliche Angaben,
e) die dem Signator zugeordneten Signaturprüfdaten,
f) Beginn und Ende der Gültigkeit des Zertifikates,
g) die eindeutige Kennung des Zertifikates,
h) gegebenenfalls eine Einschränkung des Anwendungsbereichs des Zertifikats und
i) gegebenenfalls eine Begrenzung des Transaktionswerts, auf den das Zertifikat ausgestellt ist.

Dem Zertifikat muß einerseits zu entnehmen sein, daß es sich um ein qualifiziertes Zertifikat handelt (und nur bei diesen!), und von welchem Zertifizierungsdiensteanbieter es ausgestellt wurde. Dies soll es dem Empfänger ermöglichen, zu entscheiden, welches Vertrauen er in das Zertifikat setzt. Dazu ist eben eine genaue Identifikation des Ausstellers notwendig. Die Angabe des Staates der Niederlassung des Zert.-Anbieters hat den Sinn, eine Überprüfung zu ermöglichen, da in der EU kein Land ein vollständiges Verzeichnis für alle Länder führen muß (auch nicht durch eine EU-Instanz vorgesehen). In Österreich ist zwar eine zentrale Stelle vorgesehen, bei der alle Zertifikate der inländischen Zert.-Anbieter hinterlegt werden müssen, doch sind auch hier ausländische Zertifikate nur auf Antrag aufzunehmen (§ 13 Abs 3 SigG).

Auch Pseudonyme sind als Inhalt von Zertifikaten zulässig, diese dürfen jedoch weder anstößig sein, noch offensichtlich Verwechslungen mit Namen oder Kennzeichen hervorrufen (§ 8 Abs 4 SigG). Dies bedeutet jedoch keine vollständige Anonymität: dem Zertifizierungsdiensteanbieter muß immer die tatsächliche Identität bekannt sein, auch wenn diese nicht im Zertifikat aufscheint.

Angaben über eine Vertretungsmacht betreffen insbesondere die Befugnis zur Außenvertretung von Gesellschaften (Prokura, Handlungsvollmacht). Diese Eigenschaften müssen dem Zertifizierungsdiensteanbieter nachgewiesen werden, bevor ein entsprechendes Zertifikat ausgestellt werden darf.

Eine Einschränkung des Anwendungsbereichs ist möglich. Dies wäre beispielsweise eine Einschränkung auf bestimmte Rechtsgeschäfte, wie etwa Kaufverträge über bewegliche Sachen (Ausschluß von Kaufverträgen über Grundstücke, Darlehensgewährung, etc.). Optional kann auch eine Beschränkung des Transaktionswertes erfolgen, der mit dem Zertifikat möglich ist. Dies hat zwar keine Auswirkung auf die Zulässigkeit der Verwendung bei höherwertigen Verträgen, doch wird dadurch die Haftung des Zert.-Anbieters eingeschränkt. Dies eignet sich daher insbesondere für Personen, deren Ausgaben eingeschränkt werden sollen (Kinder, Unmündige, ...). Wer ein solches Zertifikat akzeptiert kann sich später nicht darauf berufen, daß er von der Beschränkung nichts wußte.

3. Widerruf von Zertifikaten

Manchmal ist es auch nötig, Zertifikate zu widerrufen, bevor ihr Geltungszeitraum abgelaufen ist. In aufsteigender Wahrscheinlichkeit sind dies:

- Es wurde zufällig ein gleiches Schlüsselpaar erzeugt,
- der private Schlüssel der Zertifizierungsinstanz wurde bekannt,
- der private Schlüssel des Signators wurde bekannt,
- der Signator ist tot oder nicht mehr im Besitz des privaten Schlüssels, oder
- die Angaben im Zertifikat sind nicht mehr gültig (Namensänderung, Änderung der Vertretungsmacht, etc.)

Es ist zwischen “Sperren” und “Widerrufen” von Zertifikaten zu unterscheiden: Eine Sperre bedeutet nur eine temporäre Ungültigkeit von maximal drei Werktagen, während ein Widerruf die Gültigkeit eines Zertifikates endgültig beseitigt. Eine Sperre erfolgt dann, wenn es Gründe gibt, das Zertifikat zu widerrufen, aber noch genauere Ermittlungen notwendig sind. Ab einer Sperre erfolgt daher die Akzeptierung des Zertifikates auf eigene Gefahr: Wird es widerrufen, so wirkt dies ab dem Zeitpunkt

der Sperre. Stellen sich die Gründe jedoch als falsch heraus, war das Zertifikat während der gesamten Zeit gültig und bleibt es auch weiterhin.

Sowohl Sperre als auch Widerruf müssen mit einem sicheren Zeitstempel versehen sein, um den genauen Zeitpunkt feststellen zu können (Rückwirkende Sperren und Widerrufe sind unzulässig). Um dies den Benutzern auch zur Kenntnis zu bringen, muß jeder Zertifizierungsdiensteanbieter entsprechende Verzeichnisse elektronisch und frei zugänglich (gratis und ohne Identifizierung des Abfragers!) führen. Unterbrechungen (z. B. Systemzeiten) sind nicht erlaubt; dafür ist ein Ersatzsystem vorzusehen. Jede länger als 30 Minuten dauernde Unterbechung ist als Störfall zu protokollieren. Ein Widerruf (auch schriftlich möglich) muß nach der SigVO während der Geschäftszeiten[10] spätestens 3 Stunden nach Bekanntwerden des Widerrufsgrundes erfolgen.

Für die Praxis ist wichtig, daß eine Prüfung des Widerrufs des Zertifikates immer dann notwendig ist, wenn der Transaktionswert eine bestimmte Höhe erreicht, die von der eigenen Risikobereitschaft abhängt. Da diese Verzeichnisse elektronisch und unentgeltlich zur Verfügung stehen müssen, ist aber auch eine grundsätzliche Prüfung in allen Fällen möglich. Damit jedoch später ein Beweis möglich ist, muß in einen Vertrag ein gesicherter Zeitstempel aufgenommen werden: Ansonsten ist es nicht möglich zu beweisen, wann die Signierung erfolgte. Ohne diesen Stempel kann nicht festgestellt werden, ob die Signatur noch vor dem Widerruf erfolgte (und damit gültig ist), oder danach (und somit ungültig), wobei auf eine Überprüfung des Widerrufs verzichtet wurde.

4. Zertifizierungsstellen (Certificate Authorities)

An Anbieter von Zertifizierungsdiensten werden hohe Anforderungen gestellt. Dies ist auch notwendig, da an eine Signatur unter Umständen erhebliche rechtliche und finanzielle Folgen geknüpft sind. Es ist daher ein Mißbrauch so weit wie nur irgend möglich auszuschließen. Dies soll auch das Vertrauen der Benutzer fördern, da ansonsten keine weite Verbreitung und die damit verbundenen Vorteile wie einfachere und schnellere Erledigung, mehr Möglichkeiten für Kontakte mit der Verwaltung etc. zu erwarten sind.

4.1. Datenschutz

Zertifikate haben nicht nur Vorteile: Durch ihre Verwendung wird jede Anonymität beseitigt. Einzige Möglichkeit dagegen ist, entweder keine Zertifikate zu verwenden (eher ungünstig) oder Zertifikate mit Pseudonym einzusetzen (aber zusätzliche Zertifikate kosten auch mehr Geld). Um die Gefahr des "gläsernen Menschen" nicht zu groß zu gestalten, werden an den Datenschutz in bezug auf Zertifikate besondere Anforderungen gestellt:

- Zertifizierungsdiensteanbieter dürfen nur diejenigen personenbezogenen Daten verwenden, die für die Durchführung der Dienste notwendig sind. Insbesondere dürfen keine Aufzeichnungen und Auswertungen von Anfragen bezüglich des etwaigen Widerrufs durchgeführt werden, da sich dadurch eine Datenspur ergibt und Gewohnheiten des Zertifikatsinhabers (besuchte Webseiten, bevorzugte Internet-Geschäfte, ...) festgestellt werden könnten.
- Alle notwendigen Daten für die Überprüfung der Ausstellung (inkl. Angaben über besondere Eigenschaften, etwa die Vertretungsmacht) dürfen ausschließlich beim Antragsteller erhoben werden (oder mit seiner **ausdrücklichen** Zustimmung bei Dritten). Werden keine Nachweise

[10] Mindestumfang: Werktage 9-17 Uhr, Samstag 9-12 Uhr

erbracht, so sind weitere Prüfungen verboten; in diesem Fall darf kein Zertifikat ausgestellt werden.

- Eine Verwendung der legal erhobenen Daten für andere Zwecke (z. B. Adressenverkauf) ist nur im Rahmen des Datenschutzgesetzes erlaubt (Nach der SigRL ist dies ausschließlich mit ausdrücklicher Zustimmung des Zertifikatsinhabers erlaubt).

4.2. Private Zertifizierungsstellen (CA)

Grundsätzlich kann jede Person eine Zertifizierungsstelle betreiben. Von einem Anbieter, der keine qualifizierten Zertifikate ausstellt, werden auch keine besonderen Maßnahmen verlangt: Er muß lediglich ein Sicherheits- und ein Zertifizierungskonzept an die Aufsichtsstelle melden und dieses dann einhalten. Dieses Konzept ist selbst in elektronischer Form[11] zu übersenden und muß signiert sein. Dafür gelten keine besonderen Vorschriften, es ist daher auch keine hohe Qualität notwendig und die Gebühren sind sehr niedrig (SigVO: 100 Euro; Zertifizierungsdiensteanbieter für qual. Zertifikate hingegen: 6.000 Euro). Weiters sind einfache Anbieter auch nicht verpflichtet, Verzeichnis- und Widerrufsdienste zu führen.

Werden Schlüsselpaare von der Zertifizierungsstelle erzeugt (und nicht vom Zertifikats-Antragsteller), so muß dafür ein physikalischer Zufallszahlengenerator verwendet werden und die erzeugten Schlüssel sind auf ihre Zufälligkeit und Eignung zu prüfen. Diese Generatoren sind auch längstem in einem Abstand von einem Monat auf ihre Qualität zu überprüfen[12]. Bei der Erzeugung werden ganz besondere Sicherheitsvorkehrungen verlangt: Jeder Zugriff muß überwacht, der Benutzer identifiziert und jede Verwendung registriert werden. Weiters muß es technisch unmöglich sein, den Schlüssel zwischen dem Zeitpunkt der Erstellung und der Übergabe an den Signator (z. B. Speicherung in der Chipkarte) zu duplizieren.

4.3. Anforderungen an Zertifizierungsdiensteanbieter für qual. Zertifikate

Gegenüber "normalen" Zertifizierungsdiensteanbietern bestehen für die Anbieter qualifizierter Zertifikate besondere Anforderungen. So müssen etwa die Personalien anhand eines gültigen amtlichen Lichtbildausweises überprüft werden. Eine Ablichtung davon ist mit dem Antrag zu archivieren (§ 11 Abs 1 SigVO). Bei einer Verlängerung eines bestehenden Zertifikates (während der Gültigkeitsdauer der Signatur!), ist es ausreichend, wenn ein solcher Antrag mit der (noch) gültigen Signatur versehen ist. In diesem Fall ist daher persönliches Erscheinen nicht mehr notwendig. Dies ist aber jedenfalls nur bis zum Ablauf der Gültigkeit des verwendeten Algorithmus oder der Schlüssellänge möglich. Gemäß § 8 Abs 2 SigG kann die Überprüfung der Identität des Antragstellers auch von einer beauftragten Stelle des Zert.-Anbieter erfolgen. Dieser Passus wurde vermutlich für die Post vorgesehen, sodaß eine Prüfung in jedem Postamt möglich ist. Doch könnten auch andere Firmen davon Gebrauch machen (z. B. Banken).

An besonderen Anforderungen sind in § 7 SigG für Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, unter anderem weiters festgelegt:

1. Er muß die erforderliche Zuverlässigkeit aufweisen
2. Ein schneller und sicherer Verzeichnisdienst, sowie ein sicherer und unverzüglicher Widerrufdienst muß gewährleistet werden.

---

[11] Erlaubte Formate nach SigVO: RTF, PDF, ASCII, Postscript

[12] Bei mangelhaftem Ergebnis sind alle Zertifikate, die seit dem letzten bestandenen Test erstellt wurden zu widerrufen!

3. Qualifizierte Zeitstempel müssen verwendet werden, inbesondere für die Zeitpunkte des Ausstellens und Widerrufens von qualifizierten Zertifikaten.
4. Zuverlässiges Personal mit den erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen muß beschäftigt werden.
5. Genügend Finanzmittel für Betrieb und insbesondere Haftung müssen vorhanden sein.
6. Alle maßgeblichen Umstände über ein qual. Zertifikat sind aufzuzeichnen, um später die Zertifizierung nachweisen zu können (insbesondere in Gerichtsverfahren).
7. Es müssen Vorkehrungen getroffen werden, daß Signaturerstellungsdaten weder vom Zertifizierungsdiensteanbieter noch von Dritten gespeichert oder kopiert werden können.
8. Technische Einrichtungen zur Erbringung von Signatur- und Zertifizierungsdiensten sind von anderen Funktionen und Anwendungen zu trennen (sowohl im Normalfall, wie auch bei Störfällen).
9. Die Einrichtungen sind gegen unbefugten Zutritt zu sichern.
10. Eingesetzte Systeme und Produkte sind genau zu dokumentieren. Zusätzliche Systemelemente (selbst wenn nicht sicherheitsrelevant!) oder sicherheitsrelevantes Abweichen von der Dokumentation gilt als Kompromittierung der Sicherheit, auch wenn diese Elemente nicht für die Erbringung der Signatur- oder Zertifizierungsdienste notwendig sind.

Grob gesagt, ist ein sicheres Rechenzentrum mit besonderer Hard- und Software, speziellen Vorkehrungen und ein gleichartiges Ersatzrechenzentrum gefordert. Aus diesem Grund kann davon ausgegangen werden, daß qualifizierte Zertifikate in Zukunft nur von relativ wenigen Anbietern ausgegeben werden.

4.4. Aufsichtsstelle

Im SigG ist als Aufsichtsstelle die Telekom-Control-Kommission vorgesehen[13]. Diese könnte zwar als eine oberste Zertifizierungsstelle (Root-CA) agieren, also die Zertifikate der einzelnen Zertifizierungsdiensteanbieter signieren, doch muß dies nicht so sein (und wird wahrscheinlich auch nicht erfolgen). Sie ist verantwortlich, daß jederzeit ein elektronisches und frei zugängliches Verzeichnis der gültigen, gesperrten und widerrufenen Zertifikate der österreichischen (auf Antrag unter Einschluß ausländischer) Zertifizierungsdiensteanbieter geführt wird. Diese Verzeichnisse sind jedoch (auch wenn sie keine Root-CA darstellt) mit ihrer eigenen el. Signatur zu versehen. Das zugehörige Zertifikat ist im Amtsblatt zur Wiener Zeitung zu veröffentlichen.

Da in der Telekom-Control-Kommission weder die notwendige detaillierte Fachkenntnis noch der personelle Umfang vorhanden ist, um diese Aufgaben zu erfüllen, kann sie sich einer oder mehrerer “Bestätigungsstellen” bedienen. Zusätzlich kann auch noch die Telekom-Control-GmbH mit der Durchführung der von der Kommission vorzunehmenden Aufsicht beauftragt werden. Sowohl Bestatätigungsstellen wie auch die Telekom-Control-GmbH werden in diesem Fall als beliehene Unternehmen tätig und üben daher behördliche Tätigkeiten aus. Bestätigungsstellen werden vom Bundeskanzler und dem Justizminister im Einvernehmen per Verordnung ernannt.

[13] Siehe dazu § 110 TKG; dies ist ein unabhängiges und weisungsfreies Kollegialorgan mit richterlichem Einschlag gem. Art 133 Z 4 B-VG, das in erster und oberster Instanz entscheidet. Die Anrufung des Verwaltungsgerichtshofes ist explizit gestattet.

Als Bestätigungsstelle ist ein Verein vorgesehen: **"Zentrum für sichere Informationstechnologie – Austria (A-SIT)".** Als Mitglieder fungieren derzeit das Bundesministerium für Finanzen, die Oesterreichische Nationalbank und die Technische Universität Graz. Dies ist einer der Kritikpunkte an dem Gesetz, da hiermit ein weiterer privater Verein mit behördlichen Aufgaben betraut wird. Als Alternative wurde beispielsweise der TÜV (Technischer Überwachungs-Verein) vorgeschlagen, der bereits jetzt umfangreiche Technikprüfungen durchführt.

5. Akkreditierung

Die Akkreditierung eines Zertifizierungsdiensteanbieters bringt keine zusätzlichen Qualitätsmerkmale mit sich: Es handelt sich nur um eine Bestätigung, daß die (ohnedies einzuhaltenden) Bestimmungen besonders überprüft wurden und ihnen entsprochen wird. Eine erfolgreiche Akkreditierung berechtigt dazu, das Bundeswappen zu führen und sich als "Akkreditierter Zertifizierungsdiensteanbieter" zu bezeichnen, was hauptsächlich für Werbezwecke geeignet ist. Für sie ist bei der Aufsichtsstelle ein eigenes Verzeichnis zu führen (bzw. werden sie wahrscheinlich im allgemeinen Verzeichnis besonders gekennzeichnet werden).

Daß ein Zertifikat von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellt wurde, ist in das Zertifikat aufzunehmen, sodaß ein Empfänger deswegen (eventuell) ein höheres Vertrauen darin setzen kann. In Zertifikate nicht akkreditierter Anbieter darf diese Bezeichnung nicht aufgenommen werden.

Nach der SigRL ist eine Beschränkung der Anzahl der akkreditierten Anbieter nicht zulässig, es hat daher jeder Anbieter die Möglichkeit, dies zu erreichen, wenn er qualifizierte Zertifikate ausstellt (Anbieter "einfacher" Zertifikate können sich nicht akkreditieren lassen). Da diese Überprüfung auch erst im Nachhinein erfolgen darf (Zulassungsbeschränkungen sind explizit verboten), muß ein Zertifizierungsdiensteanbieter zuerst den Betrieb aufnehmen und kann erst dann den Antrag auf Überprüfung und anschließende Akkreditierung stellen.

6. Rechtswirkungen elektronischer Signaturen

Aus der Verwendung einer elektronischen an Stelle eine handschriftlichen Unterschrift ergeben sich einige Rechtswirkungen: Erstens eine Gleichstellung der beiden und zweitens ein Verbot der Diskriminierung elektronischer Signaturen vor Gericht.

6.1. Erfüllung der (einfachen)Schriftform

Eine sichere elektronische Signatur (d. h. auf einem qualifizierten el. Zertifikat beruhend), erfüllt die Anforderung einer eigenhändigen Unterschrift und damit das Erfordernis der Schriftlichkeit gemäß § 886 ABGB[14]. Besondere Formen der Schriftlichkeit, wie etwa Notariatsakt, notarielle Beurkundung, etc. sind davon nicht betroffen und können daher nicht elektronisch erfolgen. Weiters ausgenommen von dieser Regelung sind Rechtsgeschäfte des Familien- und Erbrechts mit Schriftlichkeitserfordernis. Diese deshalb, da diese Bereiche besonders sensibel sind, häufig vermögensrechtliche Belange besonders schutzbedürftiger Personen betreffen und ein Beweis hier vielfach nur schwer erbracht werden kann. Ein Testament in elektronischer Form ist daher nicht wirksam. Ebenso ausgenommen

[14] Im Gegensatz zu Deutschland erfordert „Schriftlichkeit„ nicht das Vorliegen einer Urkunde, was in Österreich bei el. Daten auch nicht möglich ist (Siehe dazu Kapitel Strafrecht).

sind Bürgschaftserklärungen[15] durch Nicht-Kaufleute, für die gem. § 1346 Abs. 2 ABGB ebenfalls die Schriftform gefordert ist. Dies erfolgt, um die besondere Warnfunktion der eigenhändigen handschriftlichen Unterschrift nicht zu entwerten. (Siehe dazu auch E-Commerce RL Art. 9)

Die Nichteinhaltung zivilrechtlicher Schriftformerfordernisse führt zu einer Naturalobligation, welche zwar erfüllbar, aber nicht einklagbar ist. Dies hat zur Folge, daß die tatsächliche Leistung den Formmangel heilt. Eine Rückabwicklung formmangelhafter Verträge ist damit ausgeschlossen (§ 1432 ABGB). Gleiches gilt auch für Signaturen, die nicht allen Anforderungen für sichere Signaturen entsprechen: Ihre Verwendung führt zu einer Naturalobligation.

Wichtig ist festzustellen, daß hierdurch keine Formvorschriften berührt werden: Rechtsgeschäfte die Schriftlichkeit erfordern, benötigen diese weiterhin (sie kann nun eben auch anders erfüllt werden), während nicht formgebundene Geschäfte weiterhin formfrei bleiben.

6.2. Zulässigkeit als Beweismittel vor Gericht

Sichere elektronische Signaturen müssen vor Gericht als Beweismittel zugelassen werden. Dies ist in Österreich kein besonderes Problem, da fast keine Beweisverbote existieren. Nach derzeitigem Beweisrecht stellt ein elektronisches Dokument im visualisiertem Zustand ein Augenscheinsobjekt dar. Wird ein elektronisches Dokument ausgedruckt, so liegt eine – jedoch nicht unterschriebene – Urkunde vor.

Aber auch nicht-sichere Signaturen, also solche, die nicht auf einem qualifizierten Zertifikat beruhen, müssen vor Gericht beachtlich sein. Weder daß sie nur in elektronischer Form vorliegen, nicht auf einem qualifzierten Zertifikat beruhen, nicht von einem akkreditierten Zertifizierungsdiensteanbieter stammen oder nicht mit einer sicheren Signaturerstellungseinheit erzeugt wurden, darf einen grundsätzlichen Ausschluß bedeuten. Ihr Beweiswert ist jedoch weiterhin der freien Beweiswürdigung unterworfen und wird daher geringer sein, als bei sicheren Signaturen (darf jedoch nicht ohne Begründung ausgeschlossen werden). Dies gilt nur für Gerichte; Verwaltungsbehörden müssen solchen Signaturen daher keinen Wert beilegen[16].

6.3. Haftung der Zertifizierungsdiensteanbieter

Ein Zertifizierungsdiensteanbieter haftet gegenüber dritten Personen gemäß § 23 SigG, sofern diese auf das qualifizierte Zertifikat vertrauen, für folgende Punkte:

- Alle Angaben im Zertifikat sind im Zeitpunkt der Ausstellung richtig
- Der Empfänger ist im Ausstellungszeitpunkt im Besitz der Signaturerstellungsdaten
- Die Signaturerstellungsdaten und die Signaturprüfdaten entsprechen einander komplementär, wenn von ihm empfohlene oder bereitgestellte Produkte oder Verfahren verwendet werden
- Ein Widerruf erfolgt sofort nach Bekanntwerden der Erfüllung der Voraussetzungen dafür
- Die Widerrufsdienste sind verfügbar
- Die Einhaltung der Sicherheitsvorschriften in seinem Unternehmen

[15] Dies findet analoge Anwendung auf Garantie-Erklärungen. Ein Fax (selbst mit Original-Unterschrift) reicht nicht aus, da das „aus der Hand geben" ein wichtiges Element der Warnfunktion ist.

[16] Der europäische Begriff „Gericht" kann mehr umfassen als in der österreichischen Rechtssprache, z. B. auch die unabhängigen Verwaltungssenate (UVS).

Alle diese Punkte sind unverzichtbar, es kann daher nur nach Entstehen des Anspruchs darauf verzichtet werden. Ein Ausschluß oder Verzicht im vorhinein ist unwirksam.

Diese Haftung unterliegt jedoch auch Einschränkungen: Der Zert.-Anbieter haftet nicht, wenn er nachweist, daß ihn kein Verschulden trifft (inklusive Gehilfenhaftung, d. h. er haftet sehr wohl für die Handlungen seiner Angestellten). Darin enthalten ist auch eine Haftung bis hinab zu leichter Fahrlässigkeit. Weiters haftet er nicht, wenn das Zertifikat entgegen den darin enthaltenen Beschränkungen verwendet wird. In diesem Fall haftet er gar nicht, wenn das Zertifikat für ein nicht in den Einschränkungen enthaltenen Rechtsgeschäft verwendet wurde, bzw. nur in Höhe der Beschränkung des Transaktionswertes bei Überschreitung desselben.

Um Benutzern von Zertifikaten in einem Prozeß den Beweis zu erleichtern, genügt es, wenn er es **wahrscheinlich** macht, daß die Kompromittierung in der Sphäre des Zertifizierungsdiensteanbieters erfolgt ist. Dies bedeutet jedoch keine Umkehr der Beweislast, da der Zert.-Anbieter sein Haftung wieder dadurch abwenden kann, daß er gleichfalls wahrscheinlich macht, daß die Kompromittierung in der Sphäre des Signators liegt (außer Kraft setzen des Anscheinsbeweises des Signators).

Gemäß der Signaturverordnung ist ein Zertifizierungsdiensteanbieter verpflichtet, eine Haftpflichtversicherung in Höhe von 1.000.000 Euro pro Versicherungsfall abzuschließen, bevor er seine Tätigkeit aufnehmen darf.

6.4. Sonstige Rechtswirkungen

Der Unterschrift kommt auch im Beweisrecht eine wichtige Bedeutung zu. Für unterschriebene Privaturkunden gelangt nämlich eine besondere zivilprozessuale Beweisregel (§ 294 ZPO) zur Anwendung. Ist eine Unterschrift unbestritten oder nachgewiesenermaßen echt, so begründet eine Privaturkunde vollen Beweis dafür, daß der Inhalt vom Aussteller, also vom Namensträger der Unterschrift, stammt. Dabei handelt es sich um eine qualifizierte Echtheitsvermutung für den Erklärungsinhalt**,** die eine Zuordnung der in einer Urkunde enthaltenen Erklärung zum Unterzeichner bewirkt. Der Beweis des Gegenteils ist zulässig. Dies bedeutet, daß die Beweislast für die Unechtheit des Inhalts der Urkunde den Gegner des Beweisführers trifft. Die Umkehr der Beweislast bezieht sich aber nur auf den Urkundeninhalt**,** hinsichtlich der Echtheit der Unterschrift gelangen die normalen Beweislastregeln zur Anwendung.

Alle diese Rechtswirkungen treten jedoch nicht ein, wenn nachgewiesen wird, daß die Sicherheitsanforderungen durch den Zertifizierungsdiensteanbieter nicht eingehalten oder die Signaturerstellungsdaten kompromittiert wurden (also der private Schlüssel irgend jemand anderem bekannt wurde). Dies ist zwar unwahrscheinlich, doch können sich dadurch Personen von ihrer Haftung befreien. Sie müssen aber ihrer Sorgfaltspflicht bei der Geheimhaltung des Schlüssels entsprochen haben!

7. Rechte und Pflichten der Anwender

Der Signator hat die Pflicht, seine Signaturerstellungsdaten sicher zu verwahren und sie nicht weiterzugeben. Verliert er die Erstellungsdaten oder vermutet er, daß sie bekannt wurden, so hat er selbst den Widerruf des Zertifikates zu veranlassen. Ebenso ist er verpflichtet, das Zertifikat widerrufen zu lassen, wenn die Angaben im Zertifikat nicht mehr richtig sind. Er darf nur die vom Zert.-Anbieter bereitgestellten oder empfohlenen Hash- und Signatur-Verfahren verwenden.

Im Gegensatz dazu ist der Zertifizierungsdiensteanbieter verpflichtet, den Zertifikatswerber umfassend zu unterrichten. Dies muß vor der Vertragsschließung erfolgen und hat entweder schriftlich oder auf einem dauerhaften Datenträger zu erfolgen (d. h. CD-ROM, aber wohl nicht Disketten). Über folgendes ist der Zertifikatswerber (vor Vertragsschluß bzw. bei Ausstellung) aufzuklären:

- Inhalt des Sicherheits- und Zertifizierungskonzeptes des Zert.-Anbieters
- Bedingungen der Verwendung des Zertifikates (Anwendungsbereichs- oder Transaktionswerts-Beschränkungen)
- Erfolgte bzw. nicht erfolgte Akkreditierung des Zertifizierungsdiensteanbieters
- Besondere Streitbeilegungsverfahren
- Geeignete technische Komponenten und Verfahren für das verwendete Signaturverfahren bzw. auch sonstige Maßnahmen und Anforderungen für die Erzeugung und Prüfung sicherer Signaturen
- Mögliche Rechtswirkungen des verwendeten Signaturverfahrens
- Pflichten eines Signators
- Haftung von Zertifizierungsdiensteanbietern
- Wann und wie eine Nachsignierung zu erfolgen hat

8. Widerspruch zwischen SigRL und SigG

Zwischen der Signaturrichtlinie der EU und dem österreichischen Signaturgesetz besteht (inzwischen nur mehr ein) wichtiger Unterschied, welcher entweder durch eine spätere Novelle beseitigt werden muß, sollen nicht die üblichen Folgen derartiger Verstöße eintreten: Das österreichische SigG ist nicht anzuwenden und Benutzer können sich direkt auf die RL berufen.

8.1. Zertifikate nur für natürliche Personen

Die SigRL definiert in Art 2 Z 3 einen "Unterzeichner" allgemein als eine Person (streitig!), während das SigG in § 2 Z 2 einen Signator ausschließlich als natürliche Person (mit Ausnahme von Zertifizierungsdiensteanbietern) festlegt.

Der dahinterstehende Sinn ist, daß juristische Personen nie handlungsfähig sind, sondern zur Vornahme einer Unterschrift immer eines Organs oder Vertreters bedürfen, der in ihrem Auftrag handelt. Dies sollte hiermit nachgebildet werden, da insbesondere in Zertifikaten auch Angaben über die Vertretungsmacht enthalten sein können. Damit soll sichergestellt werden, daß eine Signatur immer einer natürlichen Person zugeordnet werden kann, welche den Signierungsvorgang auslöste. Bei juristischen Personen würde sonst oft der Fall eintreten, daß mehrere Person dazu berechtigt und in der Lage sind, eine Firmen-Signatur anzubringen, ohne daß sich später aus der Signatur feststellen ließe, welche der Personen dafür verantwortlich ist. Es ist jedoch zu beachten, daß dieses Ziel auch auf einem anderem Wege erreichbar wäre: Mit der Richtlinie vereinbar wäre es, z. B. eine Doppelsignatur durch die juristische Person und diejenige natürliche Person, welche die Signierung auslöste, zu verlangen.

8.2. Rechtsfolgen des Widerspruches

Vor Ablauf der Umsetzungsfrist der Richtlinie (18 Monate nach Inkrafttreten) ergeben sich daraus keine Rechtsfolgen: Es gilt das österreichische Signaturgesetz. Erst durch Fristablauf und mangelnde oder fehlerhafte Umsetzung können sich besondere Rechtsfolgen ergeben.

Eine Richtlinie ist dann direkt anwendbar, wenn

1. die Umsetzungsfrist abgelaufen ist,
2. die Richtlinie nicht oder nicht richtig in nationales Recht umgesetzt wurde, und
3. die Vorschrift hinreichend genau ist (klar und eindeutig; "self-executing")

Direkte Anwendbarkeit bedeutet, daß jeder sich unmittelbar auf die Richtlinie berufen kann und entgegenstehendes nationales Recht (auch Verfassungsrecht!) nicht mehr anzuwenden ist. Dabei ist jedoch eine sehr wichtige Einschränkung zu beachten: Diese direkte Anwendbarkeit kann nur dem Staat gegenüber geltend gemacht werden (ausschließlich vertikale Wirkung)[17]. Dies bedeutet in Bezug auf das SigG in der derzeitigen Form (ohne Novellierung) folgendes:

- Privatpersonen können sich gegenüber Privatperson nicht darauf berufen: Bei einer Behörde kann eine juristische Person dann als solche unterschreiben. Schließt sie jedoch eine normalen Vertrag mit einer anderen natürlichen oder juristischen Person, dann muß eine natürliche Person für sie signieren. Ebenso können Bürgschaftserklärungen weiterhin nicht elektronisch abgegeben werden (außer gegenüber dem Staat, etwa dem Finanzamt).
- Die Wirksamkeit wird sich daher in vielen Fällen darauf beschränken, daß keine Bestrafung wegen Mißachtung der Vorschriften möglich ist (etwa wenn ein Zertifizierungsdiensteanbieter einer juristischen Person ein qualifiziertes Zertifikat ausstellt).
- Entsteht unmittelbar durch die mangelnde Umsetzung ein Schaden, so kann die Republik Österreich auf Schadenersatz geklagt werden (hier wohl kein Anwendungsfall möglich).

9. Verwaltungsstrafbestimmungen

In § 26 des SigG sind einige Verwaltungsstrafbestimmungen festgelegt, welche aber nur dann zur Anwendung kommen, falls die Tat nicht strenger zu bestrafen ist oder in die Zuständigkeit der Gerichte fällt (Subsidiarität).

Für den Benutzer ist nur relevant, daß eine Verwaltungübertretung begeht, wer fremde Signaturerstellungsdaten ohne Wissen und Willen des Signators mißbräuchlich verwendet (Strafrahmen bis 56.000 ATS). Wichtig ist zu beachten, daß auch eine Benutzung ohne Wissen des Berechtigten straflos ist, wenn sie im Interesse des Berechtigten erfolgt (kein Mißbrauch). Fahrlässiger Mißbrauch ist nicht strafbar.

Für Zertifizierungsdiensteanbieter sind die Strafen zahlreicher und auch mit einem höheren Strafrahmen ausgestattet: Eine Verwaltungsübertretung mit Geldstrafe bis 112.000 ATS begeht, wer die Widerrufspflicht verletzt, die Dokumentationspflicht verletzt oder den Zertifikatswerber nicht

[17] Z. B. können direkt anwendbare Regelungen über einen Dienstvertrag von einem Vertragsbediensteten eines Ministeriums diesem gegenüber geltend gemacht werden. Ein Angestellter in einer Privatfirma mit einem identischen Vertrag und identischen Aufgaben kann diese gegenüber der Firma jedoch **nicht** geltend machen.

ordnungsgemäß unterrichtet. In allen diesen Fällen reicht schon die Verletzung in Beziehung auf einen einzelnen Benutzer aus. Mit bis zu 224.000 ATS zu bestrafen ist ein Zertifizierungsdiensteanbieter, wenn er verschiedene der Vorschriften verletzt, welche die Sicherheit in seinem Betrieb oder der Zertifikate gewährleisten sollen.

Weiters können Gegenstände, mit denen die strafbare Handlung begangen wurde für verfallen erklärt werden. Dies betrifft insbesondere Computer oder Geräte mit denen Schlüssel berechnet wurden oder die zur Duplizierung von Erstellungsdaten dienen.

10. Derzeitige Parameter nach der SigVO

Einige wichtige Elemente der Signaturverordnung, welche die möglichen kryptographischen Verfahren, die Schlüssellängen und die Dauer deren Zulässigkeit beschreiben, sind:

- Gültigkeitsdauer von Zertifikaten: Maximal 3 Jahre
- Gebühr der Aufsichtsstelle pro ausgestelltem und gültigen qual. Zertifikat pro Jahr: 2 Euro
- Signaturerstellungsdaten müssen mit einem physikalischen Zufallszahlengenerator erzeugt werden
- Signaturverfahren der Aufsichtsstelle: SHA-1 in Verbindung mit RSA und eventuell zusätzlich Signaturerstellungsdaten für sichere Zertifikate
- Signaturerstellungsdaten für sichere Zertifikate (ohne führende Nullen, privater Schlüssel):
    - RSA, zumindest 1023 Bit Schlüssellänge
    - DSA, zumindest 1023 Bit Schlüssellänge
    - DSA-Varianten[18] auf Basis elliptischer Kurven, zumindest 190 Bit
    - Zulässige Hashverfahren: RIPEMD-160, SHA-1
    - Geltung dieser Werte bis 31.12.2005
- Elektronische Signaturen **sollen** einem international anerkannten Standard entsprechen: z. B. PKCS#7
- Vorläufige **Empfehlung** für qualifizierte Zertifikate: X.509v3 certificate, X.509v2 CRL for use in the internet.
- Verzeichnis und Widerrufsdienste **sollen** einem international anerkannten Stadard entsprechen:
    - 1988 CCITT (ITU-T) X.500 / ISO IS9594
    - RFC 2587 Internet X.509 Public Key Infrastructure LDAPv2 Schema
    - RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile
    - RFC 2589 Lightweight Directory Access Protocol (LDAPv3) Extensions for Dynamic Directory Services

[18] ISO/IEC 14883-3 Annex A.2.2 (Agnew-Mullin-Vanstone analogue), IEEE-Standard P1363, Abschnitt 5.3.3 (Nyberg-Rueppel-version), IEEE-Standard P1363 [5], Abschnitt 5.3.4 (DSA version)

11. US Electronic Signatures Act

Bei diesem Bundesgesetz (USSigAct) handelt es sich um eine breitere Regelung als bei der EU Signatur-Richtlinie, da auch elektronische Urkunden und Inhaberpapiere geregelt werden. Es betrifft jedoch ausschließlich den Handelsverkehr zwischen einzelnen Bundesstaaten sowie mit dem Ausland.

11.1. Elektronische Urkunden und elektronische Signaturen

Eine elektronische Signatur wird als Geräusch, Symbol oder Prozess definiert, der zu einer elektronischen Urkunde hinzugefügt oder logisch mit ihr verknüpft ist und von einer Person mit der Absicht zu unterzeichnen erzeugt wurde. Es handelt sich daher um eine sehr breite Definition, die insbesondere vollkommen Technologie-unabhängig ist. Auch eine elektronische Urkunde wird sehr breit definiert: Ein Vertrag oder eine Urkunde, die mittels elektronischer Mittel erzeugt, generiert, gesendet, übermittelt, empfangen oder gespeichert wird (wobei "elektronisch" extrem breit ist; auch optische und elektromagnetische Technolgien oder solche mit ähnlichen Eigenschaften sind enthalten.).

Elektronische Signaturen oder Urkunden dürfen gegenüber handschriftlichen nicht diskriminiert werden (anaolg zur EU-RL), sowohl als Beweismittel als auch beim Abschluß von Verträgen. Demgegnüber besteht jedoch auch keine Verpflichtung, sich dieser Möglichkeiten zu bedienen, ausgenommen für Behörden, welche entsprechende Anträge apzeptieren müssen (außer für privatrechtliche Verträge mit ihnen).

Weiters sind detaillierte Regelungen enthalten, in welchen Fällen eine elektronische Mitteilungen an einen Konsumenten ausreichend und rechtsgültig ist (Vorherige Zustimmung, jederzeitge Widerrufsmöglichkeit, Information über Hard- und Software-Anforderungen, etc.).

Auch Aufbewahrungsvorschriften können durch elektronische Urkunden erfüllt werden. Die enthaltene Information ist exakt zu repräsentieren und hat für alle beteiligten Personen zugänglich zu sein. Dies ist wohl besonders im Hinblick auf die Aufbewahrungsvorschriften für Belege sinnvoll.

Von Bedeutung ist weiters, daß auch höherwertige Formen durch elektronische Signaturen erfüllt werden können: Notarielle Beurkundungen oder besondere Beglaubigungen können durch elektronische Urkunden ersetzt werden, wenn sie mit der elektronischen Signatur (und ev. zusätzlichen erforderlichen Daten) dessen versehen sind, der sie sonst handschriftlich beglaubigen müßte. Eine Notars-Unterschrift kann daher voll rechtsgültig durch die elektronische Signatur des Notars ersetzt werden (im Kontrast zur EU-RL!).

Eine besondere Vorschrift sieht noch vor, daß elektronische Agenten im Geschäftsverkehr nicht diskriminiert werden dürfen. Erfolgt daher ein Teil eines Vertragsabschlusses automatisch (Hard- / Software), so ist er dennoch rechtsgültig. Die elektronische Signatur eines Agenten ist daher rechtserheblich, auch wenn sie ohne direkte Beeinflussung oder ohne Aufsicht durch den Besitzer des Agenten erfolgte.

11.2. Ausnahmen

Einige Bereiche sind, analog zur EU-RL, vom Geltungsbereich ausgenommen:

- Rechtsgeschäfte des Erbrechts
- Adoption, Scheidung und andere familienrechtliche Angelegenheiten
- Alle handelsrechtlichen Angelegenheiten außer Kauf, Miete, schriftliche Verzeichtserklärungen und unterschriebene Kaufverträge (UCC 1 107, 1 206, Art. 2, 2A, [UCC])

Folgende Dokumente müssen auch weiterhin in physikalischer Form ausgestellt werden und sind einer el. Signatur nicht zugänglich:

- Gerichtsdokumente (Urteile, schriftliche Anträge, etc.)
- Beendigung von Infrastrukturleistungen (Wasser, Strom, Heizung, …)
- Bestimmte Mitteilungen (z. B. Kündigung) im Zusammenhang mit Mietverträgen oder Kreditverträgen für den Hauptwohnsitz einer Person
- Beendigung einer Kranken- oder Lebensversicherung sowie von Leistungen daraus
- Rückruf von Produkten oder Mitteilung über Produktfehler, welche die Gesundheit oder Sicherheit beeinträchtigen können
- Begleitdokumente für Gefahrenguttransporte

11.3. Inhaberpapiere

Unter Inhaberpapieren versteht man Urkunden, bei denen der Rechts-Besitz durch den Urkunden-Besitz bewiesen wird (d. h. Zahlung an den Überbringer, analog zu Geldscheinen). Dies ist natürlich bei elektronischer Abbildung ein besonderes Problem, da jederzeit absolut identische Kopien hergestellt werden können. Mittels Kryptographie kann jedoch ähnliches realisiert werden (doch ist dann keine Anonymität mehr gegeben).

Voraussetzung für die rechtliche Anerkennung sind:

- Eine einzige “Authoritative Kopie” muß existieren, welche einmalig und identifizierbar ist
- Sie muß den Besitzer bzw. auch den Nachbesitzer angeben
- Der Besitzer oder dessen Beauftragter muß die tatsächliche Kontrolle darüber besitzen
- Änderungen des Originals dürfen nur mit Zustimmung des Besitzers möglich sein (Unberechtigte Änderungen können erkannt werden)
- Jede Kopie (sowohl des Originals wie auch von Kopien) ist eindeutig als solche zu identifizieren

Weiters muß ein Besitzer nachweisen können, daß er Inhaber der authoritativen Kopie ist (d. h. Änderungen vornehmen und damit das Papier übertragen kann).

12. Literatur

12.1. Allgemein

Bertsch, Andreas, Pordesch, Ulrich: Zur Problematik von Prozeßlaufzeiten bei der Sperrung von Zertifikaten. DuD 23, 9/1999, 514ff

Brenn, Christoph: Signaturgesetz. Vortrag bei der ÖCG am 23.6.1999

Fischer, Peter; Köck, Heribert: Europarecht. 3. Auflage, Wien: Linde 1997

Kresbach, Georg: E-Commerce. Nationale und internationale Rechtsvorschriften zum Geschäftsverlehr über elektronische Medien. Wien: Linde 2000

Menzel, Thomas, Schweighofer, Erich: Das österreichische Signaturgesetz. Umsetzung des EG-Richtlinienvorschlages in einem österreichischen Signaturgesetz. DuD 23, 9/1999, 503ff

Sonntag, Michael: Electronic Signatures for Legal Persons. In: Hofer Susaane, Beneder Manfred (Ed.): IDIMT-2000. 8th Interdisciplinary Information Management Talks. Linz: Universitätsverlag Rudolf Trauner 2000, 233-256

Sterbenz, Andreas: Digitale Signaturen - Eine Einführung. Institut für Angewandte Informationsverarbeitung und Kommunikationstechnik, TU Graz. http://akitsicherheit.iaik.tu-graz.ac.at/DiGSig-prinzip.htm (16.3.2000)

A-SIT: http://www.a-sit.at

Telekom Control Kommission: http://www.signatur.tkc.at/de/index.html

12.2. Rechtsvorschriften

SigRL: Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. 19.1.2000 L 13/12

EComm-RL: Richtlinie 2000/31/EG des Europäischen Parlamentes und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr"), Abl. 17.7.2000 L 178/1

SigG: Bundesegesetz über elektronische Signaturen (Signaturgesetz - SigG), BgBL I 190/1999

SigVO: Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung - SigV) vom 2.2.2000, BGBl II 30/2000

Bericht des Justizausschusses über die Regierungsvorlage (1999 der Beilagen): Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG) JAB 2065 BlgNR 20. GP

USSigAct: Electronic Signatures in Global and National Commerce Act http://www.dud.de/dud/documents/usesignact0608.pdf (31.1.2001)

UCC: Uniform Commercial Code http://www.law.cornell.edu/ucc/ucc.table.html (31.1.2001)

III. Das Datenschutzgesetz 2000

E-Commerce bietet für den Kunden viele Vorteile, doch können sich auch erhebliche Nachteile daraus ergeben: Ist es praktisch unmöglich aus dem normalen Einkaufen einer Person in vielen verschiedenen Geschäften bestimmte Vorlieben oder Gewohnheiten herauszulesen und diese dann auszunützen, so ist dies bei E-Commerce problemlos möglich: Der Kunde kann beispielsweise auf der eigenen Webseite haargenau verfolgt werden, bestimmte Möglichkeiten (z. B. Werbebanner einer Firma auf verschiedenen Shops) erlauben es sogar, ein übergreifendes Profil über die Bewegungen eines Kunde im WWW herzustellen. Da diese Verfolgung aber durchaus auch von Nutzen für den Kunden sein kann (Siehe Kapitel Personalisierung), ist es nicht sinnvoll, sie einfach völlig zu verbieten. Es muß vielmehr darauf geachtet werden, welche Verwendung von personenbezogenen Daten akzeptabel ist und welche nicht. Solche Regeln sind in Datenschutzgesetzen festgelegt.

Da in derlei Gesetzen meist Regeln enthalten sind, in welche Länder welche Daten weitergegeben werden dürfen (um eine Umgehung durch Export und Verarbeitung im Ausland zu verhindern), wurde dazu eine Richtlinie der EU geschaffen (DSRL). Diese Richtlinie war bis zum 24.10.1998 umzusetzen (und Österreich daher bereits säumig!). Im Jahr 1999 wurde verstärkt an einer Novellierung des Datenschutzgesetzes aus dem Jahre 1978 gearbeitet, welches der Richtlinie nicht vollständig entsprach. Das neue Datenschutzgesetz wurde am 29.7.1999 dann als "Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG)" vom Nationalrat beschlossen. Daß der Datenschutz ein wichtiges Anliegen ist, kann auch daraus ersehen werden, daß die Generalversammlung der Vereinten Nationen bereits am 14.12.1990 eine "Richtlinie betreffend personenbezogener Daten in automatisierten Dateien" beschlossen hat, welche freilich nur an die Staaten adressiert ist und lediglich den Charakter einer Empfehlung hat (keine Rechtsverbindlichkeit). Ebenso ist der Datenschutz auch im Entwurf für eine "Charta der Grundrechte der Europäischen Union" enthalten (EUCharta[19]).

1. Einleitung

Das neue "Datenschutzgesetz 2000" setzt die Datenschutz-Richtlinie der EU um, geht aber in Teilbereichen noch darüber hinaus. So werden z. B. auch die Daten von juristischen Personen geschützt, ein Bereich der aus der DSRL ausgenommen ist. Dieser Schutz bestand schon im alten Datenschutzgesetz und wurde beibehalten. Ein Problem könnte sich dadurch ergeben, daß daher nur in den wenigsten Ländern ein angemessenes (und gleichwertiges) Datenschutzniveau besteht. Um dennoch eine Vereinfachung beim Export von Daten zu erreichen, wurden die Ausnahmen von der Genehmigungspflicht für die Daten natürlicher Personen auch auf solche von juristischen Personen

[19] Art. 8: Schutz personenbezogener Daten. (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten. (2) Diese Daten dürfen nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

erstreckt. Dahinter steht der Grundsatz, daß Daten natürlicher Personen jedenfalls schützenswerter sind als solche von juristischen. Wenn daher eine Übermittlung keine Geheimhaltungsinteressen von natürlichen Personen gefährdet, kann auch davon ausgegangen werden daß eine solche in Bezug auf juristische Personen ungefährlich ist.

Ein wichtiges Element ist das Datengeheimnis: Auftraggeber einer Verarbeitung, beauftragte Dienstleister oder Mitarbeiter von diesen müssen Daten, die ihnen ausschließlich auf Grund ihrer beruflichen Beschäftigung anvertraut oder bekannt wurden, geheim halten und dürfen nur aus einem rechtlich zulässigen Grund eine Übermittlung vornehmen. Diese Verschwiegenheitspflicht ist auch durch eine Verwaltungsstrafe abgesichert (siehe Abschnitt 7.2).

Hinzuweisen ist auch noch darauf, daß für publizistische Tätigkeit, private Verarbeitung sowie wissenschaftliche Forschung und Statistik Ausnahmen bzw. Erleichterungen gelten.

2. Begriffsbestimmungen

In diesem Abschnitt werden die Begriffe erläutert, wie sie im Datenschutzgesetz definiert sind. Am Beispiel “Daten”, welche hier ausschließlich als “personenbezogene Daten” verstanden werden, kann man ersehen, daß diese Definitionen nicht allgemeingültig sind, sondern ausschließlich für dieses Gesetz gelten. Die Definitionen sind im DSG in § 4 und in der DSRL in Art. 2 zu finden (teilweise andere Benennung und geringere Differenzierung).

2.1. Daten

Unter Daten werden Angaben über natürliche (z. B. Name, Geschlecht oder Internet-Surfgewohnheiten) und juristische Personen (z. B. Rechtsform, Eigentümer oder Ertragsdaten) (=Betroffene) verstanden, wenn die genaue Identität der Person, der sie zugeordnet sind, bestimmt oder zumindest bestimmbar ist. Es handelt sich daher ausschließlich um personenbezogene Daten. Informationen die anonymisiert wurden (d. h. von **niemandem** mehr einer Person zuordenbar sind), sind nicht geschützt.

Damit es sich um “personenbezogene” Daten handelt ist es nicht notwendig, daß der Verarbeiter die Identität der Person feststellen kann (z. B. wenn ihm nur die Sozialversicherungsnummer bekannt ist, aber nicht Name oder Wohnort), sondern daß dies zumindest für irgendeine andere Person möglich ist. Diese Unterscheidung in “direkt” und nur “indirekt” personenbezogene Daten besitzt jedoch eine große praktische Bedeutung, da im zweiten Fall die Vorschriften für die Verarbeitung durch einen bestimmten Verarbeiter (für den sie eben nur indirekt personenbezogen sind) erleichtert sind. Indirekt personenbezogen sind Daten dann, wenn es mit **legalen** Mitteln und **vertretbarem** Aufwand nicht möglich ist, sie einer einzigen bestimmten Person zuzuordnen. Die Möglichkeit der Verwendung illegaler Mittel (z. B. verbotene Verknüpfung mit anderen Daten) beseitigt daher nicht den nur indirekten Bezug.

Im Gegensatz zum alten Datenschutzgesetz ist nicht mehr gefordert, daß die Daten auf einem Datenträger festgehalten sein müssen. Auch bloß temporäre Daten und im Speicher befindliche Informationen sind geschützt.

2.2. Sensible Daten

Bei sensiblen Daten handelt es sich um besonders geschützte Informationen. Der Katalog ist abschließend in Art. 8 Abs 1 der DSRL angeführt. Er betrifft ausschließlich natürliche Personen (nicht juristische; siehe auch Inhalt!) und besteht aus:

- Rassische und ethnische Herkunft
- Politische Meinung
- Gewerkschaftszugehörigkeit
- Religiöse oder philosophische Überzeugung (daher auch z. B. Atheismus)
- Gesundheit
- Sexualleben

2.3. Auftraggeber

Bei einem Auftraggeber handelt es sich um eine natürliche oder juristische Person, Personengemeinschaften oder Organe (="Behörden") oder deren Geschäftsapparate (="Ämter") einer Gebietskörperschaft, welche die Entscheidung getroffen haben, Daten (=personenbezogene Daten) für einen bestimmten Zweck zu verarbeiten.

Auch wenn für die tatsächliche Verarbeitung Dienstleister herangezogen werden, verbleibt die Auftraggebereigenschaft beim Erteiler des Werkes bzw. der Dienstleistung. Nur wenn der Auftragnehmer trotz ausdrücklichen Verbotes oder aufgrund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln eine gesonderte Verarbeitung vornimmt, gilt er als Auftraggeber. Diese Zurechnungsregeln haben den Sinn, daß für den Betroffenen meist nur der Auftraggeber, aber nicht der Dienstleister ersichtlich ist. Weiters besitzt dieser meist auch das Verfügungsrecht über die Daten, sodaß daher nur er eine Löschung, Richtigstellung oder Auskunft durchführen darf.

2.4. Datei

Eine Datei ist eine strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich ist. Eine elektronische Verarbeitung ist nicht vorausgesetzt, daher erfüllen auch Zettelkarteien und Listen diesen Begriff. Daraus ergibt sich auch die Ausweitung des Datenschutzes auf manuell verarbeitete Daten, da auch diese nunmehr unter den Begriff "Datei" fallen können.

Diese Definition wurde direkt der Richtlinie entnommen und ist leider mißverständlich. Aus den Beratungen ergibt sich, daß eigentlich nicht strukturierte Sammlungen von Daten sondern Sammlungen von strukturierten Daten geschützt werden sollen. Eine Korrektur ist eventuell durch Auslegung möglich. Diese Unterscheidung ist deswegen notwendig, da beispielsweise eine Sammlung von Akten nicht als Datei gelten soll, obwohl sie zweifellos eine strukturierte Sammlung ist (nach der Aktenzahl), während eine Datenbank meist nicht strukturiert ist, sondern nur aus einer ungeordneten Menge (und damit nicht strukturiert; auch wenn schneller Zugriff oder Sortierungen über z. B. Indizes möglich sind!) von Datensätzen besteht, welche jedoch in sich stark strukturiert sind.

2.5. Datenanwendung

Hierbei handelt es sich um die Summe von logisch verbundenen Verwendungsschritten (siehe Abschnitt 2.6: Verwenden von Daten) zur Erreichung eines inhaltlich bestimmten Ergebnisses. Diese Verarbeitung muß zumindest teilweise automationsunterstützt (maschinell und programmgesteuert) erfolgen. Wichtig ist, daß die Datenverarbeitung eine logische Einheit ist, die aus unterschiedlichen

Handlungen wie Verarbeitung, Übermittlung, etc. in beliebiger Reihenfolge bestehen kann, aber einem übergeordneten Gesamtzweck dient.

Problematisch kann hierbei sein, daß keinerlei Struktur der Verarbeitung notwendig ist, daher fällt z. B. auch die Verwendung von Adressen zur Adressierung eines Briefes in einer Textverarbeitung unter die Verwendung: Auch die Textverarbeitung ist dann eine Datenanwendung. Um dies zu lösen ist beabsichtigt, eine Musteranwendung für Textverarbeitung (einschließlich Archivierung) zu schaffen.

2.6. Verwenden von Daten

Im Gegensatz zur DSRL wird im DSG eine feinere Differenzierung getroffen. Das "Verarbeiten" der Richtlinie wird in Österreich als Verwenden definiert und in Verarbeiten und Übermitteln unterschieden. Es betrifft jede Handhabungsart von Daten in einer Datenanwendung.

2.6.1. Verarbeiten von Daten

Das Verarbeiten von Daten ist umfassend definiert und besteht aus vielen einzelnen Elementen: Ermitteln, Überlassen, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Sperren, Löschen, Vernichten oder jeder anderer Art der Handhabung. Ausgenommen davon ist lediglich die Übermittlung. Jeder Einsatz von Daten ist daher entweder eine Übermittlung oder der Rest, welcher als Verarbeitung definiert wird. Das Übermitteln wurde aus der Verarbeitung ausgeschieden, da hierfür besondere Vorschriften gelten, die von denen für die Verarbeitung abweichen.

- Ermitteln von Daten: Beim Ermitteln von Daten handelt es sich um das Erheben von personenbezogenen Daten in der Absicht, sie in einer Datenanwendung zu verwenden. Entstehen solche Daten zufällig, so findet zwar keine Ermittlung statt, doch sind auch die daraus entstehenden Daten geschützt.
- Überlassen von Daten: Darunter wird die Weitergabe von Daten vom Auftraggeber an einen Dienstleister verstanden. Hierbei handelt es sich eben nicht um eine Übermittlung, sondern eine Verarbeitung, und ist daher diesen Vorschriften unterworfen. Der Unterschied zur Übermittlung liegt darin, daß beim Überlassen von Daten eine (natürliche oder juristische) Person beauftragt wird, eine bestimmte Verarbeitung mit beigestellten Daten durchzuführen, während eine Übermittlung keinem festen Zweck unterliegt, beziehungsweise dieser wechselt.

2.7. Übermitteln von Daten

Bei einer Datenübermittlung werden Daten einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder Dienstleister weitergeben. Daher ist eine Auskunft von Daten (an den davon Betroffenen) keine Übermittlung, ebensowenig wie die Weitergabe an andere zum Zwecke der gleichen Verarbeitung ($\Rightarrow$ Überlassung). Eine Übermittlung stellt jedoch auch die Veröffentlichung dar. Ein Personenwechsel ist nicht unbedingt notwendig, eine Übermittlung findet auch dann statt, wenn Daten bei einem Auftraggeber von einer Datenanwendung zu einer anderen transferiert werden.

Die Essenz liegt also in einem Wechsel des Verwendungszweckes der Daten, um sie für ein anderes Aufgabengebiet zu nutzen. Unter Aufgabengebiet kann eine Tätigkeitsfeld verstanden werden, das seinem Umfang und der Verkehrsauffassung nach geeignet ist, für sich allein einen eigenen Geschäftsbereich eines Auftraggebers zu bilden, also eine echt "andere" Datenanwendung darstellt.

In den Erläuterungen wird dieser im privaten Bereich mit dem Umfang einer Gewerbeberechtigung und im öffentlichen Bereich mit einem Kompetenztatbestand (Art. 10 bis 15 B-VG) verglichen.

2.8. Zustimmung

Eine Zustimmung zur Verwendung von Daten liegt dann vor, wenn der Betroffene gültig (d. h. ohne Irrtum), ohne Zwang und in Kenntnis der Sachlage in die konkrete Verwendung seiner Daten einwilligt. Eine Zustimmung kann daher immer nur auf eine bestimmte Verarbeitung bezogen sein, auch wenn diese relativ weit gefaßt werden kann. Eine generelle Ermächtigung ist jedoch keine Zustimmung.

Die Zustimmung muß bei "normalen" Daten nicht unbedingt ausdrücklich erfolgen, sondern kann auch konkludent erteilt werden. Im Gegensatz dazu muß sie bei sensiblen Daten sehr wohl ausdrücklich erfolgen. Schriftlichkeit ist nicht erforderlich, kann aber für den Nachweis der Erteilung notwendig sein.

3. Das Grundrecht auf Datenschutz

Ein Grundrecht ist ein verfassungsgesetzlich gewährleistetes subjektives Recht. Das Grundrecht auf Datenschutz bewirkt einen Anspruch auf Geheimhaltung personenbezogener Daten. Da es jedoch viele Situationen gibt, in denen dieses Recht ohne schwere Folgen nicht unbeschränkt bleiben darf, gibt es vielfältige Ausnahmen dazu.

3.1. Inhalt

Das Grundrecht auf Datenschutz bezieht sich nur auf personenbezogene Daten, d. h. Daten, die einer bestimmten Person eindeutig zuordenbar sind. Der Schutz besteht auch nur dann, wenn ein schutzwürdiges Interesse an der Geheimhaltung besteht. Dies setzt voraus, daß die Daten geheim gehalten werden können. Allgemein zugängliche Daten (z. B. Telefonbuch[20]) unterliegen daher nicht dem Datenschutz, solange sie im Augenblick der Verarbeitung auch tatsächlich noch frei zugänglich sind. Der Anspruch besteht nur für die Person selbst, es handelt sich daher um ein persönliches Recht.

3.1.1. Erhebungsschutz

Aus dem Anspruch auf Geheimhaltung personenbezogener Daten kann das Recht auf den Schutz vor Erhebung abgeleitet werden. Daten dürfen nur dann festgestellt werden, wenn dies den gesetzlichen Vorschriften entspricht oder eine Zustimmung des Betroffenen vorliegt.

3.1.2. Auskunft

Gemäß § 26 DSG hat jeder Betroffene das Recht darauf, vom Auftraggeber einer Datenverwendung innerhalb von 8 Wochen Auskunft darüber zu erhalten, ob, und wenn ja welche, Daten über ihn verarbeitet werden. Dies betrifft daher nur "echt" personenbezogene Daten; nur indirekt personenbezogene Daten unterliegen, da ja die Identität des Betroffenen für den Verarbeiter nicht feststellbar ist, nicht der Auskunftspflicht. Dazu muß ein schriftlicher Antrag gestellt werden und der Betroffene muß seine Identität in geeigneter Form nachweisen (zur Verhinderung der Datensammlung über andere Personen; es handelt sich um ein höchstpersönliches Recht). Folgende Informationen sind dem Betroffenen in allgemein verständlicher Form mitzuteilen:

[20] Siehe dazu jedoch den urheberrechtlichen Schutz!

- Welche Daten verarbeitet werden (Kategorie und Inhalt)
- Sofern verfügbar, woher die Daten stammen (Ermittlung, Übermittlung, ...)
- Wenn anwendbar, an welche Empfänger/ Empfängerkreise die Daten übermittelt wurden
- Der Zweck der Datenverwendung
- Die Rechtsgrundlagen für die Verwendung

Die Auskunft darf nicht erteilt werden, wenn dies zum Schutz des Betroffenen aus besonderen Gründen notwendig ist (z. B. medizinische Gründe oder Strafregisterauszug) oder soweit überwiegende berechtigte Interessen des Auftraggebers oder Dritter (z. B. öffentliche Interessen) dem entgegenstehen.

Um dem Auftraggeber keine zu große Belastung aufzubürden ist der Antragsteller verpflichtet, über Befragung in zumutbarem Ausmaß mitzuwirken. Dies bedeutet, daß er, sofern ihm bekannt, beispielsweise angeben muß, in welchem Zusammenhang seine Daten vermutlich gespeichert sind (Firma), oder daß er seine Kundennummer angeben muß, um die Suche nach seinen Daten zu erleichtern.

Betrifft die Anfrage den aktuellen Datenbestand einer Datenanwendung und hat der Betroffene im laufenden Jahr noch kein Auskunftsbegehren an den Auftragsteller zum selben Aufgabengebiet gestellt, so ist die Auskunft unentgeltlich zu erteilen. Andernfalls (mehrere Auskunftsbegehren oder z. B. Auskunft über einen Datenbestand zu einem bestimmten Zeitpunkt in der Vergangenheit) ist ein pauschalierter Kostenersatz von 260 ATS vorgesehen, vom dem nur wegen tatsächlich höherer Kosten abgewichen werden darf. Führt die Auskunft zu einer Richtigstellung oder wurden die Daten rechtswidrig verwendet, so ist der Kostenersatz rückzuerstatten. Der Auftraggeber hat in diesen Fällen den notwendigen Aufwand selbst zu tragen.

3.1.3. Richtigstellung oder Löschung

Jeder Auftraggeber ist verpflichtet, von sich aus Daten richtigzustellen bzw. zu löschen, sobald ihm die Unrichtigkeit oder die Unzulässigkeit der Verwendung bekannt wird. Darüber hinaus ist er dazu auch auf begründeten Antrag des Betroffenen verpflichtet. Diese Pflicht ist jedoch auf diejenigen Daten eingeschränkt, die einer Person zuordenbar sind (keine indirekt personenbezogenen Daten) und deren Unrichtigkeit oder Unvollständigkeit für den Zweck der Datenanwendung von Bedeutung ist. Wenn gesetzlich nicht anderes angeordnet ist, muß der Auftraggeber die Richtigkeit der Daten nachweisen. Dies gilt dann nicht, wenn die Daten ausschließlich durch Angaben des Betroffenen ermittelt wurden (und diesen Angaben entsprechen). Die Richtigstellung/Löschung hat innerhalb von 8 Wochen nach Einlangen des Antrags zu erfolgen. Gleichzeitig ist dem Betroffenen Mitteilung zu machen, wie mit seinem Begehren verfahren wurde.

Kann eine Richtigstellung oder Löschung aus technischen Gründen nicht erfolgen (oder läßt der Dokumentationszweck der Datenanwendung dies nicht zu wie etwa bei Krankengeschichten), so ist an Stelle einer Korrektur oder Löschung ein entsprechender Vermerk den Daten hinzuzufügen.

Kann die Korrektheit oder Unrichtigkeit von Daten nicht festgestellt werden und wird die Richtigkeit dieser Daten vom Betroffenen bestritten, so ist keine Richtigstellung durchzuführen, sondern ein Bestreitungsvermerk anzubringen. Dieser Vermerk darf nur mit Zustimmung des Betroffenen oder auf Grund einer Entscheidung eines Gerichtes oder der Datenschutzkommission gelöscht werden.

Wurden Daten richtiggestellt oder gelöscht und erfolgte in der Vergangenheit eine Übermittlung dieser Daten, so ist der Auftraggeber verpflichtet, die Empfänger der Daten von der Korrektur in geeigneter Weise zu unterrichten, um auch die dadurch entstandenen Kopien zu berichtigen. Dies ist dann nicht erforderlich, wenn die Empfänger nicht mehr feststellbar sind oder wenn dies einen unverhältnismäßigen Aufwand im Hinblick auf das berechtigte Interesse des Betroffenen an der Propagierung der Änderung bedeutet. Umso bedeutender daher das Interesse des Betroffenen an der Richtigstellung (oder Löschung) ist, desto extensiver müssen die Bemühungen des Auftraggebers ausfallen, um auch alle im Wege der Übermittlung abgeleiteten Daten zu korrigieren.

Auch in besonderen Konstellationen (siehe Abschnitt 3.3.5) besteht dieses Recht, doch ist dem Betroffenen dann nur mitzuteilen, daß eine Prüfung des Begehrens durchgeführt wurde (unabhängig davon, ob Daten verarbeitet werden, diese richtiggestellt oder gelöscht wurden oder dies nicht erfolgte).

3.1.4. Widerspruch

Das Widerspruchrecht stellt das Recht eines Betroffenen dar, die Verwendung seiner Daten (daher nicht bei nur indirekt personenbezogenen Daten) wegen Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen, die sich aus seiner besonderen Situation ergeben, zu untersagen (sofern die Verwendung nicht gesetzlich vorgesehen ist). In diesem Fall hat der Auftraggeber einer Verwendung die Daten innerhalb von 8 Wochen zu löschen und darf keine weiteren Übermittlungen dieser Daten durchführen. Dies unterscheidet sich vom Recht auf Löschung darin, daß die Daten zwar rechtmäßig verarbeitet werden, jedoch einzelne Betroffene aufgrund besonderer Umstände trotzdem die Verwendung ihrer Daten untersagen können. Ein typischer Anwendungsbereich ist die Speicherung von Adressen für Marketingzwecke.

Zusätzlich zu diesem allgemeinen Widerspruchsrecht existiert noch ein spezielles: Sollen Daten ohne gesetzliche Anordnung in eine öffentliche Datei aufgenommen werden, so kann jederzeit auch ohne Begründung Widerspruch eingelegt werden. Die Daten sind dann ebenfalls binnen 8 Wochen zu löschen. Dies stellt darauf ab, daß für die Öffentlichkeit nützliche Verzeichnisse (Bsp.: Telefonbuch, E-Mail-Adressen-Verzeichnis, Branchenverzeichnisse, etc.) meist nicht gesetzlich vorgesehen sind und in einer Durchschnittsbetrachtung auch keine Verletzung von schutzwürdigen Geheimhaltungsinteressen darstellen. Wenn jedoch Personen abweichend von der Durchschnittsbetrachtung für sich eine größere Gefahr annehmen, so soll dieses besondere Interesse einfach berücksichtigt werden können.

3.2. Umfang

Der Schutz erstreckt sich nicht nur auf automationsunterstützt verarbeitete Daten, sondern allgemein auf alle Daten, die ein Dateien abgelegt sind, also auch bei manueller Speicherung bzw. Zugänglichkeit. Dies ist eine bedeutende Ausweitung gegenüber den bisherigen Vorschriften, die lediglich automationsunterstützt verarbeitete Daten schützten. Dies hat den Sinn, eine Umgehung des Datenschutzes zu vermeiden, obwohl für Betroffene “gefährliche” Datensammlungen meist ohne Automationsunterstützung mangels Auswertungsmöglichkeiten nicht besonders gefährlich sind.

Der räumliche Umfang erstreckt sich auf alle Verwendungen von Daten, die im Inland stattfinden. Weiters ist österreichisches Recht auch dann anzuwenden, wenn ein österreichischer Auftraggeber eine Verwendung in einem anderen EU-Staat vornimmt, ohne dort eine Niederlassung zu besitzen. Spiegelbildlich ist in Österreich fremdes Recht anzuwenden, wenn ein Auftraggeber aus einem anderen EU-Staat Daten im Inland verwenden läßt, ohne hier eine Niederlassung zu besitzen. Zu

beachten ist, daß eine Niederlassung nur dann vorliegt, wenn die zu verarbeitenden Daten auch mit dieser Niederlassung in materiellem Zusammenhang stehen. Eine Verarbeitung materiell "fremder" Daten unterliegt daher trotz Vorhandensein einer Filiale oder Niederlassung nicht dem lokalen Recht. Für Auftraggeber mit Sitz außerhalb der EU gilt immer das Recht des Landes, in dem die Verwendung stattfindet.

3.3. Ausnahmen

Wie bereits erwähnt, gibt es viele Ausnahmen vom Grundrecht auf Datenschutz. Diese werden im Folgenden erläutert.

3.3.1. Zustimmung

Die wichtigste Ausnahme ist die Zustimmung des Betroffenen selbst. Er soll darüber entscheiden können, welche Daten über ihn für welche Zwecke verwendet werden. Ein Widerruf der Zustimmung ist jederzeit möglich und bewirkt die Unzulässigkeit einer weiteren Verwendung. Als Unterfall kann gesehen werden, daß eine Verwendung auch dann zulässig ist, wenn dies im lebenswichtigen Interesse des Betroffenen liegt, da dann eine Zustimmung meist gegeben werden würde. Ein Widerspruch dagegen ist jedoch nicht möglich.

3.3.2. Private Verarbeitung

Werden die Daten ausschließlich für persönliche oder familiäre Tätigkeiten verarbeitet, so sind sie vom Datenschutz ausgenommen (Keine Meldepflicht, kein Auskunftsrecht, etc.). Sie müssen jedoch entweder durch eine rechtmäßige Übermittlung erworben worden sein, oder dem Verarbeiter direkt vom Betroffenen mitgeteilt worden sein. Um eine Umgehung zu verhindern, ist eine Übermittlung aus diesem Bereich heraus, um die Daten für andere Zwecke zu verwenden, nur mit Zustimmung des Betroffenen erlaubt.

3.3.3. Gesetzesvorbehalt (gem. Art 8 Abs 2 MRK)

Das Grundrecht steht unter einem materiellen Gesetztesvorbehalt, daher kann der einfache Gesetzgeber weitere Ausnahmen schaffen, die jedoch besonderen Anforderungen genügen müssen:

1. Die Beschränkung muß der Wahrung der überwiegender und berechtigter Interessen des Betroffenen selbst oder anderer dienen. Diese müssen gegenüber dem Geheimhaltungsinteresse des Betroffenen überwiegen.
2. Sie muß durch Gesetz erfolgen (daher z. B. nicht durch Verordnung).
3. Der Eingriff muß im Bereich der Gründe des Art. 8 Abs. 2 EMRK[21] liegen.
4. Der Eingriff muß notwendig sein und in der gelindesten möglichen Art erfolgen (Notwendigkeit und Verhältnismäßigkeit).
5. Betrifft der Eingriff besonders schutzwürdige Daten (insbesondere sensible), so muß er zudem aus einem wichtigen öffentlichen Interesse erfolgen und angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen gewährleisten.

[21] Art. 8 EMRK lautet: „(1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs. (2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft *für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer* notwendig ist.

3.3.4. Wissenschaftliche Forschung und Statistik

Für Zwecke konkreter wissenschaftlicher Forschung und statistischer Untersuchung dürfen folgende Kategorien von Daten verwendet werden, sofern keine personenbezogenen Ergebnisse erzielt werden sollen:

1. Öffentlich zugängliche Daten
2. Daten, die vom Auftraggeber für andere Untersuchungen oder andere Zwecke zulässigerweise ermittelt wurden.
3. Daten, die für den Auftraggeber nur indirekt personenbezogen sind.

In diesen Fällen ist daher z. B. keine Zustimmung der Betroffenen zur Übermittlung oder Verarbeitung notwendig. Dies soll die Durchführung von statistischen Erhebungen erleichtern, die häufig mit einer großen Anzahl von Betroffenen verbunden ist und deren Verständigung daher großen Aufwand bedeuten würde.

Sind die Ergebnisse jedoch personenbezogen oder stellen sie kein konkretes Projekt dar (z. B. führen von Hilfs-Registern), so bestehen strenger Voraussetzungen für nicht-öffentliche Daten: Es müssen besondere gesetzliche Vorschriften bestehen (Verpflichtung zur Verarbeitung/Erstellung einer Statistik) oder die Zustimmung der Betroffenen muß vorliegen. Die Zustimmung kann unter bestimmten Voraussetzungen durch eine Genehmigung der Datenschutzkommission ersetzt werden, die für jede Verarbeitung eingeholt werden muß. Besondere Auflagen und Bedingungen können vorgeschrieben werden.

In jedem Fall ist der Personenbezug so früh wie möglich durch Verschlüsselung zu beseitigen bzw. die Daten zu anonymisieren, sobald die Verarbeitung dies zuläßt. Werden die Daten nicht mehr benötigt, so muß der Personenbezug vollständig beseitigt werden (oder die Daten gelöscht werden). Diese Ermächtigung betrifft nur wissenschaftliche Statistik, welche keiner besonderen gesetzlichen Regelung unterliegt (⇒ Bundesstatistikgesetz).

3.3.5. Sonstige

Von der Meldepflicht (§17 Abs 3), der Informationspflicht des Auftraggebers (§ 24 Abs. 4) und dem Auskunftsrecht (§ 26 Abs. 2) sind Daten bzw. Datenanwendungen ausgenommen, wenn sie für folgende Zwecke dienen und die Ausnahme zur Zweckverwirklichung auch notwendig ist:

- Schutz der verfassungsmäßigen Einrichtungen der Republik Österreich
- Sicherstellung der Einsatzbereitschaft des Bundesheeres
- Sicherstellung der Interessen der umfassenden Landesverteidigung
- Schutz wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union
- Vorbeugung, Verhinderung oder Verfolgung von Straftaten

Daten aus solchen Datenanwendungen dürfen auch ohne explizite Genehmigung ins Ausland übermittelt oder überlassen werden.

3.4. Drittwirkung

Das Grundrecht auf Datenschutz ist mit Drittwirkung ausgestattet. Dies bedeutet, daß es nicht nur gegenüber dem Staat in Hoheitsfunktion geltend gemacht werden kann, sondern auch zwischen den Bürgern untereinander zu beachten ist.[22]

4. Grundsätze für die Verwendung von Daten

In der Datenschutzkonvention des Europarates finden sich Grundsätze, die für die Erhebung, Verwendung und Qualität von Daten gelten sollen. Diese Grundsätze wurden auch in die DSRL aufgenommen und finden sich daher nun auch im DSG. Neben diesen allgemeinen Grundsätzen wird auch erläutert, welche Geheimhaltungsinteressen vom Gesetz als schutzwürdig eingestuft werden. Dies erfolgt in einer negativen Abgrenzung: Außer in den angeführten Fällen besteht immer ein Schutz. Da auch die Ermittlung von Daten eine Verwendung ist, werden hier auch die Informationspflichten des Auftraggebers erläutert, deren Einhaltung (neben anderen Verpflichtungen) eine Erhebung rechtmäßig macht.

4.1. Allgemeine Grundsätze

Daten dürfen nur nach Treu und Glauben und auf rechtmäßige Weise verwendet werden. Dies beinhaltet, daß der Betroffene über alle Aspekte der Verwendung informiert ist und er nicht irregeführt oder im Unklaren gelassen wird. Insbesondere ist er über seine Rechte und deren Durchsetzungsmöglichkeiten zu informieren bzw. darauf hinzuweisen. Dazu zählen besonders die Informationspflicht des Auftraggebers (4.5), das Auskunftsrecht (3.1.2) und die Anmeldung der Datenanwednung beim Datenverarbeitungsregister (6.1). Daß Daten nur auf rechtmäßige Weise verwendet werden dürfen weist darauf hin, daß eine ausreichende rechtliche Befugnis (Private) bzw. Zuständigkeit (Öffentlicher Bereich) notwendig ist.

Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden. Aus diesem Grundsatz ergibt sich das Prinzip der Zweckbeschränkung: Eine Übermittlung von Daten (= jeder Wechsel des Verwendungszweckes) ist nur erlaubt, wenn dafür eine gesetzliche Grundlage vorliegt, beispielsweise die Einwilligung des Betroffenen. Weiters enthält dieser Grundsatz den Erhebungsschutz: Personenbezogene Daten dürfen grundsätzlich nicht ermittelt werden, es sei denn, daß dafür eine explizite Erlaubnis (durch den Betroffenen oder durch Gesetz) vorliegt. Diese Genehmigung ist jeweils auf einen bestimmten konkreten Zweck beschränkt, worauf auch das grundsätzliche Übermittlungsverbot beruht.

Daten dürfen nur insoweit verwendet werden, als sie für den Zweck der Datenanwendung wesentlich sind und nicht darüber hinausgehen. Hier wird ein Minimalitätsprinzip festgelegt: Nur diejenigen Daten, die unbedingt für die Datenanwendung notwendig sind, dürfen verwendet werden. Dadurch soll vermieden werden, daß große Datensammlungen "vorsorglich" angelegt werden. Da der Zweck einer Datenanwendung jedoch (im Rahmen der Gesetze) frei festgelegt werden kann, hat dieser Grundsatz nur für den Fall der Zwecküberschreitung eine Bedeutung und ist auch dann stark

[22] Die Vereinsfreiheit ist z. B. nicht mit Drittwirkung ausgestattet: Eine staatliche Stelle darf daher u. A. niemandem verbieten, einem bestimmten Verein beizutreten. Unter Bürgern ist jedoch ohne weiteres ein Vertrag möglich, bei dem sich eine Person verpflichtet, einem bestimmten Verein nicht beizutreten. Wäre die Vereinsfreiheit mit Drittwirkung ausgestattet, wäre ein solcher Vertrag nicht erlaubt.

auslegungsbedürftig (Was ist für diesen bestimmten Zweck wirklich notwendig/noch nützlich/eigentlich unwichtig?).

Daten dürfen nur so verwendet werden, daß sie in Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig sind und, wenn nötig, auf dem neuesten Stand sind. Das Genauigkeitsprinzip legt fest, daß der Auftraggeber einer Datenanwendung dafür zu sorgen hat, daß die von ihm verwendeten Daten sachlich richtig sind. Es ist jedoch keine absolute, objektive Richtigkeit gefordert, sondern nur eine relative: Im Hinblick auf den Zweck der Verwendung der Daten dürfen keine Fehler enthalten sein[23]. Dieses bloß relative Korrektheitsgebot ist jedoch gefährlich: Bei einem Zweckwechsel wie einer Übermittlung wird in der Praxis kaum überprüft werden, ob die Daten auch noch für den neuen Zweck richtig (genug) sind. Dieser Grundsatz ist daher eher streng auszulegen. Aus den Erläuterungen geht auch hervor, daß in bestimmten Fällen daraus eine Pflicht des Auftraggebers abgeleitet werden kann, Daten regelmäßig auf ihre Aktualität zu überprüfen und gegebenenfalls von sich aus richtigzustellen, um ungerechtfertigte Nachteile für Betroffene zu vermeiden.

Daten dürfen nur so lange in personenbezogener Form aufbewahrt werden, als dies für die Zweck, für die sie ermittelt wurden erforderlich ist, oder gesetzliche Vorschriften dies erfordern. Daten müssen daher gelöscht oder anonymisiert werden, sobald sie nicht mehr benötigt werden. Da jedoch vielfach gesetzliche Vorschriften bestehen, daß Daten zu archivieren sind und bei vielen Anwendungen der Zweck auch auf sehr lange oder unbestimmte Zeit angelegt ist (z. B. Kundendatei: Die Person könnte ev. in vielen Jahren wieder Kunde sein, daher müssen die Daten theoretisch bis zum Tode des Betroffenen aufbewahrt werden), ist auch dieser Grundsatz nur bei Verletzungen von Bedeutung. Zu beachten ist, daß auf den Zweck der Ermittlung abgestellt wird: Ein späterer Zweckwechsel, um Daten länger aufbewahren zu können, ist daher eine Übermittlung und muß rechtmäßig erfolgen.

Neben diesen allgemeinen Richtlinien bestehen für die Zulässigkeit einer konkreten Datenanwendung zwei Voraussetzungen: Der Auftraggeber muß die notwendige Berechtigung für die konkrete Verarbeitung besitzen und die schutzwürdigen Interessen der Betroffenen müssen berücksichtigt werden. Sollen Daten nicht nur verarbeitet sondern auch übermittelt werden, so müssen sie nicht nur aus einer zulässigen Datenanwendung stammen, sondern der Empfänger muß dem Übermittelnden seine rechtliche Befugnis im Hinblick auf den Zweck der Übermittlung glaubhaft machen (Nachweis der Berechtigung des Empfängers zur Verarbeitung der zu empfangenden Daten). Weiters darf weder der Zweck noch der Inhalt der Übermittlung die schützwürdigen Geheimhaltungsinteressen der Betroffenen verletzen.

Allgemein ist bei jeder Datenverwendung besondere Rücksicht auf das Grundrecht zu nehmen und die Verhältnismäßigkeit des Eingriffs gegenüber den Interessen des Betroffenen zu beachten. Nur der gelindest mögliche Eingriff ist erlaubt und dieser muß nach den oben angeführten Grundsätzen erfolgen.

4.2. Verhaltensregeln

In Art. 27 der DSRL ist vorgesehen, daß "Berufsverbände und andere Vereinigungen, die andere Kategorien von für die Verarbeitung Verantwortlichen vertreten" Verhaltensregeln ausarbeiten. Diese

[23] Beispiel: Ein Verzeichnis „säumiger Kunden„ darf nur Kunden enthalten, bei denen die Zahlungsfrist auch tatsächlich abgelaufen ist, jedoch keine Kunden, die zwar sehr spät, aber noch innerhalb der Frist bezahlen. Anders bei einem Verzeichnis von „Kunden, die eventuell säumig werden„.

sollen näher präzisieren, was eine Datenverwendung nach Treu und Glauben im Einzelnen für den privaten Bereich darstellt. Diese Regeln sind vor der Veröffentlichung dem Bundeskanzler vorzulegen, der ihre Gesetzmäßigkeit zu prüfen hat. Diese für das österreichische Recht äußerst ungewöhnliche Einrichtung wurde durch die genaue Vorgabe in der DSRL notwendig. Obwohl der Bundeskanzler eine Vorab-Prüfung vorzunehmen hat, ist damit keine Aussage über die Gesetzmäßigkeit der Verhaltensregeln verbunden; er gibt lediglich ein Gutachten darüber ab. Weiters haben die Verhaltensregeln keinen verbindlichen Charakter, sondern dienen lediglich als Richtschnur und können nur für die Auslegung herangezogen werden. Bedeutung könnten sie unter Umständen bei Schadenersatzprozessen erhalten, da ein Verstoß dagegen wohl eine zumindest fahrlässige Verletzung von Sorgfaltspflichten darstellt. Eine Prüfung durch die Datenschutzkommission kommt nicht in Frage, da diese die Regeln in einem Beschwerdefall konkret zu prüfen hat und daher keine Vorabkontrolle vornehmen kann, ohne die Unvoreingenommenheit zu verlieren (Recht auf “fair trial” ach EMRK).

4.3. Schutzwürdige Geheimhaltungsinteressen

Sollen nicht-sensible Daten verwendet werden, so werden schutzwürdige Geheimhaltungsinteressen in den folgenden Fällen nicht verletzt:

1. Es besteht eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten. Dies gilt insbesondere für den öffentlichen Bereich, hat aber auch für den privaten Geltung.
2. Der Betroffene hat der Verwendung seiner Daten zugestimmt. Ein Widerruf ist jedoch jederzeit möglich und bewirkt die Unzulässigkeit der weiteren Verwendung der Daten.
3. Lebenswichtige Interessen des Betroffenen erfordern die Verwendung.
4. Überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten erfordern die Verwendung.

4.3.1. Beispiele, in denen keinesfalls eine Verletzung vorliegt

Die folgende Aufzählung bringt nur Beispiele, in denen keine Verletzung vorliegt. Dies sind Unterfälle des letzten Punktes der allgemeinen Regelung (Überwiegende berechtigte Interessen). Sie besitzen jedoch trotzdem eine gewisse Sonderstellung, da hier niemals eine Verletzung vorliegen kann. In anderen Fällen, die unter die Generalklausel fallen, kann es jedoch in Einzelfällen dennoch dazu kommen, daß trotz grundsätzlicher Erlaubtheit eine Verletzung vorliegt. Bei den nachfolgend angeführten Beispielen erübrigt sich daher die Prüfung im Einzelfall, sondern es ist lediglich zu untersuchen, ob einer der Fälle vorliegt, um die Gesetzmäßigkeit zu bejahen. Schutzwürdige Geheimhaltungsinteressen sind dann jedenfalls nicht verletzt, wenn die Verwendung der Daten

1. für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist. Dies soll vermeiden, daß für jeden Fall, daß eine Datenverwendung notwendig ist, eine explizite gesetzliche Ermächtigung/Auftrag notwendig ist. Es muß sich jedoch um eine wesentliche Voraussetzung handeln und daher anders gar nicht oder nur mit großen Schwierigkeiten möglich sein, die Aufgabe zu erfüllen. Eine bloße Erleichterung der Tätigkeit ist nicht ausreichend.
2. für einen Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung zur Amtshilfe (Art. 22 B-VG) erfolgt. Die Zulässigkeit ist nach der ersuchenden Stelle zu beurteilen und die Amtsverschwiegenheit zu beachten.

3. zur Wahrung lebenswichtiger Interessen eines Dritten erforderlich ist. Gegenüber einem Menschenleben (auch dem eines Dritten) tritt der Datenschutz zurück. Beispiel dafür wäre etwa das Durchsuchen einer (fremden) Datenbank nach einem geeigneten Blutspender.
4. zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenem erforderlich ist. Es wird fingiert, daß mit dem Vertragsabschluß auch gleichzeitig die Einwilligung gegeben wurde. Dies soll vermeiden, daß sonst gültige Verträge durch Weglassen einer expliziten Regelung und folgenden Einspruch beseitigt werden können. Die Verwendung muß jedoch "erforderlich" sein, d. h. die Erfüllung ansonsten nicht möglich sein.
5. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden. Einem Auftraggeber, der Daten rechtmäßig in seinem Besitz hat, kann nicht zugemutet werden, diese nicht verwenden zu dürfen, um ihm zustehende Rechte zu verfolgen. Dasselbe wird auch für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor Gerichten anzunehmen sein, da kein gewichtiger Grund ersichtlich ist, der dies ausschließen würde (problematisch könnte aber die Öffentlichkeit einer Verhandlung sein).
6. ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand hat.

4.3.2. Geheimhaltungsinteresse bei Daten ohne Geheimhaltungsanspruch

Besteht kein Geheimhaltungsanspruch, so wird in zwei Fällen doch das Widerspruchsrecht eingeräumt. Diese Daten dürfen daher solange legal verwendet werden, wie der Betroffene keinen Widerspruch nach dem DSG eingelegt hat. Es handelt sich hierbei um zulässigerweise veröffentlichte Daten und nur indirekt personenbezogene Daten. Bei veröffentlichten Daten ist jedoch genau zu prüfen, ob auch tatsächlich alle Daten veröffentlicht wurden, oder ob Teile davon aus den öffentlichen Daten durch eine Auswertung gewonnen wurden (und selbst aber nicht veröffentlicht wurden). In diesem Fall handelt es sich um "normale" Daten, und es sind die oben angeführten Interessen zu prüfen. Der Grund hierfür ist, daß auch aus einer Auswertung von veröffentlichten Daten in besonderen Fällen neue Daten gewonnen werden könnten, die schutzwürdige Geheimhaltungsinteressen berühren. Daher soll auch hier die Möglichkeit bestehen, die Verwendung zu untersagen.

4.3.3. Sonderregelungen für Straftaten

Zwischen den "normalen" und den sensiblen Daten (siehe nächster Abschnitt) existiert noch eine Zwischenkategorie: Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen, Daten über den Verdacht der Begehung von Straftaten und über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen. Werden diese Daten verwendet, so liegt nur dann keine Verletzung des Datenschutzes vor, wenn:

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung solcher Daten besteht. Beispiel: Strafregister.
2. die Verwendung der Daten für Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung zur Wahrung einer ihnen gesetzlich übertragenen Aufgabe ist.
3. sich sonst die Zulässigkeit der Verwendung dieser Daten aus gesetzlichen Sorgfaltspflichten oder sonstigen, die schutzwürdigen Geheimhaltungsinteressen des Betroffenen überwiegenden berechtigten Interessen des Auftraggebers ergibt und die Art und Weise, in der die Datenanwendung vorgenommen wird, die Wahrung der Interessen der Betroffenen gewährleistet.

Gegenüber normalen Daten ist hier lediglich eine besondere Sorgfalt bei der Verwendung gefordert, um die Interessen der Betroffenen zu wahren (besondere Aufmerksamkeit hinsichtlich des Schutzes vor unbefugtem Zugriff). Alle anderen Punkte entsprechen den allgemeinen Regeln, wobei aber die Interessen des Auftraggebers im Verhältnis stärker sein müssen, um die Verwendung strafrechtsbezogener Daten zu rechtfertigen.

4.4. Schutzwürdige Geheimhaltungsinteressen bei sensiblen Daten

Im Gegensatz zu den nichtsensiblen Daten handelt es sich hier um eine abschließende Aufzählung: Andere Eingriffe sind auf jeden Fall verboten (Siehe dazu auch Art. 8 Abs. 2 und 3 der DSRL). Schutzwürdige Geheimhaltungsinteressen werden daher nur dann nicht verletzt, wenn

1. der Betroffene die Daten offenkundig selbst öffentlich gemacht hat.. Wer Daten selbst veröffentlicht, gibt damit zu erkennen, daß er kein besonderes Interesse an der Geheimhaltung hat. Dies gilt um so mehr, je stärker die Daten sonst geschützt wären.
2. die Daten in nur indirekt personenbezogener Form verwendet werden. Da kein Rückschluß auf eine bestimmte Person möglich ist, besteht kein Geheimhaltungsinteresse.
3. sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen. Dieser gesetzliche Eingriff muß dem Vorbehalt des Grundrechts entsprechen und ist dann erlaubt.
4. die Verwendung durch Auftraggeber des öffentlichen Bereichs in Erfüllung ihrer Verpflichtung zur Amtshilfe geschieht. (Siehe oben: 4.3.1)
5. Daten verwendet werden, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben. (Siehe oben: 4.3.1)
6. der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat. Dieser Punkt ist ähnlich dem Tatbestand bei nichtsensiblen Daten mit dem einen Unterschied, daß hier eine ausdrückliche Zustimmung erforderlich ist: konkludente Einwilligung reicht nicht.
7. die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann. Auch dies ist ähnlich den allgemeinen Ausnahmen, doch darf eine Verarbeitung nur dann erfolgen, wenn keine Zustimmung mehr eingeholt werden konnte, ohne den Zweck der Verwendung zu vereiteln. Ist die Einholung möglich, so ist eine Verwendung ausschließlich auf Grund der Zustimmung erlaubt (und sonst verboten; Selbstbestimmungsrecht[24]).
8. die Verwendung der Daten zur Wahrung lebenswichtiger Interessen eines anderen notwendig ist. (Siehe oben: 4.3.1) Hier ist keine Zustimmung notwendig, wie wenn es um den Betroffenen selbst geht.
9. die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden. (Siehe oben: 4.3.1; wohl auch für Gerichte)
10. die Daten für private Zwecke verwendet werden (oder wissenschaftliche Forschung oder Statistik oder zur Benachrichtigung des Betroffenen). Private Verwendung ist vom Datenschutz nicht erfaßt und für die anderen Bereiche bestehen Sonderregelungen.

[24] Ähnlich bei ärztlicher Behandlung: Jede Person kann jede Behandlung an sich selbst ablehnen; ist dies nicht erfolgt oder keine Äußerung mehr möglich, so hat der Arzt sie durchzuführen.

11. die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechtes Rechnung zu tragen, und sie nach besonderen Rechtsvorschriften zulässig ist. Dies betrifft insbesondere Gesundheitsdaten und die Gewerkschaftszugehörigkeit.

12. die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist, und die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen.

13. nicht auf Gewinn gerichtete Vereinigungen mit politischem, philosophischem, religiösem oder gewerkschaftlichem Tätigkeitszweck Daten, die Rückschlüsse auf die politische Meinung oder weltanschauliche Überzeugung natürlicher Personen zulassen, im Rahmen ihrer erlaubten Tätigkeit verarbeiten und es sich hierbei um Daten von Mitgliedern, Förderern oder sonstigen Personen handelt, die regelmäßig ihr Interesse für den Tätigkeitszweck der Vereinigung bekundet haben; diese Daten dürfen, sofern sich aus gesetzlichen Vorschriften nichts anderes ergibt, nur mit Zustimmung der Betroffenen an Dritte weitergegeben werden. Hiermit wird es Vereinen erlaubt, die Daten ihrer Mitglieder oder eng mit ihnen verbundener Personen zu verarbeiten. Da viele Organisationen (Vereine, Parteien, etc.) existieren, die Zwecke im Bereich der sensiblen Daten verfolgen (z. B. politische Parteien), lassen sich aus ihren Mitgliederlisten naturgemäß sensible Daten extrahieren. Diese Daten dürfen daher nur mit Zustimmung des Betroffenen weitergegeben werden, obwohl die Vereinigung selbst sie verwalten und verwenden darf.

4.5. Informationspflicht des Auftraggebers

Bei einer Ermittlung von Daten muß der Betroffene in geeigneter Weise über bestimmte Sachverhalte informiert werden (§ 24 DSG), falls er diese nicht bereits hat[25]: Der Zweck der Datenanwendung, für den die Daten ermittelt werden und Name und Adresse des Auftraggebers.

In vielen Fällen werden noch zusätzliche Informationen weiterzugeben sein, um eine Verwendung nach Treu und Glauben zu gewährleisten. Dies ist insbesondere dann der Fall, wenn der Betroffene ein Widerspruchsrecht (siehe 3.1.4) gegen die Verarbeitung oder Übermittlung besitzt oder es für den Betroffenen aus den Umständen nicht klar ist, ob er zur Beantwortung der Fragen rechtlich verpflichtet ist.

Keine Informationspflicht besteht für Datenanwendungen gemäß § 17 Abs. 2 und 3. Hierbei handelt es sich um die nicht meldepflichtigen Datenanwendungen (insbesondere Standardanwendungen nach VO des Bundeskanzlers) und u. A. um Datenanwendungen zum Schutz der Republik Österreich, der Einsatzbereitschaft des Bundesheeres und der Vorbeugung oder Verfolgung von Straftaten.

5. Datenverkehr mit dem Ausland

Der Datenverkehr (Übermittlung oder Überlassung; bloße Durchfuhr ist nicht betroffen) mit dem Ausland ist in zwei große Gruppen zu unterteilen: EU-Staaten und sonstige Staaten. Befindet sich der Empfänger einer Übermittlung in der Europäischen Union, so gibt es keinerlei Beschränkungen für den privaten Bereich. Bei Auftraggebern des öffentlichen Bereichs betrifft dies jedoch nur

[25] So geht z. B. bei einer schriftlichen Bestellung auf einem Formular eines Versenders schon aus dem Umständen hervor, daß Name, Adresse, etc. zum Zweck der Bestellungsbearbeitung verarbeitet werden. Ebenso ist der Auftraggeber bekannt (= der Versender). Hier ist keine gesonderte Information notwendig. Anders jedoch, wenn die Daten auch an andere Firmen weitergegeben werden sollen!

Angelegenheiten, die dem Recht der EU unterliegen. Nicht enthalten ist daher insbesondere die Datenverwendung im Bereich der "dritten Säule" (Zusammenarbeit im Bereich Justiz und Inneres).

Im Verkehr mit Drittstaaten ist grundsätzlich eine Genehmigung der Datenschutzkommission notwendig, die auch Auflagen und Bedingungen festsetzen kann. Alle Übermittlungen haben als Voraussetzung, daß die Datenanwendung im Inland rechtmäßig erfolgt. In folgenden Ausnahmefällen ist keine Genehmigung (und auch keine Anzeige) notwendig:

1. Wenn im Empfängerstaat ein angemessener Datenschutz besteht. Welche Staaten dies sind, wird per Verordnung des Bundeskanzlers bzw. Feststellung der Kommission bestimmt. Ob ein entsprechendes Niveau vorliegt, ist an der Ausgestaltung der allgemeinen Grundsätze (siehe 4.1) und der Möglichkeit ihrer Durchsetzung zu messen.
2. Wenn die Daten im Inland zulässigerweise veröffentlicht wurden. Dies muß nicht durch den Betroffenen selbst, aber jedenfalls rechtmäßig erfolgt sein.
3. Falls die Daten für den Empfänger nur indirekt personenbezogen sind. Wenn sie daher für den Absender direkt personenbezogen sind, der Empfänger jedoch nur einen Teil der Daten erhält oder ihm andere Daten fehlen, sodaß sie für ihn nur mehr indirekt personenbezogen sind, besteht durch die Übermittlung keine Gefahr.
4. Ist die Übermittlung oder Überlassung von Daten ins Ausland in innerstaatlichen Gesetzen mit direkter Anwendbarkeit vorgeschrieben, so ist dies erlaubt.
5. Die Übermittlung erfolgt für private oder publizistische Zwecke.
6. Wenn der Betroffene ohne jeden Zweifel seine Zustimmung zur Übermittlung oder Überlassung seiner Daten ins Ausland gegeben hat. Es ist zu beachten, daß eine Zustimmung zur Verwendung und Übermittlung normalerweise eine Übermittlung in Drittstaaten nicht miteinschließt. Dafür ist aus den Umständen (konkludent) oder explizit eine gesonderte Zustimmung notwendig.
7. Wenn die Erfüllung eines vom Auftraggebers mit dem Betroffenen oder mit einem Dritten eindeutig im Interesse des Betroffenen abgeschlossenen Vertrages nicht anders als durch Übermittlung der Daten ins Ausland erfüllt werden kann. Beachtenswert ist, daß lediglich im Interesse des Betroffenen abgeschlossene Verträge nicht grundsätzlich zu einer Verwendung der Daten ermächtigen. In diesem Fall muß daher im Inland ein zusätzlicher Grund vorliegen, bevor dann eine Übermittlung ins Ausland jedoch zulässig ist.
8. Erlaubt ist die erforderliche Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor ausländischen Behörden, wenn die Daten rechtmäßig ermittelt wurden.
9. Wenn die Übermittlung oder Überlassung in einer Standardverordnung oder Musterverordnung (siehe dazu auch 6.1.1) ausdrücklich angeführt ist. In den meisten Fällen wird es sich bei diesen Verordnungen lediglich um Verwendungen der Daten handeln, doch falls eine Übermittlung explizit angeführt ist, so ist dies erlaubt.
10. Datenverkehr mit österreichischen Dienststellen im Ausland ist nicht betroffen. Die Daten verlassen zwar physikalisch und rechtlich Österreich, befinden sich jedoch praktisch immer noch in österreichischem Einflußbereich. Eine Gefährdung ist daher nicht zu befürchten, da auch diese Dienststellen das DSG anzuwenden haben.
11. Übermittlungen oder Überlassungen aus Datenanwendungen, die gemäß § 17 Abs. 3 DSG von der Meldepflicht ausgenommen sind, können in Drittstaaten erfolgen. Hierbei handelt es sich um Datenanwendungen zum Schutz des Staates, der Landesverteidigung, wirtschaftlicher und

außenpolitischer Interessen Österreichs und der EU und der Vorbeugung, Verhinderung und Verfolgung von Straftaten (Siehe auch 3.3.5).

12. Wenn zwar eine Genehmigung zur Übermittlung notwendig ist, diese aber nicht ohne Gefährdung der Interessen eingeholt werden kann, so ist aus den folgenden Zwecken die Übermittlung erlaubt, muß aber der Datenschutzkommission angezeigt werden: Zur Wahrung eines wichtigen öffentlichen Interesses oder zur Wahrung eines lebenswichtigen Interesses einer Person. Die Kontrolle wird daher von einer Vorab- zu einer Nachkontrolle umgewandelt.

6. Rechtsdurchsetzung

Um Betroffenen die Möglichkeit zu geben herauszufinden, welche Datenarten von wem über sie verarbeitet werden, wird bei der Datenschutzkommission ein Register aller Datenanwendungen geführt. Nichtsdestotrotz heißt es "Datenverarbeitungsregister" und nicht "Datenanwendungsregister", was historische Gründe hat. Weiters wird in diesem Abschnitt noch die Beschwerde bei der Datenschutzkommission (und der Unterschied zur Anregung einer Kontrolle durch diese) sowie die Schadenersatzregelungen erläutert.

6.1. Anmeldung beim Datenverarbeitungsregister

Die Datenschutzkommission hat ein Register aller Datenanwendungen in Österreich zu führen. Grundsätzlich sind alle Datenanwendungen dort anzumelden (inklusive späteren Änderungen oder Ergänzungen), sofern nicht eine der Ausnahmen vorliegt. Dieses Register ist öffentlich zugänglich. Ist man Betroffener und stehen dem keine schutzwürdigen Interessen des Auftraggebers oder Dritter entgegen, so ist auch Einsicht in den Registrierungsakt (einschließlich der darin enthaltenen Bescheide) möglich. Eine Meldung muß auch automationsunterstützt möglich sein. Leider ist nicht vorgesehen, daß auch die Einsicht auf diese Weise möglich sein muß (sie könnte aber so erfolgen). Nicht meldepflichtig sind Datenanwendungen, die:

- ausschließlich veröffentlichte Daten enthalten. Da an ihnen kein Geheimhaltungsanspruch besteht, ist eine besondere Publizität der Anwendung entbehrlich. Wie in Abschnitt 4.3.2 ist jedoch streng zu prüfen, ob ausschließlich veröffentlichte Daten enthalten sind, oder auch Auswertungen aus veröffentlichten Daten, wodurch sich eine Meldepflicht ergibt.
- von Gesetz wegen eingerichtete öffentliche Register zum Inhalt haben. Die Einsicht muß nicht völlig öffentlich sein, zumindest bei Nachweis eines berechtigten Interesses muß jedoch Einsicht möglich sein. Ansonsten besteht Meldepflicht. Diese ist hier entbehrlich, da die Existenz als bekannt vorauszusetzen ist und jeder sich durch eine Abfrage von dem genauen Umfang der verwendeten Daten informieren kann (enthält auch gleichzeitig das Auskunftsrecht).
- nur indirekt personenbezogene Daten enthalten. Da kein Geheimhaltungsanspruch besteht, ist auch eine Meldung nicht sinnvoll. Das Datenverarbeitungsregister soll insbesondere das Auskunftsrecht ermöglichen: Dieses ist bei nur indirekt personenbezogenen Daten von den Tatsachen her schon ausgeschlossen, daher ist eine Registrierung nicht notwendig.
- einer Standardanwendung entsprechen (siehe Abschnitt unten).

Laut § 17 Abs. 3 DSG sind folgende Datenanwendungen von der Meldepflicht ausgenommen, wenn dies zur Verwirklichung des Zweckes der Datenanwendung notwendig ist: Schutz der Republik Österreich, der Einsatzbereitschaft des Bundesheeres und der Vorbeugung und Verfolgung von Straftaten (siehe dazu näher sonstige Ausnahmen Abschnitt 3.3.5)

6.1.1. Inhalt der Meldung

Eine Meldung an die Datenschutzkommission hat die folgenden Elemente zu enthalten:

1. Name und Anschrift des Auftraggebers. Besitzt der Auftraggeber bereits eine Registernummer, so ist auch diese zur Vereinfachung anzuführen.
2. Nachweis der gesetzlichen Zuständigkeit (öffentlicher Bereich) oder der rechtlichen Befugnis (privater Bereich; meist Gewerbeberechtigung) für die erlaubte Ausübung der Tätigkeit des Auftraggebers. Dies ist nur notwendig, wenn eine solche Befugnis notwendig ist.
3. Der Zweck der zu registrierenden Datenanwendung und ihre Rechtsgrundlagen, soweit diese sich nicht bereits aus der Befugnis ergeben. Der Zweck ist genau anzugeben, da er für die Beurteilung, ob eine Übermittlung vorliegt oder nicht, ausschlaggebend ist.
4. Die Kreise der von der Datenanwendung Betroffenen.
5. Die verarbeiteten Datenarten. Typischerweise die einzelnen Felder, die in der geplanten Datenbank enthalten sein sollen mit ihrer genauen Inhaltsbeschreibung.
6. Handelt es sich um die Meldung einer Übermittlung, so ist auch anzugeben, welche Kreise von Betroffenen darin enthalten sein sollen, die zugehörigen Empfängerkreis einschließlich der allfälligen ausländischen Empfangsstaaten und die Rechtsgrundlagen der Übermittlungen.
7. Ist eine Genehmigung der Datenschutzkommission notwendig, so ist die Geschäftszahl der Genehmigung anzuführen.
8. Allgemeine Angaben über die getroffenen Datensicherheitsmaßnahmen, die eine Beurteilung der Angemessenheit erlauben. Im Gegensatz zu den vorherigen Punkten sind diese Angaben im Register jedoch nicht öffentlich einsehbar.

6.1.2. Musteranwendungen

Der Bundeskanzler kann per Verordnung Musteranwendungen definieren, welche eine Anmeldung vereinfachen. Hier handelt es sich um anmeldungspflichtige Datenanwendungen, die dennoch oft in gleicher Form vorkommen. Darin liegt lediglich eine Vereinfachung der Verfahrens, materiell sind jedoch alle Bestimmungen über eine Anmeldung anzuwenden (im Gegensatz zu Standardanwendungen, welche nicht anmeldepflichtig sind!).

Eine Anmeldung nach einer Musteranwendung darf nur dann erfolgen, wenn nicht mehr als die darin enthaltenen Daten, Verwendungen und Übermittlungen vorgesehen sind (Teilmenge). Zu einer Anmeldung genügt dann die Bezeichnung gemäß der Musteranwendung, Name und Anschrift des Auftraggebers, der Nachweis seiner Befugnis zur Verarbeitung (falls erforderlich) und die Registernummer des Auftraggebers, falls eine solche bereits existiert.

6.1.3. Standardanwendungen

Für jene Fälle, in welchen Datenanwendungen mit demselben Inhalt oder Übermittlungen aus diesen von vielen Auftraggebern in gleicher Weise üblicherweise durchgeführt werden und gleichzeitig inhaltlich die schutzwürdigen Geheimhaltungsinteressen voraussichtlich nicht gefährdet werden, kann der Bundeskanzler per Verordnung eine Standardanwendung schaffen, wodurch die Meldepflicht entfällt. Es werden darin sowohl die Kreise der Betroffenen (bei Übermittlungen auch die der möglichen Empfänger) als auch die zulässigen Datenarten und die Höchstdauer der Datenaufbewahrung festgelegt. Eine Registrierung im Datenverarbeitungsregister ist nicht notwendig, da die Vornahme solcher Anwendungen jedermann in einer bestimmten Situation voraussetzen muß.

Ein Beispiel hierfür ist die Führung einer automationsunterstützten Buchhaltung. Es ist daher nicht notwendig, die Betroffenen durch eine explizite Meldung darauf hinzuweisen. Um aber das Auskunftsrecht auch hier sicher zu gewährleisten, ist jeder Auftraggeber verpflichtet, jedermann (nicht nur Betroffenen!) mitzuteilen, welche Standardanwendungen er tatsächlich durchführt.

6.2. Gerichtliche Geltendmachung

Ein Betroffener hat Anspruch auf Unterlassung und Beseitigung eines dem Datenschutzgesetz widersprechenden Zustandes (Verletzung der Geheimhaltung, Richtigstellung, Löschung, Schadenersatz). Ist der Verursacher ein Auftraggeber des privaten Bereichs, so sind diese Ansprüche vor den ordentlichen Gerichten durchzusetzen.

Zuständig ist in erster Instanz das Landesgericht, in dessen Sprengel der Betroffene seinen gewöhnlichen Aufenthalt (bzw. Sitz bei juristischen Personen) hat. Der Betroffene hat nach seiner Wahl jedoch auch die Möglichkeit, Klage bei dem Gericht zu erheben, in dessen Sprengel der Auftraggeber oder Dienstleister seinen gewöhnlichen Aufenthalt oder Sitz hat.

Die Datenschutzkommission hat einem Verfahren als Nebenintervenient beizutreten, wenn der Betroffene dies verlangt und es zur Wahrung der Interessen einer größeren Zahl von Betroffenen geboten ist. Hierbei ist vor allem an Musterprozesse oder Prozesse gegen große Auftraggeber mit entsprechend großen Möglichkeiten (z. B. Privatgutachten) zu denken.

6.3. Beschwerde bei der Datenschutzkommission

Es ist zwischen einer Beschwerde an die Datenschutzkommission (§ 31 DSG) und der Anregung einer Kontrolle (§ 30; siehe Abschnitt 8.2) zu unterscheiden: Im ersten Fall hat sie eine quasi-richterliche Entscheidungsfunktion, während bei einer Kontrolle nur eine amtswegige Überprüfung ohne Anspruch auf ein bestimmtes Ergebnis durchgeführt wird. Die Zuständigkeit der Datenschutzkommission umfaßt alle Verletzungen des Auskunftsrechts (auch durch Auftraggeber des privaten Bereichs) und Verletzungen durch Auftraggeber des öffentlichen Bereichs. Handelt es sich um Handlungen, die nach funktionalen Gesichtspunkten entweder der Gerichtsbarkeit oder der Gesetzgebung[26] zuzurechnen sind, so ist die DSK unzuständig; es verbleibt daher nur mehr (allerdings die gesamte; inklusive der obersten Organe) die Verwaltung. Die Datenschutzkommission kann auch einstweilige Verfügungen mit dem Inhalt treffen, daß eine weitere Verwendung der Daten untersagt wird oder ein Bestreitungsvermekr anzubringen ist. Erfolgt eine Beschwerde wegen Daten, die nicht dem Auskunftsrecht unterliegen, so ist während des Verfahrens die Geheimhaltung zu wahren (Gegenüber des DSK besteht daher kein Recht zur Geheimhaltung!). Ist die Geheimhaltung im Ergebnis nicht gerechtfertigt, so ist eine Offenlegung per Bescheid anzuordnen. Erfolgt diese nicht binnen 8 Wochen, so wird die Auskunft der Daten, bzw. welche Berichtigung oder Löschung erfolgte, von der Datenschutzkommission selbst vorgenommen.

6.4. Schadenersatzregelung

Grundsätzlich gelten die allgemeinen Bestimmungen über Schadenersatz bzw. Amtshaftung. Dies bedeutet, daß nur bei Verschulden eine Haftung eintritt. In besonderen Fällen wird jedoch auch (sonst nicht enthaltener!) immaterieller Schaden[27] ersetzt: Handelt es sich um die öffentlich

[26] Siehe Bericht des Verfassungsausschusses, welche Teile der Parlamentsverwaltung der Kontrolle Datenschutzkommssion unterstehen sollen. Diese Aufzählung hat freilich keinen verbindlichen Charakter.

[27] Gemäß § 6 und 7 MedienG: Derzeit maximal 200.000,- ATS

zugängliche Verwendung von sensiblen, strafrechtlich relevanten oder die Kreditwürdigkeit betreffenden Daten und wird dadurch eine Bloßstellung im Sinne des Mediengesetzes (§ 7 Abs. 1 MedienG) verwirklicht, so fällt die dort nötige Veröffentlichung in einem Medium als Tatbestandsmerkmal weg. Sowohl rechtsmißbräuchliche wie auch fehlerhafte Datenverwendung kann diese Folge auslösen.

Zugunsten des Betroffenen wurde eine Beweislastumkehr geschaffen und die Haftung beim Auftraggeber konzentriert: Er haftet auch für das Verhalten seiner Leute und auch von Dienstleistern und deren Angestellte, die er mit der Verarbeitung beauftragt hat. Der Auftraggeber kann sich nur dadurch von der Haftung befreien, daß er nachweist, daß der Umstand, der den Schaden verursachte, nicht ihm bzw. seinen Mitarbeitern zur Last gelegt werden kann. Diesfalls haftet nur mehr der Dienstleister. Zuständig ist das gleiche Gericht, wie für Klagen gegen private Auftraggeber wegen Verletzung der Rechte des Betroffenen.

7. Strafbestimmungen

Gegenüber dem alten Datenschutzgesetz aus dem Jahr 1980 wurden die gerichtlichen Strafbestimmungen stark ausgedünnt, da sich zeigte, daß sie einerseits fast nicht zu verwirklichen waren, bzw. zu einer Kriminalisierung des Großteils aller Arbeitstätigen führen könnten. Dafür wurden mehrere Verwaltungsstrafen eingeführt, die diesen Ausfall ersetzen und ergänzen.

7.1. Gerichtliche Strafbestimmung

Gerichtlich strafbar mit Freiheitsstrafe bis zu einem Jahr bleibt lediglich die rechtswidrige Verwendung von personenbezogenen Daten in besonders verwerflicher Absicht: Um sich einen Vermögensvorteil zu verschaffen oder einem Anderen einen Schaden zuzufügen. Voraussetzung dabei ist, daß es sich um personenbezogene Daten handelt, an denen der Betroffene ein schutzwürdiges Geheimhaltungsinteresse (§ 8, 9) hat. Diese Daten müssen dem Täter ausschließlich durch seine berufliche Tätigkeit anvertraut oder bekanntgeworden sein, bzw. er sie sich widerrechtlich verschafft haben. Die Tathandlung besteht darin, die Daten zu benützen (ohne daß das Gesetz dies näher definiert), sie insbesondere anderen zugänglich zu machen oder zu veröffentlichen. Es handelt sich um ein Ermächtigungsdelikt, der Täter darf daher nur mit Zustimmung des Verletzten verfolgt werden.

Zu beachten ist, daß kein Bezug auf die automatisierte Verarbeitung erfolgt. Das Delikt kann daher bei jederlei personenbezogenen Daten begangen werden, unabhängig davon, wie die Daten verarbeitet werden (Computer, Kartei), oder ob sie überhaupt gespeichert werden.

7.2. Verwaltungsstrafen

Die Verwaltungsstrafbestimmungen sind in zwei große Gruppen eingeteilt: Tatbestände, bei denen eine tatsächliche Verletzung stattgefunden hat und solche, bei denen zwar noch keine Verletzung vorliegt, aber zumindest die Gefahr dafür oder für eine Behinderung der Durchsetzbarkeit besteht. Bei allen Taten ist schon der Versuch strafbar.

Für die Verfolgung ist die Bezirksverwaltungsbehörde zuständig, in dem der Auftraggeber der Datenverarbeitung seinen gewöhnlichen Aufenthalt bzw. Sitz hat. Es kommt also nicht darauf an, wo die Daten verarbeitet wurden, noch wo die geschädigte (oder in ihren Rechten gefährdete) Person ihren Sitz hat. Letzteres deshalb, da in vielen Fällen die Anzahl der Verletzten oder Gefährdeten sehr groß ist und das Verwaltungsstrafverfahren ohnehin amtswegig durchgeführt wird (Partei ist nur der

Beschuldigte). Zusätzlich zur Geldstrafe kann auch noch der Verfall von Datenträgern und Programmen ausgesprochen werden, die im Zusammenhang mit der strafbaren Handlung stehen. Dies soll dazu dienen, die personenbezogenen Daten (bzw. deren Auswertung) zu entziehen, die widerrechtlich erlangt oder erstellt wurden, sowie die Programme, die dazu verwendet wurden. Zu beachten ist, daß die Datenverarbeitungsanlagen selbst nicht für Verfallen erklärt werden können. Höchstens Festplatten könnten als Datenträger entfernt werden.

7.2.1. Konkrete Verletzungen

Diese Straftaten sind subsidiär zu strengeren Verwaltungsstrafen und von Gerichten zu ahndenden Taten. Die Strafdrohung ist mit Geldstrafe bis 260.000,- ATS relativ hoch. Strafbar ist:

- wer sich vorsätzlich und widerrechtlich Zugang zu einer Datenanwendung verschafft. Dies entspricht dem klassischen "Hacken" von Rechnern. Es ist hierbei unerheblich, ob auch tatsächlich personenbezogene Daten ausspioniert wurden, es kommt lediglich darauf an, daß jemand sich die Möglichkeit hierzu verschafft. Aufgrund der Definition von "Daten" in § 4 Abs 1 DSG, müssen jedoch in der Anwendung zumindest personenbezogene Daten verarbeitet werden. Der Fall von "Zeitdiebstahl" ist daher auch hier nicht erfaßt. Nur wer vorsätzlich versucht, in personenbezogene Daten Einsicht zu nehmen, ist strafbar.
- wer einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält. Darunter fallen beispielsweise das Arbeiten an einem Terminal, auf dem personenbezogene Daten verarbeitet werden, welches dadurch möglich ist, da der vorherige Benutzer auf das Ausloggen vergaß oder auch das versehentliche Einloggen mit anderem Namen und Paßwort, wodurch Zugang erlangt wird. Wenn daher jemand erkennt, daß er Zugang zu personenbezogenen Daten hat, obwohl er diesen nicht haben dürfte, so ist er verpflichtet, diesen Zugang zu schließen oder schließen zu lassen und währenddessen keine Kenntnis von den Daten oder Einfluß auf die Verarbeitung zu nehmen.
- wer Daten vorsätzlich in Verletzung des Datengeheimnisses übermittelt. Hierzu reicht es bereits aus, wenn die Daten einer Person übermittelt werden. Es ist zu beachten, daß auch schon die Verwendung von Daten für einen anderen Zweck eine Übermittlung darstellt und daher strafbar ist. Sowohl Indiskretionen als auch kommerzieller Verkauf verletzen das Datengeheimnis und fallen daher unter diese Strafdrohung.
- wer Daten trotz rechtskräftigem Urteil oder Bescheid verwendet, keine Auskunft dazu erteilt, nicht richtigstellt oder die Löschung unterläßt. Hierbei handelt es sich um eine zusätzliche Maßnahme, um die rasche und vollständige Erfüllung von festgestellten Pflichten zu erzwingen. Dies ersetzt nicht die normale Durchsetzung von Urteilen oder Bescheiden, sondern ist eine zusätzliche Strafe.
- wer Daten vorsätzlich löscht, obwohl er bereits Kenntnis von einem Auskunftsverlangen oder der Erhebung einer Beschwerde bei der Datenschutzkommission hat. Dies soll verhindern, daß Beweismittel vernichtet werden. Es stellt sich jedoch wie bei allen elektronischen Beweismitteln insbesondere die Frage, wie sich nachweisen läßt, daß sie zu einem früheren Zeitpunkt existierten und zu einem bestimmten anderen Zeitpunkt dann gelöscht wurden.

7.2.2. Gefährdungen von Rechten oder der Durchsetzbarkeit

Diese Straftaten sind subsidiär zu gerichtlichen Straftaten. Die Strafdrohung ist Geldstrafe bis 130.000,- ATS. Strafbar ist:

- die Ermittlung, Verarbeitung oder Übermittlung von Daten, ohne daß die Meldepflicht erfüllt wurde. Ist eine Meldepflicht gegeben (Ausnahmen siehe Abschnitt 6.1), so darf in den meisten Fällen unmittelbar nach dieser Meldung der Betrieb aufgenommen werden. Erfolgt jedoch keine Meldung oder darf der Betrieb erst nach Genehmigung aufgenommen werden (§ 18 Abs 2) und wird dennoch sofort begonnen, so wird dieser Tatbestand verwirklicht. Auch eine Überschreitung der eigenen Meldung fällt hierunter.
- die Übermittlung von Daten ins Ausland, obwohl dafür eine Genehmigung der Datenschutzkommission notwendig gewesen wäre und diese nicht eingeholt wurde. Hiermit soll sichergestellt werden, daß Übermittlungen nur dann erfolgen, wenn diese auch tatsächlich geprüft und genehmigt wurden. Auch wenn die Übermittlung voll genehmigungsfähig ist, wird das Delikt durch die Übermittlung vollendet.
- die Verletzung der Offenlegungsvorschriften. Darunter fallen die Auskunft über vorgenommene Standardanwendungen an Benutzer und nicht-meldepflichtige Anwendungen an die Datenschutzkommission (§ 23), Verletzungen der Informationspflicht des Auftraggebers gegenüber den Betroffenen (§ 24) und die Offenlegung der Identität des Auftraggebers (§ 25). In diesem Tatbestand sind Verletzungen der Vorschriften enthalten, welche die Durchsetzbarkeit der Rechte der Betroffenen schmälern: Wenn eine Person nicht weiß, wer genau welche speziellen Daten über sie besitzt oder verarbeitet, kann dies auch nicht auf die Rechtmäßigkeit überprüfen oder per Beschwerde prüfen lassen.
- die gröbliche Außerachtlassung der erforderlichen Sicherheitsmaßnahmen. Hiermit soll verhindert werden, daß durch schwere Verletzungen der Sorgfalt beim Umgang mit Daten ein unbefugter Zugriff viel leichter möglich ist. Das Delikt ist daher bereits dann verwirklicht, wenn aufgrund mangelnden Schutzes die Gefahr für eine unrechtmäßige Verarbeitung sehr groß ist.

8. Die Datenschutzkommission

Im Gegensatz zum Datenschutzrat spielt die Datenschutzkommission eine wichtige Rolle im Gefüge des DSG. Sie ist zur Wahrung der Rechte aufgrund des DSG berufen und besitzt wichtige Kontroll- und Entscheidungsbefugnisse.

Im Gegensatz zu den Grundsätzen der Bundesverfassung ist sie auch zur Kontrolle der obersten Organe der Vollziehung ermächtigt (Verfassungsbestimmung). Dies bezieht sich darauf, daß Bundespräsident, Bundesminister und Mitglieder der Landesregierung auch ihrer Kontrolle unterliegen (was sonst bei **obersten** Organen begrifflich ausgeschlossen ist).

In Ausübung ihres Amtes sind die Mitglieder der Datenschutzkommission weisungsfrei. Dies ist eine Verfassungsbestimmung aufgrund der ihr eingeräumten Kontrollbefugnisse. Für ihre Entscheidungen würde sich die Weisungsfreiheit auch aus Art. 20 Abs. 2 B-VG ergeben. Administrativ ist sie jedoch dem Bundeskanzleramt zu- und untergeordnet.

8.1. Zusammensetzung

Die Datenschutzkommission besteht aus 6 Mitgliedern, die für die Dauer von 5 Jahren vom Bundespräsidenten auf Vorschlag der Bundesregierung bestellt werden. Dabei bestehen folgende Vorschlagsrechte:

- Dreiervorschlag des Präsidenten des Obersten Gerichtshofs für das richterliche Mitglied (das den Vorsitz führt)

- Vorschlag der Länder für zwei Mitglieder
- Dreiervorschlag der Arbeiterkammer für ein Mitglied
- Dreiervorschlag der Wirtschaftskammer für ein Mitglied
- Ein Mitglied muß dem Kreis der rechtskundigen Bundesbeamten angehören

Zusätzlich ist für jedes Mitglied ein Ersatzmitglied zu bestellen, welches bei Verhinderung dessen Stelle einnimmt. Ihre Funktionsperiode läuft immer gleich der des von ihnen vertretenen Mitgliedes. Ein Ausschluß eines Mitgliedes aus schwerwiegenden Gründen oder wegen wiederholtem unentschuldigtem Fernbleiben ist nur durch Beschluß der Kommission selbst möglich. Die Mitglieder (Ersatzmitglieder nur bei Vertretung) haben Anspruch auf Abgeltung der Reisekosten und einer dem Arbeitsaufwand entsprechenden Vergütung (vom Bundeskanzler per VO festgelegt). Die Kommission gibt sich ihre Geschäftsordnung selbst.

Beschlüsse erfolgen mit einfacher Mehrheit, wobei bei Stimmengleichheit die Stimme des Vorsitzenden den Ausschlag gibt. Eine Stimmenthaltung ist unzulässig. Im Gegensatz zum Datenschutzrat ist die Beifügung von Minderheitenvoten unzulässig.

8.2. Kontrollbefugnisse

Die Datenschutzkommission kann in zwei Fällen eine Kontrolle der Datenverarbeitung vornehmen: Wenn eine Person eine Verletzung ihrer Rechte oder die Verletzung ihn betreffender Pflichten eines Datenverarbeiters behauptet und in bestimmten Fällen[28] auch ohne Verdacht. Wird auf Anzeige einer Person hin untersucht (oder auch nicht), so ist diese über das Ergebnis, bzw. den Grund der nicht erfolgten Kontrolle zu informieren.

Im Fall des begründeten Verdachtes der Verletzung der Rechte einer Person kann (hier wohl im Sinn von "muß" gebraucht) die Datenschutzkommission die Datenanwendung überprüfen. Dazu kann sie alle notwendigen Aufklärungen vom Verarbeiter verlangen, selbst Einschau nehmen und auch Verarbeitungen durchführen. Um dies zu ermöglichen, ist es ihr gestattet, die Räume, in denen die Verarbeitung stattfindet, nach Verständigung des Inhabers zu betreten und auch Kopien von Datenträgern herzustellen. Letzteres jedoch nur in dem Umfang, wie es zur Kontrolle des konkreten Vorfalles bzw. etwaiger sich aus dem Laufe der bisherigen Durchführung der Kontrolle ergebenden weiterer Anhaltspunkte erforderlich ist. Diese Kontrolle ist unter möglichster Schonung der Rechte des Auftraggebers (z. B. nur innerhalb der Betriebszeiten) und Dritter (z. B. Behinderung der Verarbeitung von deren Daten durch Beanspruchung der Rechenanlagen durch die Kontrolle) durchzuführen.

Bezüglich der bei einer Kontrolle gewonnenen Informationen, welche nicht die Anzeige, bzw. den Verdacht oder sonstige datenschutzrechtliche Vorschriften betreffen, besteht eine strenge Verschwiegenheitspflicht. Sie besteht sowohl gegenüber Gerichten wie Verwaltungsbehörden[29]. Es ist jedoch zu beachten, daß bei Verletzung dieser Vorschrift die Information dennoch verwendet werden darf (keine Nichtigkeit!). Folgende Ausnahmen bestehen:

---

[28] Bei Anwendungen, die der Vorabkontrolle gem. § 18 Abs. 2 DSG unterliegen: Keine Musteranwendung und u. A Verarbeitung sensibler oder strafrechtlicher Daten oder die Kreditwürdigkeit betreffend. In diesen Fällen darf der Betrieb erst nach der Prüfung aufgenommen werden (sonst unmittelbar nach Abgabe der Meldung).

[29] Explizit angeführt sind die Abgabenbehörden; daher dürfen steuerrelevante Erkenntnisse nicht weitergegeben werden!

1. Eine gerichtlich oder von Verwaltungsbehörden strafbare Handlung des Datenschutzgesetzes wird aufgedeckt oder es ergeben sich Hinweise darauf (§ 51f DSG; Siehe Abschnitt 7).
2. Es kommen Anhaltspunkte für eine strafbare Handlung zutage, welche mit mindestens 5 Jahren Freiheitsstrafe bedroht ist.[30]

Tritt ein Verdacht für eine dieser Handlungen während der Kontrolle auf, so ist Anzeige zu erstatten und auch entsprechende Auskunftsbegehren von Gerichten zu beantworten.

Falls bei der Kontrolle Unregelmäßigkeiten oder Verstöße hervorkommen, so kann die Datenschutzkommission eine Empfehlung aussprechen, wie diese Mißstände behoben werden können, und diese Empfehlung mit einer angemessenen Frist ausstatten. Wird dieser Empfehlung nicht (oder nicht rechtzeitig) entsprochen, so stehen der Datenschutzkommission die folgenden Möglichkeiten offen:

- Ein Verfahren zur amtswegigen Berichtigung des Datenverarbeitungsregisters kann eingeleitet werden (fehlende oder unrichtige Angaben werden ergänzt / korrigiert / gestrichen).
- Es kann Strafanzeige erstattet werden entweder bei Gericht (§ 51; siehe Abschnitt 7.1) oder der Bezirksverwaltungsbehörde (§ 52; siehe Abschnitt 7.2).
- Handelt es sich um einen schwerwiegenden Verstoß, der sonst vom Verletzten selbst vor Gericht zu verfolgen wäre (Auftraggeber entstammt dem privaten Bereich), so kann[31] die Datenschutzkommission statt ihm eine Feststellungsklage erheben. Der Betroffene erhält damit (ohne das Prozeßrisiko tragen zu müssen!) eine sichere rechtliche Basis für folgende Unterlassungs- oder Schadenersatzansprüche.
- Handelt es sich beim Auftraggeber der Verarbeitung um eine Gebietskörperschaft, so kann sie das zuständige oberste Organ befassen (Minister, Landesregierung/Landesrat, Gemeinderat). Innerhalb einer angemessenen Frist (maximal 12 Wochen) muß der entsprechende Zustand hergestellt werden, oder der Datenschutzkommission mitgeteilt werden, warum der Empfehlung nicht entsprochen wurde. Um auch hier gewisse Sanktionen setzen zu können, kann die Kommission die Begründung der Öffentlichkeit in geeigneter Weise zur Kenntnis bringen (Presse), wenn dies die Amtsverschwiegenheit erlaubt.

8.3. Rechtszug und besondere Bescheidwirkungen

Erläßt ein einzelnes Mitglied der Kommission einen Bescheid (geschäftsführendes Mitglied: Vorläufige Untersagung der Datenanwendung § 20 Abs 2 und amtswegige Änderungen uns Streichungen im Datenverarbeitungsregister § 22 Abs 3), so kann Vorstellung an die Kommission erhoben werden, die dann endgültig entscheidet. In allen anderen Fällen entscheidet die gesamte Kommission als erste Instanz (und gleichzeitig letztinstanzlich). In diesem Fall ist die Anrufung des Verwaltungsgerichtshofes möglich.

Bescheide betreffend die Genehmigung der Übermittlung von Daten ins Ausland sind gegenüber "normalen" Bescheiden mit einer geringeren Bestandskraft ausgestattet. Wird von der Europäischen

[30] Vergleiche dazu § 149c Abs. 3 Z 2 StPO (Abhören des Fernmeldeverkehrs): Vorsätzliche, mit mehr als einem Jahr Freiheitsstrafe bedrohte Handlung. Sonst mit Nichtigkeit behaftet!

[31] Nach den Erläuterungen zur Regierungsvorlage „kann", also nach Ermessen der Datenschutzkommission. Nach § 32 Abs. 5 DSG („hat") muß eine Feststellungsklage jedoch erfolgen, wenn ein begründeter Verdacht auf eine schwerwiegende Datenschutzverletzung besteht.

Kommission per Verordnung festgestellt, daß die Voraussetzungen für Übermittlungen in dieses Land nicht vorliegen (entgegen der Beurteilung durch die Datenschutzkommission), so sind die Bescheide zu widerrufen. Dies ist auch dann möglich, wenn durch Rechts- oder Sachlagenänderung die Voraussetzungen nicht mehr gegeben sind.

9. Der Datenschutzrat

Der Datenschutzrat ist in den § 41-44 geregelt. Er hat keine essentiellen Aufgaben bei der Durchführung des DSG zu erfüllen, sondern besitzt lediglich beratende Funktion. Er soll sowohl Bundes- wie auch Landesregierungen (bei diesen aus kompetenzrechtlichen Gründen nur auf deren Ersuchen hin) in rechtspolitischen Fragen des Datenschutzes beraten und hierzu Stellungnahmen zu Gesetzesvorhaben abgeben. Weiters kann er Kommentare zu Vorhaben im öffentlichen Bereich abgeben, die datenschutzrechtlich von Bedeutung sind. In diesem Zusammenhang kann er von Auftraggebern des öffentlichen Bereichs Auskünfte, Berichte und Unterlageneinsicht verlangen, wenn dies für die Beurteilung eines Vorhabens in datenschutzrechtlicher Hinsicht notwendig ist.

Der Datenschutzrat ist folgendermaßen zusammengesetzt: Vertreter der Nationalratsparteien entsprechend ihrer Stärke, je ein Vertreter der Arbeiterkammer und der Wirtschaftskammer, zwei Ländervertreter, je ein Vertreter des Gemeinde- und des Städtebundes und ein Vertreter des Bundes. Diese Mitglieder sind auf unbestimmte Zeit ernannt und scheiden nur durch Nominierung eines anderen Mitgliedes oder Zurücklegung aus. Die Beratungen sind vertraulich und nach Bedarf abzuhalten (Einberufung durch den Vorsitzenden oder auf Verlangen eines Mitgliedes). Die Tätigkeit ist ehrenamtlich, es besteht lediglich Anspruch Reisekostenersatz.

10. Besondere Aspekte

In diesem Abschnitt sollen abschließend noch einige besondere Punkte betrachtet werden: Um die Geheimhaltung von Daten, die gesetzlich vorgeschrieben ist, auch zu gewährleisten, müssen entsprechende Maßnahmen gesetzt werden. Weiters hat oft auch der Betroffene ein Interesse an der Weiterexistenz der Daten, sodaß auch die Sicherung gegen Verlust Teil davon ist. Eine besondere Gefahr für einzelne Personen besteht auch dann, wenn sie einer ausschließlich automatisierten Entscheidung unterworfen werden sollen (z. B. Beurteilung ihrer Kreditwürdigkeit). Besonders im Bereich der Direktwerbung spielt der Datenschutz eine besondere Rolle, da die Werbungsversender großes Interesse daran haben, ihre Werbung möglichst zielgerichtet zu adressieren. Dieser Aspekt ist zwar in der DSRL enthalten, ist in Österreich aber in der Gewerbeordnung (GewO) enthalten. Aufgrund des Zusammenhangs wird er jedoch auch hier behandelt.

10.1. Datensicherheitsmaßnahmen

Je nach Art der verwendeten Daten und nach Umfang und Zweck der Verwendung ist sicherzustellen, daß Daten vor zufälliger oder unrechtmäßiger Zerstörung oder Verlust geschützt sind, daß ihre Verwendung ordnungsgemäß erfolgt und daß Unbefugte keinen Zugang dazu erlangen. Beim Ausmaß des Schutzes ist auf den Stand der technischen Möglichkeiten und die wirtschaftliche Vertretbarkeit der Maßnahmen Bedacht zu nehmen. Es muß ein Schutzniveau gewährleistet werden, das den von der Verwendung ausgehenden Risiken, der Art der zu schützenden Daten und den aus der Durchführung entstehenden Kosten angemessen ist. Erforderlich sind z. B. die folgenden Maßnahmen (von entsprechendem Niveau):

1. Die Aufgabenverteilung bei der Datenverwendung ist zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen.
2. Die Datenverwendung muß an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter gebunden werden.
3. Jeder Mitarbeiter ist über seine Pflichten nach dem DSG und nach innerbetrieblichen Datenschutz- und Datensicherheitsvorschriften zu belehren.
4. Die Zutrittsberechtigung zu den Räumlichkeiten ist zu regeln.
5. Zugriffsberechtigungen auf Daten und Programme sind vorzusehen.
6. Datenträger sind vor Einsicht und Verwendung durch Unbefugte zu sichern. Dies schließt wahrscheinlich auch die Sicherung vor Löschung/Entfernung mit ein.
7. Berechtigungen zum Betrieb von Datenverarbeitungsgeräten sind festzulegen und die Geräte durch Vorkehrungen (Hard-/ Software) gegen unbefugte Inbetriebnahme zu sichern.
8. Protokolle müssen geführt werden, damit tatsächliche durchgeführte Verwendungsvorgänge (insbesondere Änderungen, Abfragen und Übermittlungen) auf ihre Zulässigkeit im notwendigen Ausmaß überprüft werden können.
9. Es ist eine Dokumentation über alle Datensicherheitsmaßnahmen zu führen, um eine Kontrolle und Beweissicherung zu erleichtern.

Die Protokoll- und Dokumentationsdaten dürfen ausschließlich für den Zweck ihrer Ermittlung verwendet werden: Die Kontrolle der Zulässigkeit der Verwendung des Datenbestandes. Nicht erlaubt ist insbesondere die Verwendung zur Kontrolle der Personen, deren Daten im Datenbestand enthalten sind. Weiters dürfen sie nicht zu einem anderen Zwecke dienen, die Personen zu kontrollieren, welche auf den Datenbestand zugreifen, als ihre Zugriffsberechtigung zu prüfen (z. B. Erstellung von Zugriffsprofilen). Eine Ausnahme von diesem Verbot besteht, wenn es sich um die Verfolgung oder Verhinderung eines Verbrechens handelt, das mit mindestens fünfjähriger Freiheitsstrafe bedroht ist. Protokoll- und Dokumentationsdaten sind drei Jahre lang aufzubewahren. Abweichungen sind nur zulässig, insoweit die davon betroffenen Daten länger oder kürzer existieren.

10.2. Automatisierte Einzelentscheidungen

Gemäß § 49 DSG darf niemand einer Entscheidung zum Zweck der Bewertung einzelner Aspekte seiner Person unterworfen werden, die ausschließlich auf Grund einer automationsunterstützen Verarbeitung von Daten getroffen wurde, wenn dies für ihn rechtliche Folgen nach sich zieht oder ihn erheblich beeinträchtigt. Als Beispiele werden die berufliche Leistungsfähigkeit, die Kreditwürdigkeit, die Zuverlässigkeit oder das Verhalten angeführt.

Da jedoch vielfach ein starkes Bedürfnis nach solchen Entscheidungen besteht (insbesondere im staatlichen Bereich: Beihilfeverfahren, Steuerbescheide, etc.), wurden einige Ausnahmen geschaffen, welche das Verbot sehr stark einschränken:

1. Ist die automatisierte Einzelentscheidung gesetzlich vorgesehen, so ist dies erlaubt.
2. Ergeht die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertrages und wurde dem Ersuchen des Betroffenen auf Abschluß oder Erfüllung des Vertrages entsprochen (Bsp.: automatische Überprüfung der Kreditwürdigkeit bei Vertragsabschluß; wird diese jedoch verneint, so muß eine persönliche Nachkontrolle stattfinden!).

3. Kein Verbot besteht, wenn die berechtigten Interessen des Betroffenen durch geeignete Maßnahmen garantiert werden. Da als Beispiel die Möglichkeit angeführt wird, daß der Betroffene seinen Standpunkt geltend machen kann, erlaubt dieser Punkt sehr weite Einschränkungen.

Auf Antrag des Betroffenen ist der Ablauf der automatisierten Entscheidung in allgemein verständlicher Form vom Auftraggeber darzulegen. Einschränkungen dieses Rechts ergeben sich jedoch u. A aus dem Urheberrecht und dem Geschäftsgeheimnis. Diesbezüglich ist eine Verhältnismäßigkeitsprüfung durchzuführen.

10.3. Direktwerbung

Die Tätigkeit von Adressverlagen und Direktwerbeunternehmen ist nicht im DSG, sondern in § 268 GewO geregelt. Dieser Bereich ist jedoch auch in der DSRL enthalten und gehört inhaltlich dazu, daher wird er auch hier behandelt.

Adressverlage und Direktwerbeunternehmen dürfen Daten aus öffentlich zugänglichen Quellen, aus eigenen Erkundungen und aus Kunden- und Interessentendateien anderer Adressverlage und Direktwerbeunternehmen erheben. Für die Ermittlung besteht eine enge Zweckbindung: Sie darf nur für die Vorbereitung und Durchführung von Direktwerbeaktionen, die Gestaltung und den Versand der Werbemittel für Waren oder Dienstleistungen anderer sowie für die Tätigkeit als Mittler zwischen Inhabern und Nutzern von Kunden- und Interessendateien erfolgen.

Betroffene haben das Recht, ihre Daten kostenlos auf Verlangen löschen zu lassen. Im Gegensatz zu normalen Daten besteht hier keine so enge Zweckbindung. Daten dürfen grund-sätzlich an andere solche Gewerbetreibende übermittelt werden, außer der Betroffene hat dies ausdrücklich untersagt. Werden die Daten schriftlich erhoben, so ist auf diese Möglichkeit ausdrücklich und schriftlich hinzuweisen[32]. Demgegenüber besteht allerdings eine Begrenzung der Daten über Betroffene, die zulässig übermittelt werden dürfen (Für die eigene Verwendung besteht diese Begrenzung nicht!). Sollen mehr Daten übermittelt werden, ist auf die Regelungen des DSG zurückzugreifen. Nach der GewO dürfen nur übermittelt werden: Namen, Titel, akademische Grade, Anschrift, Geburtsjahr, Berufs-, Branchen- und Geschäftsbezeichnung und die Zugehörigkeit des Betroffenen zu der Kunden- oder Interessentendatei. Für sensible und strafrechtsbezogene Daten[33] besteht ein weitergehender Ermittlungs- und Verarbeitungsschutz. Für diese ist eine ausdrückliche schriftliche Zustimmung notwendig.

11. Literatur

11.1. Allgemein

DuD: Datenschutz und Datensicherheit http://www.dud.de (16.12.1999)

Kresbach, Georg: E-Commerce. Nationale und internationale Rechtsvorschriften zum Geschäftsverlehr über elektronische Medien. Wien: Linde 2000

[32] Diese Untersagung hat auf ein Vertragsverhältnis mit dem Inhaber der Kunden- und Interessentendatei keinen Einfluß.

[33] Der genaue Katalog ist demgegenüber leicht abgewandelt, so ist etwa die Gewerkschaftszugehörigkeit nicht enthalten; siehe dazu genauer § 268 Abs. 7 GewO

Schaumüller-Bichl, Ingrid: Datenschutz und Informationsrecht. Vorlesung SS 99. Universität Linz 1999

11.2. Rechtsvorschriften

DSG: Datenschutzgesetz 2000 - DSG 2000, BGBl. I Nr. 165/1999

Datenschutz-Richtlinie: Richtlinie 95/46/EG des Europäischen Parlamentes und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Amtsblatt der Europ. Gemeinschaften L 281; 23.11.1995; S 31ff

Erläuterungen zur Regierungsvorlage (1613 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP)

Bericht des Verfassungsausschusses (2028 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP)

Richtlinien betreffend personenbezogenen Daten in automatisierten Dateien (UN Generalversammlungsbeshluß vom 14.12.1990)

Charta der Grundrechte der Europäischen Union (Entwurf 21.9.2000) http://www.dud.de/dud/documents/convent47de.pdf

IV. Verträge im Internet: Kaufverträge und Konsumentenschutz

Einer der Hauptpunkte (nach manchen Definitionen auch der einzige Inhalt) von E-Commerce ist der Abschluß von Kaufverträgen mittels elektronischer Kommunikation. Hier stellen sich weniger rechtliche Fragen, als vielmehr Fragen der Beweissicherung und der Anwendung. So kommt ein Vertrag durch Übereinstimmung von Angebot und Annahme zustande: Aber was ist im Internet nun ein Angebot: Eine Webseite, ein Warenkorb mit Lieferauskunft oder etwa eine persönliche Mail? Weiters werden in diesem Kapitel noch Vorschriften für den Verbraucherschutz erläutert.

1. Einleitung

In diesem Abschnitt wird erläutert, wie Verträge im allgemeinen und Kaufverträge im besonderen abgeschlossen werden, jedoch noch ohne auf Besonderheiten von elektronischer Kommunikation einzugehen. Weiters wird untersucht, welches Recht anzuwenden ist: Das Recht des Käuferlandes, des Verkäuferlandes oder überhaupt das eines dritten Ortes. Zum Abschluß werden kurz Besonderheiten dargestellt, die sich aus Verbraucherverträgen sowie der EU-Fernabsatzrichtlinie ergeben. Für Details und nähere Erläuterungen siehe [Koziol/Welser], worauf sich diese Ausführungen im Wesentlichen stützen.

1.1. Der Vertragsabschluß allgemein

Nach § 861 ABGB kommt ein Vertrag durch übereinstimmende Willenserklärungen von mindestens zwei Personen zustande. Hierbei wird regelmäßig in Angebot und Annahme unterschieden. Von einem Angebot kann nur dann gesprochen werden, wenn es zwei Punkte erfüllt: Erstens muß der Inhalt des gewünschten Vertrages ausreichend bestimmt sein und zweitens muß ein endgültiger Bindungswille darin zum Ausdruck kommen:

1. Bestimmtheit: Je nach Art des Vertrages müssen verschiedene Punkte enthalten sein. Beim Kaufvertrag handelt es sich hierbei um Ware und Preis. Stehen diese beiden fest, oder sind sie zumindest bestimmbar (z. B. Verkauf von Aktien zum aktuellen Börsepreis), so ist dieses Kriterium erfüllt. Es reicht aber auch aus, wenn die Punkte entweder aus dem Gesetz oder den Umständen hervorgehen, sodaß auch "verminderte" Angebote tatsächlich Angebote sein können. Weiters muß der Inhalt so konkret sein, daß ein reines und alleiniges "Ja" der anderen Partei den Vertrag perfekt machen kann.
2. Bindungswille: Aus dem Angebot muß der Bindungswille entnehmbar sein. Daher sind reine Werbung, "Angebote" zu Verhandlungen oder Vorschläge kein Angebot. Beispielsweise sind Auslagen, Zusendung von Katalogen etc. keine Angebote, sondern nur Aufforderungen an Kunden, ein solches zu stellen. Der Bindungswille bedeutet im Zusammenhang mit dem Zugang (siehe unten), daß das Angebot für eine gewisse Zeit nicht mehr geändert werden kann, sondern es nur mehr am Empfänger liegt, ob der Vertrag zustande kommt. Ein guter Hinweis darauf, ob der notwendige Bindungswille vorliegt kann meist darin gesehen werden, an wie viele Personen

das zu prüfende "Angebot" gerichtet ist: Handelt es sich um eine unbestimmte Anzahl, so wird regelmäßig kein Angebot vorliegen, da man nicht davon ausgehen kann, daß z. B. der Verkäufer eine rechtliche Bindung eingehen will, da sein Warenvorrat meist begrenzt ist und er daher an einer eventuell sehr großen Zahl von bindenden Verträgen nicht interessiert sein kann. Erst wenn eine Konkretisierung auf eine oder mehrere bestimmte Personen erfolgt, kann im Regelfall davon ausgegangen werden, daß der Angebotssteller sich an dieses Äußerung binden will.

Im Gegensatz zum Angebot ist die Annahme sehr einfach. Sie besteht darin, das zugehörige Angebot anzunehmen, und zwar vollständig und ohne Änderung. Werden auch nur in einem einzigen Punkt andere Bedingungen vorgeschlagen, handelt es sich nicht mehr um eine Annahme sondern um ein neues Angebot (der anderen Seite). Von der Unterscheidung in Angebot und Annahme ist die Rolle der Parteien bei einem Vertrag streng zu unterscheiden: Ein Angebot kann bei einem Kaufvertrag sowohl vom Käufer wie auch vom Verkäufer ausgehen.

Sowohl Angebot wie auch Annahme sind empfangsbedürftige Willenserklärungen. Dies bedeutet, daß ein Angebot im Rechtssinn erst dann vorliegt, wenn es dem Empfänger zugegangen ist (siehe Kapitel 3). Das Übertragungsrisiko liegt daher beim Sender (Beweislast für vollständigen/rechtzeitigen Empfang; § 862a ABGB). Auch kommt der Vertrag erst in dem Augenblick zustande, in dem der Angebotssteller von der Annahme erfährt. Rechtlich gesehen ist nur der Zugang maßgeblich, was nicht immer mit der Kenntnisnahme übereinstimmen muß; der Eintritt in die Sphäre des Empfängers genügt (z. B. Einwurf in dessen Briefkasten). Von dieser Regel gibt es auch eine Ausnahme: Ist nach der Natur des Geschäftes oder der Verkehrssitte eine Annahme nicht zu erwarten, so kommt der Vertrag zustande, wenn dem Angebot innerhalb der Annahmefrist tatsächlich entsprochen wird. Typisches Beispiel hierfür ist der Kauf im Versandhandel: Der zugesandte Katalog ist die Aufforderung, ein Angebot zu stellen und die abgesandte Bestellkarte das Angebot. Eine Annahme (=gesondertes Schreiben oder Telefonat) ist nicht üblich. Die Annahme erfolgt dadurch, daß der Versender die Ware abschickt (Abgabe am Postamt).

Wie lange ist nun eine Person an ihr Angebot gebunden? Grundsätzlich kann die Frist frei bestimmt werden, doch gelten für Verbrauchergeschäfte besondere Regeln (siehe unten). Ist nichts festgelegt, so sind Angebote "unter Anwesenden"[34] sofort anzunehmen. Bei schriftliche Angeboten[35] ist die Fristberechnung komplizierter, wobei auf die normale Erwartung des Anbietenden abgestellt wird: Transport der Erklärung zum Empfänger + Angemessene Überlegungsfrist + Transport der Annahmeerklärung zurück zum Anbotssteller.

Bei E-Commerce stellt sich oft das Problem, daß manche Erklärungen (sofern es sich tatsächlich um Erklärungen im Rechtssinne handelt) des Verkäufers nicht unbedingt von einer natürlichen Person stammen, sondern es sich um automatisch erzeugt Antworten (z. B. eines Webservers) handelt. Hier ist laut österreichischer Lehre[36] der Mangel des Erklärungsbewußtseins irrelevant, wenn er die Handlung, die als solche gesetzt wird, zumindest fahrlässig verursacht hat. In der Bereitstellung eines Rechners und der Webseiten ist jedenfalls eine solche Handlung zu sehen. Durfte der Empfänger daher eine automatische Mitteilung als Erklärung werten (und hat er dies auch tatsächlich getan), so wird sie dem Absender auch dann zugerechnet, wenn dieser kein Wissen davon hat.

[34] Unter persönlich Anwesenden, aber auch Telefon; d. h. synchrone Kommunikationsmittel

[35] Briefe, aber auch Fax; d. h. asynchrone Kommunikationsmittel

[36] Siehe dazu näher [Koziol/Welser] 94

Für das Zustandekommen eines Vertrages ist die wahre Einwilligung notwendig, also die vollständige Übereinstimmung der beiden Willenserklärungen. Fehler die dabei auftreten können sind: Nicht ernst gemeinte Erklärungen, Unvollständigkeit, Erklärungsunterschiede zwischen Angebot und Annahme, Mehrdeutigkeit, Unverständlichkeit, Irrtum, List oder Zwang. Details zu diesen Problemen werden hier nicht näher erläutert.

1.2. Anzuwendendes Recht

Grundsätzlich steht es Vertragspartnern frei, den von ihnen abgeschlossenen Vertrag einem (fast) beliebigen Recht zu unterwerfen. Dieses braucht keinerlei Beziehung zum Gegenstand des Vertrages oder der Parteien besitzen. Regelmäßig wird jedoch das Recht des Ortes eines der beiden Partner vereinbart werden. Eine Einschränkung dieses Grundsatzes ergibt sich durch Schutzvorschriften für Endverbraucher (=Konsumenten), welche teilweise durch Vereinbarung nicht abgeändert werden können und daher trotz abweichender Rechtswahl bestehen bleiben (siehe unten). Von der Rechtswahl zu unterscheiden ist der Fall, daß kein Recht vereinbart wurde. In diesem Fall gilt nach internationalem Privatrecht (siehe IPRG und EVÜ) das Recht, zu dem die stärkste Beziehung besteht. Dies ist das Recht des Staates der Partei, welche die charakteristische Leistung (= nicht Geldwerte) erbringt. Dies ist bei einem Kaufvertrag der Staat, in dem der Verkäufer seinen gewöhnlichen Aufenthalt (bzw. den Sitz der Hauptverwaltung bei juristischen Personen) hat.

Allgemein ist zum anwendbaren Recht zu sagen, daß eine höchst komplizierte Rechtslage besteht. Eine ausdrückliche Wahl ist daher dringend zu empfehlen (Siehe dazu auch die AGB's der meisten Online-Shops). Doch auch wenn eine klare Aussage möglich ist (insbesondere im B2B E-Commerce[37]: freie Rechtswahl ohne Einschränkungen wie bei Verbrauchergeschäften), besteht oft das Durchsetzungsproblem. Ein gewonnenes Verfahren vor österreichischen Gerichten hat wenig Erfolg, wenn das Urteil nicht vollstreckt werden kann, da das betroffene Unternehmen seinen Sitz im Ausland hat und keine Tätigkeit in Österreich entfaltet. Die Alternative, im Ausland zu klagen, ist meist sehr kostspielig und wegen mangelnder Rechtskenntnis riskant. International sollte daher als Endverbraucher besonderes Augenmerk auf die Wahl des Verkäufers gelegt werden, um im Fall von Problemen auf Kulanzregelungen oder vorab vereinbarte Verfahren (z. B. garantiertes Rückgaberecht) vertrauen zu können.

1.3. Verbraucherverträge / Konsumentenschutzgesetz allgemein

Nach dem Europäischen Vertragsstatutübereinkommen (Art. 5 EVÜ) besteht bei Verbraucherverträgen (Vorsicht: Etwas andere Definition als im KSchG!) zwar eine freie Rechtswahl, doch sind Bestimmungen, welche dem Verbraucher den Schutz im Staat seines gewöhnlichen Aufenthalts entziehen, unwirksam (unter einigen zusätzlichen Bedingungen). Eine ähnliche Bestimmung findet sich auch im KSchG in § 13a Abs. 2. Für E-Commerce ist hier die Klausel wichtig, daß dies gilt, wenn dem Vertragsabschluß ein ausdrückliches Angebot oder eine Werbung in diesem Staat vorausgegangen ist und der Verbraucher dort die zum Abschluß des Vertrages notwendigen Rechtshandlungen vorgenommenen hat. Der letzte Punkt ist einfach zu beurteilen: Der Konsument muß seine Erklärung in Österreich abgegeben (d. h. das Bestellformular auf der Webseite ausgefüllt oder die E-Mail abgeschickt) haben. Der erste Punkt ist viel schwieriger zu beurteilen. Eine Webseite allein wird, nur weil sie im Inland abgerufen werden kann, noch nicht als Werbung im Inland zu qualifizieren sein. Demgegenüber sind Bestellseiten auf Deutsch oder die explizite (z. B. Listbox, nicht aber die Möglichkeit ein Empfangsland in ein Textfeld einzutragen!)

[37] Achtung auf die Definition von „Verbraucher"!

Möglichkeit, nach Österreich zu liefern ein Hinweis auf eine Betätigung im Inland. Wird hingegen ein österreichischer Domainname ("???.at") verwendet oder kann eine länderspezifische Darstellung gewählt werden (z. B. Landesflaggen), so liegt mit Sicherheit eine Betätigung im Inland vor, worauf der Schutz eintritt.

Für Endverbraucher legt das österreichische Konsumentenschutzgesetz besondere Schutzvorschriften fest, die auf diese Weise (trotz sonst anzuwendendem ausländischem Recht) gültig bleiben und anzuwenden sind. Um ein "Verbrauchergeschäft" im Sinne des Gesetzes handelt es sich, wenn jemand, für den das Geschäft zum Betrieb seines Unternehmens gehört, ein Rechtsgeschäft mit jemandem schließt, für den dieses Geschäft eben nicht zum Betrieb eines Unternehmens gehört[38]. Wichtigster Punkt ist, daß viele Bestimmungen dieses Gesetzes zwingender Natur sind, also entgegenstehende Vereinbarungen zum Nachteil des Verbrauchers nichtig sind. Dies sind insbesondere (§ 6 Abs. 1 KSchG):

1. Bindungswirkung des Angebots (Z1): Der Unternehmer darf sich keine unangemessen lange oder unbestimmte Frist für die Annahme des Angebotes festlegen. Diese ist bei E-Commerce auf Grund der schnellen Kommunikation regelmäßig als sehr kurz zu sehen.
2. Haftungsausschluß bei Vorsatz oder grober Fahrlässigkeit (Z9): Der Unternehmer kann den Ersatz von Personenschäden nicht einschränken und auch sonst seine Haftung für Vorsatz und grobe Fahrlässigkeit nicht ausschließen. Dies dürfte besonders beim Verkauf von Software relevant sein. So ist etwa der Ausschluß der Haftung beim Versand von Viren-verseuchter Software nicht möglich, da das Unterlassen der Prüfung jedenfalls grobe Fahrlässigkeit darstellt.
3. Zusätzliche Beweislast (Z11): Dem Verbraucher darf keine andere als die gesetzliche Beweislast auferlegt werden.
4. Überhöhte Verzugszinsen (Z13): Kommt der Verbraucher mit seiner Zahlung in Verzug, so dürfen die hierfür verlangten Zinsen höchstens 5 % betragen. Von den Zinsen sind Betreibungs- und Einbringungskosten zu unterscheiden, die sehr wohl verlangt werden können[39].
5. Irrtumsausschluß (Z14): Unterliegt der Verbraucher bei Angabe seiner Erklärung (Angebot/Annahme) einem Irrtum, so kann dieser immer geltend gemacht werden. Auch sind Klauseln des Inhalts, daß bestimmte Zusagen des Unternehmers über Produkteigenschaften keine wesentliche Beschaffenheit oder Hauptsache betreffen, unzulässig. Dies würde dazu führen, daß eine Anfechtung wegen Fehlen oder Wegfall der Geschäftsgrundlage nicht mehr möglich ist. Wesentliche angepriesene Eigenschaften müssen daher auch tatsächlich vorliegen, oder der Verbraucher kann den Vertrag anfechten.

1.4. Die Fernabsatz- und E-Commerce-Richtlinie (KSchG)

Die Vorschriften der Fernabsatzrichtlinie (Siehe auch [Kresbach]) wurden in das Konsumentenschutzgesetz (hauptsächlich § 5a-i) integriert und treten mit 1.6.2000 in Kraft. Danach treffen den Unternehmer zwei getrennte Informationspflichten und der Konsument erhält ein besonderes Rücktrittsrecht. Weiters bestehen noch Sonderregeln für die Lieferfrist und bei

[38] Geschäfte zwischen zwei Endverbrauchern sind daher nicht erfaßt! Beispiele hierfür wären Tauschbörsen oder Flohmärkte, auch wenn sie im Internet von einer Firma organisiert werden, da der Verkauf/Kauf regelmäßig nicht mit der Firma zustande kommen wird, die hier nur die Rolle eines Vermittlers übernimmt.

[39] Siehe hierzu jedoch Z 15, wonach nur notwendige Kosten verlangt werden dürfen, wenn sich der Verbraucher nach Verzugseintritt zu deren Zahlung verpflichtet.

Mißbrauch von Kreditkarten. Hinsichtlich dieser Schutzbestimmungen ist die Rechtswahl eines nicht EWR-Staates unbeachtlich, wenn ansonsten ein solches Recht anzuwenden wäre (§ 13a Abs. 1).

1.4.1. Anwendbarkeit

Diese Sonderbestimmungen kommen immer dann zur Anwendung, wenn ein Verbraucher mit einem Unternehmer einen Vertrag abschließt, wobei ausschließlich Fernkommunikationsmittel verwendet werden (ein persönliches Treffen genügt daher zum Ausschluß). Es ist nicht nur E-Commerce sondern auch Teleshopping und Versandhandel betroffen. Es bestehen einige Ausnahmen, wobei für einen Teil davon gesonderte Regelungen in Ausarbeitung sind (EU-Fernabsatz-RL Finanzdienstleistungen). Keine Anwendung finden die Bestimmungen auf Bank- und Wertpapierdienstleistungen und Versicherungsgeschäfte, Verträge über Immobilien (doch anwendbar hingegen auf Mietverträge), Warenautomaten und Versteigerungen.

1.4.2. Informationsbereitstellung

Bevor der Konsument seine Vertragserklärung abgibt, müssen ihm einige Informationen zur Verfügung gestellt werden. In der Regel **vor** seinem Angebot, bei einer Werbung des Unternehmers, welche der Konsument nur mehr annehmen muß (echtes Angebot im Rechtssinne), jedoch schon in der Werbung selbst. Alle Vertragsbestimmungen müssen dem Kunden so zur Verfügung gestellt werden, daß er sie speichern und reproduzieren kann. Die bereitzustellenden Informationen sind im Einzelnen:

1. Name und geographische Anschrift des Unternehmers
2. Wesentliche Eigenschaften der Ware oder Dienstleistung
3. Preis inklusive aller Steuern
4. Lieferkosten
5. Einzelheiten zu Zahlung und Lieferung
6. Bestehen des Rücktrittsrechts (sofern dieses nicht durch Gesetz ausgeschlossen ist)
7. Kommunikationskosten über den Grundtarif
8. Bindungsdauer für Angebot und Preis
9. Mindestlaufzeit bei Dauerschuldverhältnissen

Die folgenden Punkte sind ebenso erforderlich, falls nicht der gesamte Vertrag ausschließlich durch den Austausch von E-Mail oder vergleichbarer individueller Kommunikation erfolgte:

10. Die einzelnen technischen Schritte, die zu einem Vertragsabschluß führen (d. h. Hilfe-Seiten, welche den bestell-Vorgang erläutern)
11. Angaben, ob der Vertragstext nach Vertragsabschluß vom Anbieter gespeichert wird und ob er zugänglich sein wird (künftige Einsichtnahmemöglichkeit)
12. Technischen Mittel zur Erkennung / Korrektur von Eingabefehlern vor Bestellungsabgabe
13. Für den Vertragsabschluß zur Verfügung stehenden Sprachen

Durch die E-Commerce Richtlinie kommen noch folgende Zusatzinformationen hinzu, welche leicht, unmittelbar und ständig verfügbar sein müssen, also schon in etwaiger Werbung (Besonderheiten bestehen noch für reglementierte Berufe, wie etwa Ärzte, Rechtsanwälte, Ziviltechniker, etc.):

14. Angaben, die es ermöglichen, schnell mit dem Diensteanbieter Kontekt aufzunehmen und unmittelbar und effizient mit ihm zu kommunizieren, einschließlich seiner E-Mail Adresse
15. Handelsregister- oder gleichwertige Nummer, sofern eine solche Eintragung vorgeschrieben ist
16. Wenn eine Zulassung für die Tätigkeit nötig ist, Angaben zur Aufsichtsbehörde (im Bereich von E-Commerce nur selten anwendbar)
17. Wenn die Tätigkeit der Mehrwertsteuer unterliegt, die Identifikationsnummer (wichtig für Firmenkunden)
18. Sofern Preise angegeben werden, müssen diese klar und unzweideutig ausgewiesen werden und insbesondere angegeben werden, ob Steuern und Versandkosten darin enthalten sind

Bei Hauslieferungen und Freizeitdienstleistungen (siehe Abschnitt 1.4.4) entfallen einzelne dieser Pflichten (Punkte 1-10).

Für E-Commerce bedeutet dies, daß diese Angaben (neben den AGBs; siehe 5.4) einfach abrufbar sein müssen. Es sollten daher direkt auf der Bestellseite diese Informationen wiederholt werden oder ein klar ersichtlicher Link zu diesen plaziert werden.

Handelt es sich um Konsumenten (zwischen anderen Parteien sind abweichende Vereinbarungen möglich), so ist jeder Bestellungseingang unverzüglich auf elektronischem Wege zu bestätigen, d. h. in der Regel per Rück - E-Mail. Dies ist nicht notwendig, falls der gesamte Vorgang ausschließlich per E-Mail oder übere andere individuelle Kommunikation erfolgte.

1.4.3. Informationserteilung

Während der Erfüllung (spätestens mit Lieferung der Ware) müssen dem Konsumenten die oben angeführten Informationen noch explizit zugesandt werden, und zwar schriftlich oder auf einem dauerhaften Datenträger[40]. Zusätzlich sind ihm folgende Informationen zu geben:

1. Erläuterungen zur Ausübung des Rücktrittsrechts
2. Anschrift des Unternehmers, bei der Reklamationen vorgenommen werden können
3. Informationen über Kundendienst und Garantiebedingungen
4. Kündigungsbedingungen bei Dauerschuldverhältnissen

Auch diese Pflicht entfällt bei Hauslieferungen und Freizeitdienstleistungen (siehe unten).

1.4.4. Hauslieferungen und Freizeitdienstleistungen

Unter Hauslieferungen versteht man die Lieferung von Lebensmitteln, Getränken und sonstigen Haushaltsgegenständen des täglichen Bedarfs, sofern sie an den Wohnsitz, den Aufenthaltsort oder den Arbeitsplatz des Verbrauchers im Rahmen regelmäßiger Fahrten geliefert werden (Pizza-Zustellung).

Freizeitdienstleistungen sind Dienstleistungen in den Bereichen Unterbringung und Beförderung (Hotel-, Taxi-Bestellung) sowie Lieferung von Speisen und Getränken und Freizeitgestaltung, wenn sie zu einem bestimmten Zeitpunkt zu erbringen sind (Buffet-Service).

---

[40] Hierfür werden die Anforderungen sehr niedrig angesetzt: Ist ein Ausdruck möglich (z. B. bei E-Mail), so ist dies bereits ausreichend: E-Mail, Disketten, CD-ROMs, etc.

1.4.5. Rücktrittsrecht

Bei einem im Fernabsatz geschlossenem Vertrag kann der Verbraucher innerhalb von 7 Werktagen[41] zurücktreten, wobei die rechtzeitige Absendung der Rücktrittserklärung ausreicht. Eine besondere Form (z. B. Schriftform, wie sonst im KSchG gefordert) ist nicht notwendig (daher auch mündlich bzw. per E-Mail). Hat der Unternehmer seine Pflicht zur Informationserteilung (siehe 1.4.3; Die Informationsbereitstellungspflicht ist hier unerheblich!) nicht erfüllt, so verlängert sich diese Frist auf **3 Monate**. Werden innerhalb dieser Frist die Informationen bereitgestellt, so beginnt die 7-Tage Frist mit Empfang der (nachgereichten) Informationen durch den Konsumenten.

Mit der Rücktrittserklärung ist das gesamte Geschäft rückabzuwickeln. Der Verbraucher erhält geleistete Zahlungen zurück und der Unternehmer die Ware sowie Benützungs- und Wertminderungsersatz. Die Tatsache, daß die Ware nicht mehr im Erstbesitz ist, gilt explizit nicht als Wertminderung. Für den Konsumenten dürfen außer den Kosten der Rücksendung (und dies auch nur bei expliziter Vereinbarung) keine zusätzlichen Kosten auferlegt werden (z. B. Bearbeitungsgebühren). Für Finanzierungskredite in wirtschaftlicher Einheit mit dem Vertrag bestehen Sonderregelungen (gleichzeitiger Rücktritt vom Kreditvertrag). Für Ausverkaufs- oder reduzierte Ware besteht jedoch kein besonderes Rücktrittsrecht.

In folgenden Fällen ist das Rücktrittsrecht ausgeschlossen:

- Dienstleistungen, deren Ausführungen vereinbarungsgemäß innerhalb von 7 Werktagen nach Vertragsabschluß beginnt
- Waren und Dienstleistungen, deren Preis von der Entwicklung der Finanzmärkte abhängt auf die der Unternehmer keinen Einfluß hat
- Sonderanfertigungen nach Kundenspezifikationen
- Verderbliche oder zur Rücksendung ungeeignete Waren
- Entsiegelte Audio-, Video- oder Software-Datenträger
- Zeitungen, Zeitschriften und Illustrierte (nur bei Einzelexemplaren, nicht jedoch bei Abonnements von solchen)
- Wett- und Lotteriedienstleistungen
- Hauslieferungen und Freizeitdienstleistungen (siehe 1.4.4)

1.4.6. Leistungsfrist

Ist nichts anderes vereinbart, so hat der Unternehmer die Leistung innerhalb von 30 Tagen nach der Bestellung des Kunden auszuführen, wenn er das Angebot annimmt. Dies gilt wiederum nicht für Hauslieferungen und Freizeitdienstleistungen. Kann er die Bestellung innerhalb dieser Zeit nicht ausführen oder will er das Angebot überhaupt nicht annehmen, so hat er den Verbraucher davon unverzüglich zu verständigen (unabhängig von der Bestätigung des Bestellungs-Eingangs!) und geleistete Zahlung zurückzuerstatten. Erfolgt dies nicht oder nicht rechtzeitig, wird er eventuell Schadenersatzpflichtig.

[41] Samstag ist hierfür kein Werktag.

1.4.7. Mißbrauch von Kreditkarten

Wenn im Fernabsatz eine Zahlungskarte (hauptsächlich Kreditkarten, aber auch andere) oder deren Daten (=Kreditkartennummer, Ablaufdatum und Name) mißbräuchlich verwendet wird, so kann der Inhaber Rückerstattung verlangen. Die Besonderheit liegt darin, daß er dies vom Aussteller der Karte verlangen kann, unabhängig davon, ob diesen ein Verschulden trifft. Dies gilt sowohl für Unternehmer wie für Konsumenten, doch können Unternehmer dies vetraglich abbedingen, während dies für Konsumenten zwingendes Recht ist. Zu beachten ist, daß dies nur bei sorgfältigem Umgang gilt, d. h. wenn den Inhaber der Karte kein Verschulden trifft[42].

2. Angebot und Annahme bei E-Commerce

Es wird dargestellt, wie bestimmte Formen des Auftretens bei E-Commerce in rechtlicher Hinsicht zu bewerten sind: Was ist in den einzelnen Fällen das Angebot, was die Annahme?

2.1. Webseiten: Werbung oder Angebot?

Werden Waren auf Webseiten angeboten, so entspricht dies in den meisten Fällen dem Katalog eines Versandhauses. Dies bedeutet, daß der Verkäufer zur Stellung von Angeboten einladen will, aber sich nicht in Bezug auf jeden möglichen Interessenten fest binden will. Es ist daher regelmäßig davon auszugehen, daß die angebotenen Waren nicht in unbegrenzter Stückzahl vorhanden sind und ein unbedingter Bindungswille fehlt. Webseiten sind daher nur unverbindliche Anpreisungen. Dies gilt selbst dann, wenn beliebig vervielfältigbare Produkte (z. B. Software mit elektronischer Auslieferung) angeboten werden: Auch hier wird der Verkäufer in der Regel die Kreditwürdigkeit prüfen und daher keine feste Bindung eingehen wollen.

Wählt daher ein Kunde einige Waren aus und legt sie in seinen Warenkorb, schreitet zum "Check-out" und wählt Zahlungs- und Versandart, so wird hiermit ein ausführliches und bindendes Angebot erstellt, dem der Versender zustimmen kann oder nicht. Dies ist insbesondere deshalb wichtig, da Webseiten international zugänglich sind und es der Verkäufer sich oft vorbehält, nur in bestimmte Länder zu liefern (oder vom Gesetz verpflichtet ist, bestimmte Waren in manche Länder nicht oder nur unter besonderen Bedingungen zu liefern).

Die Annahme kann wiederum auf verschiedene Weisen erfolgen: Einerseits kann die Rückmeldung auf der Webseite eine bloße Empfangsbestätigung sein (z. B. "Vielen Dank für Ihre Bestellung"), andererseits aber auch eine explizite Annahme (z. B. "Wir danken für Ihren Auftrag. Ihre Bestellung wird am ??.?? ausgeliefert werden."). In manchen Fällen erfolgt auch eine besondere Bestätigung per E-Mail, die wiederum eine der beiden Formen annehmen kann. Bei der Entscheidung, ob eine Annahme oder lediglich eine Empfangsbestätigung vorliegt, ist darauf abzustellen, wie ein redlicher Empfänger der Mitteilung diese unter Berücksichtigung aller Umstände verstehen darf. Ein guter Hinweis für eine Annahme ist etwa, wenn ein Liefertermin genannt oder die Lieferung fix zugesagt wird. Wendungen der Art "Ihre Bestellung wird in Kürze bearbeitet werden" deuten hingegen auf eine Empfangsbestätigung hin.

[42] Als Verschulden wird z. B. angesehen, wenn die Kreditkartennummer über eine unverschlüsselte Internet-Verbindung übertragen wird.

2.2. "Persönliche Warenkörbe"

Unter einem "persönlichen Warenkorb" wird hier ein Warenkorb verstanden, der für eine ganz bestimmte Person zusammengestellt wird (d. h. in der Regel **nach** einer Anmeldung) und bereits Auskünfte über die Lieferzeit und/oder Verfügbarkeit enthält. Hierbei wird viel eher von einem Angebot auszugehen sein, da Kreditwürdigkeit, Ort des Empfängers etc. bereits feststehen und vom Verkäufer bzw. dessen Computersystem bereits beurteilt werden konnten. Auch kann bei einem modernen Warenwirtschaftssystem davon ausgegangen werden, daß es sich um einen Lagerbestand handelt, der zumindest täglich oder laufend aktualisiert wird. Es kann daher auch eine Bindungswirkung angenommen werden, da (im Gegensatz etwa zu einem Versandkatalog) der Verkäufer nicht zu befürchten braucht, über seine Liefermöglichkeiten verpflichtet zu werden.

Dies kann analog zum Automatenverkauf gesehen werden, bei dem das Angebot an die Allgemeinheit unter der Voraussetzung "solange der Vorrat reicht" gerichtet wird. Auch hier ist beim tatsächlichen Vertragsabschluß keine Person mehr involviert, wie es auch bei E-Commerce (der meist vollkommen automatisch abläuft) der Fall ist. Das Angebot (=Aufstellung des Automaten) entspricht dem Zugänglichmachen der Webseiten, während der Vorrat im Automaten mit der aktuellen Lieferauskunft (und der dahinterstehenden Programmlogik, die entweder ein längere Lieferfrist für Produktion/Bestellung festlegt oder das Produkt als "ausverkauft" markiert) verglichen werden kann. Problematisch kann bei E-Commerce jedoch sein, daß im Gegensatz zu einem Automaten für den Käufer die Aktualität der Lieferauskunft nicht klar erkennbar ist. Doch dürfte auch bei Unklarheiten eher ein Angebot vorliegen, da diese Unklarheit der Erklärung zu Lasten des Unternehmers geht (der sich des mangelhaften Programms bedient). Es ist wieder darauf abzustellen, wie ein redlicher Empfänger die Darstellung verstehen darf: Als allgemeine und ungefähre Angabe der durchschnittlichen Lieferzeit[43] oder als Auskunft über die Möglichkeit und den konkreten Zeitpunkt der Lieferung.

2.3. E-Mail Werbung

Bei einer persönliche adressierten E-Mail wird es sich viel eher um ein Angebot handeln, als um reine Werbung. Wird eine Person direkt angesprochen und ihr ein genügend konkreter Vorschlag unterbreitet, so ist von einem verbindlichen Angebot auszugehen. Auch hier ist freilich zu berücksichtigen, ob sich aus dem Inhalt nicht anderes ergibt ("Angebot freibleibend", "So lange der Vorrat reicht", ...). Handelt es sich hingegen um eine Massenaussendung mit unpersönlichem Inhalt oder ist die Nachricht an eine Mailingliste gerichtet, so liegt höchstens in Ausnahmefällen ein Angebot vor, da von einer Bindung des Absenders nicht ausgegangen werden kann. Hier handelt es sich daher um reine Werbung (und oftmals um Spam).

Schwierig ist die Abgrenzung bei personalisierter E-Mail. Hat man sich beispielsweise auf einer Webseite angemeldet und dort bestimmte Vorlieben angegeben, um ein besser abgestimmtes Service zu erhalten (siehe dazu das Kapitel über Personalisierung), so kann automatisch eine passende E-Mail mit persönlicher Anrede und anderen konkreten Angaben (z. B. bereits ausgefülltes Bestellformular) erstellt werden, die anschließend auch einzeln und persönlich adressiert verschickt wird. Hier sollte vom Anbieter aus jedenfalls klargestellt werden, ob es sich um eine Werbung oder ein Angebot handelt. Ist trotz der persönlichen Anpassung aus dem Text ersichtlich, daß es sich um eine mehrfach verschickte E-Mail handelt oder wird eine große Anzahl von Produkten angeboten, so ist dies ein Hinweis, daß es sich um Werbung handelt. Im Gegensatz dazu ist ein Angebot von

[43] Siehe Amazon.com (http://www.amazon.de; 10.4.2000): „Usually ships within 24 hours."

elektronischen Produkten (die beliebig oft vervielfältigt werden können), eher ein Angebot, wenn es derart individuell abgefaßt ist.

Allgemein kann zusammengefaßt werden, daß es sich bei E-Mail nur selten um ein echtes Angebot handeln wird. Es werden regelmäßig nur händisch und individuell abgefaßte und auf Anfrage hin erstellte Vorschläge Angebote sein, während unverlangt zugesandte E-Mails fast ausschließlich als Werbung anzusehen sind. Problemen bei der Einteilung kann durch entsprechende Formulierung abgeholfen werden.

3. Zugang von Erklärungen

Auch auf elektronischem Wege müssen Erklärungen dem Empfänger zugehen (siehe dazu § 862 ABGB). Hier stellen sich jedoch einige Probleme, die zwar bei gewöhnlichen Käufen auftreten können, jedoch sehr selten sind, wie etwa die automatische Entgegennahme von Erklärungen durch Maschinen. Wann bei verschiedenen Kommunikationsformen nun der maßgebliche Zeitpunkt vorliegt, wird im Einzelnen aufgezeigt.

3.1. E-Mail

Bei E-Mail handelt es sich um eine Kommunikation unter Abwesenden, also einem asynchronen Kommunikationsmedium. Ein Vergleich mit konventionellen Briefen ist möglich. Diese gelten als Zugegangen, sobald sie der Empfänger tatsächlich physikalisch in Händen hält. Zusätzlich gilt als Zugang aber auch die üblichere Form des Einwurfs in einen Postkasten (Allgemein: In den Machtbereich des Empfängers gelangt). Hier sind jedoch einige zeitliche Besonderheiten zu beachten: Ein Zugang liegt dann vor, wenn der Empfänger die Möglichkeit der Kenntnisnahme hat und dies nach der Verkehrsauffassung auch zu erwarten ist. Bei Geschäfts-Postkästen kann daher nur an Werktagen und während der normalen Arbeitszeit ein Zugang erfolgen. Ein Einwurf außerhalb dieser Zeiten bewirkt den Zugang daher erst zu dem nächsten innerhalb dieser Zeiten liegenden Zeitpunkt. Im Gegensatz dazu ist bei Privatpersonen ein Zugang in der Regel täglich tagsüber anzunehmen.

Auf E-Mails übertragen bedeutet dies, daß ein Zugang nur dann vorliegen kann, wenn der Empfänger auch tatsächlich Kenntnis nehmen kann (so auch die E-Commerce RL, die bei bestellungen und Empfangsbestätigungen für den Eingang auf die Abrufmöglichkeit abstellt), also die Mail auf seinem Mailserver eingelangt[44] ist. Die Nicht-Erreichbarkeit dieses Rechners für den Benutzer verhindert den Zugang solange, als dieses Hindernis besteht. Hier besteht das Problem, daß der Absender dies nicht zu erwarten braucht (auch liegt diese Schwierigkeit im Machtbereich des Empfängers, wenn dieser, wie üblich, den Provider bestellt hat). Für den genauen Zeitpunkt ist analog zu Briefen die Geschäftszeit bei Unternehmen bzw. tagsüber bei Privatpersonen maßgeblich.

3.2. Web-Seiten und -Formulare

Beim Ausfüllen von Formularen im WWW bzw. dem zur Verfügung stellen von Webseiten taucht die Frage auf, ob es sich erstens um synchrone oder asynchrone Kommunikation handelt und zweitens, ob eine solche Erklärung überhaupt zugehen kann, da in vielen Fällen keine natürliche Person diese wahrnimmt. Der zweite Fall ist von dem oben (1.1) erläuterten der unbewußten Erklärungsabgabe zu unterscheiden: Hier geht es um den gegensätzlichen Akt, die Entgegennahme einer Erklärung und

[44] Siehe dazu auch § 26a ZustellG, wonach eine Zustellung vorliegt, wenn die Sendung „in den elektronischen Verfügungsbereich des Empfängers gelangt" ist. Hier ist nur die Abwesenheit von der Abgabestelle als aufschiebendes Hindernis angeführt, doch wird dem eine Unmöglichkeit der Abfrage gleichzuhalten sein.

nicht deren Abgabe. Es kommt wieder der Grundsatz zur Anwendung, daß es genügt, wenn einer Erklärung in den Machtbereich des Empfängers gelangt. Eine tatsächliche Kenntnisnahme ist nicht erforderlich. Wird ein technisches Gerät zur Entgegennahme von Erklärungen eingerichtet, so trägt dessen Verwender die damit verbundenen Gefahren. Auch Erklärungen auf Webseiten könne daher echte Erklärungen darstellen.

Meiner Meinung nach handelt es sich bei Ausführungen auf Webseiten, welche statisch bereitgestellt werden, um Erklärungen unter Abwesenden, da eine solche Webseite nicht an einzelne Personen adressiert werden kann und daher ein Zugang zu einem bestimmten Zeitpunkt vom Erklärenden nicht erwartet werden kann. Der Zugang tritt daher unmittelbar mit dem Abruf ein. Es ist jedoch zu beachten, daß ein tatsächlicher Rechtsfolgewillen (bzw. Bindungswillen für Angebot oder Annahme eines Kaufvertrags), der für eine Erklärung notwendig ist, hier nur sehr selten vorliegen wird.

Ähnliches gilt bei dynamisch generierten Webseiten, die auf Anforderung eines Benutzers (ob dieser namentlich bekannt ist oder nicht, ist jedoch unerheblich) hin erstellt werden. Hierbei dürfte es sich ebenso um Erklärungen unter Abwesenden handeln. Im Gegensatz zu Chat (siehe unten) wird im WWW eine sofortige Antwort nicht erwartet, ganz im Gegenteil, es handelt sich um ein zustandsloses Protokoll, bei dem davon ausgegangen wird, daß eine beliebige, und oft lange, Zeit bis zur nächsten Anforderung vergeht. Die Verwendung entspricht im Verkehrsgebrauch eher dem des Briefverkehrs: Antworten (z. B. in Formularen) werden längere Zeit überlegt und geändert, bis sie dann schließlich abgeschickt werden (oder auch nicht). Der Zugang von Erklärungen erfolgt daher mit dem tatsächlichen Eingang in den Machtbereich des Empfängers (Server oder Benutzerrechner). Ob eine Bestätigung erhalten wird (z. B. Antwortseite nach Formular-Übermittlung), ist ohne Bedeutung für den Zeitpunkt und die Tatsache des Zugangs.

Da Server meist rund um die Uhr arbeiten, liegt ein sofortiger Zugang dann vor, wenn eine automatische Verarbeitung erwartet werden kann (der Server ist Adressat). Ergibt sich aus der Erklärung oder den Umständen jedoch, daß eine natürliche Person diese bearbeiten soll, so ist der Zugang erst mit Wiederbeginn der Geschäftszeiten anzunehmen (der Server ist nur ein Kommunikationsmittel ähnlich einem Briefkasten). Hier können sich Probleme stellen, wenn dieses Unterscheidungsmerkmal (gedachter Empfänger: Rechner oder Mensch?) nicht klar ersichtlich ist[45]. Ob die Erklärung jedoch tatsächlich verarbeitet bzw. angezeigt wird, ist unerheblich. Da es sich um Kommunikation unter Abwesenden handelt, hat eine Antwort daher nicht sofort zu erfolgen. Eine angemessene Überlegungszeit (bzw. Verarbeitungszeit) und die Transferzeit für die Antwort sind zu berücksichtigen.

3.3. Chat

Bei dieser, wenn auch synchronen, Kommunikationsform gibt es doch Unterschiede zu einem Telefon. Es kann sich hier durchaus auch um eine schriftliche Kommunikation unter Abwesenden handeln, bei welcher der Transport der Erklärungen eben sehr schnell erfolgt (siehe dafür [Wendel]). Es wird jedoch eher von Erklärungen unter Anwesenden auszugehen sein:

- Daß an einem Chat mehrere Personen teilnehmen ist zwar ein Unterschied zum Telefon, doch dieses wird gleich einem Gespräch unter Anwesenden behandelt und auch hier können in einem Gespräch mit mehreren Personen gleichzeitig rechtsgeschäftliche Erklärungen stattfinden, ohne daß Differenzierungen erfolgen.

[45] Zeitzone, Arbeitszeiten, wo befindet sich der Rechner physikalisch, wo werden die Daten von Menschen verarbeitet, …

- Sollte jemand eine Erklärung im Chat übersehen, da gleichzeitig sehr viele Meldungen einlangen, so entspricht dies direkt dem Überhören, wenn eine große Zahl von Personen gleichzeitig sprechen.
- Auch das von [Wendel] aufgezeigte Problem: Ein Computer stürzt ab und dadurch wird eine eingegangene Meldung nicht mehr angezeigt (und dies für den Sender der Erklärung nicht erkennbar ist), ist von einem Telefonat nicht zu unterscheiden. Auch hier kann es zu einseitigen technischen Störungen kommen, welche für den Sender nicht erkennbar sind.
- Auch die einfache Abwesenheit bei Chat entspricht direkt dem Telefon, wo der Hörer beiseite gelegt wird. Dies kann ebenfalls vom Sprecher nicht erkannt werden.
- Chat dient als eine Art Internet-Ersatz für das Telephon und wird auch auf die selbe Weise verwendet. Die Verkehrsauffassung entspricht daher viel stärker einer synchronen Kommunikation unter Anwesenden.
- Letztlich kann noch technisch eingewendet werden, daß auch bei einem Telephon bei der heutigen Technik keine direkte Verbindung mehr vorhanden ist. Die Töne werden digitalisiert und nach mehrfacher Zwischenspeicherung und Weiterleitung schließlich am anderen Ende wiederhergestellt. Ein qualitativer Unterschied zu einem Chat (Ein Text wird eingetippt, über mehrere Rechner weitergeleitet und am anderen Ende wieder angezeigt) ist nicht erkennbar. Insbesondere werden Texte bei Chat nicht (wenn auch nur kurz) zwischengespeichert (z. B. für bessere Netzwerkauslastung), sondern unverzüglich weitergeleitet.

Eine Erklärung über Chat ist daher sofort zugegangen (unter Anwesenden) und, wenn nichts anderes vereinbart wurde, auch sofort zu beantworten.

4. Erfüllung

Bei E-Commerce ist es nicht nur möglich Verträge abzuschließen, je nach Art des Kaufgegenstandes kann auch die Erfüllung direkt elektronisch erfolgen. Ebenso kann die Zahlung auch gleich Online abgewickelt werden. Hier ist jedoch zu untersuchen, wann tatsächlich die Verpflichtung erfüllt wird, da nicht jede Art von Zahlung eine sofortige Erfüllung (=Leistung des Geschuldeten) bewirkt. Im Hinblick auf die Gefahrtragung ist es auch wichtig festzustellen, wo die einzelnen Leistungen zu erbringen sind.

4.1. Erfüllungsort

Der Erfüllungsort ist der Ort, an dem die Leistung erbracht werden muß. Dies ist bei E-Commerce besonders deshalb wichtig, da sich danach regelmäßig die Maßeinheiten und Währungen bestimmen. Ist also der Erfüllungsort bei einem grenzüberschreitenden Kauf am Sitz der Verkäufers, so ist der geschuldete Betrag in der dortigen Währung zu bezahlen und die zu liefernde Menge nach dortigen Maßen[46] zu berechnen[47]. Der Erfüllungsort kann im Vertrag selbst frei festgelegt werden (nach dem Gesetz liegt eine Holschuld vor, d. h. der Gläubiger muß die Leistung am Schuldner-Wohnsitz abholen). Bei einem Versendungskauf, wie er bei E-Commerce regelmäßig vorliegen wird, besteht

[46] Wichtig etwa für Rechtsgeschäfte mit den USA oder England, wo noch immer nicht-metrische Maßsysteme vorgeschrieben bzw. in Verwendung sind!

[47] Hierbei ist jedoch zu beachten, daß der Erfüllungsort auch auseinanderfallen kann: Erfüllung der Lieferung der Ware am Wohnsitz des Konsumenten, aber Erfüllung der Geldschuld am Sitz des Verkäufers.

jedoch bezüglich der Ware eine Schickschuld[48]. Dies bedeutet, daß der Leistungsort der Wohnsitz des Schuldners bleibt, diesen aber die Verpflichtung trifft, den Schuldinhalt an den Gläubiger abzusenden (welcher auch die Transportgefahr zu tragen hat). Geldschulden sind in der Regel qualifizierte Schickschulden, wobei der Schuldner auch die Kosten und die Gefahr der Versendung tragen muß.

Für E-Commerce ergeben sich daraus die folgenden Punkte: Der Versender (=Verkäufer) muß die Ware an den Käufer abschicken, dieser trägt die Kosten und Gefahren des Versands. Der Konsument (=Käufer) muß das Geld zum Verkäufer schicken, wobei er die Kosten und Gefahr trägt (zum Inhalt siehe gleich unten). Die Menge ist nach Maßeinheiten des Versenders zu berechnen, während die Währung nach dem Käufer festgelegt ist (hierfür besteht jedoch praktisch immer eine explizite Vereinbarung).

Beim Versand der Ware in elektronischer Form (z. B. als E-Mail attachment) trägt daher der Käufer die Gefahr des Verlusts der Mail. Wird die Mail (z. B. wegen voller Mailbox) von seinem Mail-Provider nicht angenommen, so hat der Versender seine Leistung bereits erfüllt. Wurde vereinbart, daß der Käufer die Daten per FTP von einem Rechner des Verkäufers abholt, so ist mit der Bereitstellung (=Gültigkeit von Name und Paßwort) und der Erreichbarkeit des Rechners vom Internet aus die Leistung bewirkt. Verbindungsprobleme oder Schwierigkeiten beim Download treffen daher auch hier den Käufer. Eine Bringschuld (Speicherung der Daten auf einem Rechner des Käufers) wird nur höchst selten vorkommen. In diesem Fall trifft die Gefahr von Verbindungsproblemen der Verkäufer, doch muß der Käufer hier für die Zugangsmöglichkeit sorgen.

4.2. Leistungsinhalt bei Geldschulden

Bei einer Geldschuld ist grundsätzlich das gesetzliche Zahlungsmittel zu verwenden, und zwar in Form von Geldscheinen und Münzen. Dies bedeutet bei einem Versendungskauf, daß echte Geldscheine mit der Post verschickt werden müßten. Da dies unpraktisch und mit relativ hoher Gefahr verbunden ist, wird meist eine andere Zahlungsart vereinbart. Alternativ kann davon ausgegangen werden, daß der Gläubiger mit Zahlung durch Überweisung einverstanden ist, wodurch die Leistung mit der Gutschrift (und der Verfügbarkeit!) auf dem (richtigen: die Gefahr von Falschüberweisungen trägt der Käufer, da qualifizierte Schickschulden) Konto des Empfängers eintritt.

Ist die Schuld zwar im Inland (Bsp.: Versendungskauf) aber in ausländischer Währung zu leisten, so kann der Schuldner selbst bestimmen, ob er in dieser Währung oder in inländischem Geld bezahlen will. Es kann jedoch vereinbart werden, daß “effektiv” gezahlt werden muß, wodurch eine echte Fremdwährungsschuld entsteht.

Von besonderer Bedeutung ist bei E-Commerce die Bezahlung per Kreditkarte. Hier wird die Leistung erst bei der Abrechnung erbracht, welche üblicherweise monatlich erfolgt. Der Verkäufer sollte daher explizit mit Zahlung über eine Kreditkarte einverstanden sein, da er durch diese erstens zusätzliche Kosten zu tragen hat (Gebühr der Kreditkartenfirma) und der Käufer sonst sehr leicht in Zahlungsverzug kommt. Rechtlich gesehen wird hier die Schuld auch nicht durch den Käufer erfüllt, sondern über eine Anweisung an die Kreditkartenfirma. Der Kunde trägt daher das Risiko von deren Konkurs. Allgemein ist ein Verkäufer auch aus diesem Grunde nicht verpflichtet, Kreditkarten zu akzeptieren.

[48] Siehe etwa folgendes Beispiel in den USA, wo der Versand von Bier über Bundesstaatsgrenzen besondere Probleme aufwirft (es handelte sich um die Bestellung eines Minderjährigen): Die Klage wurde wegen Unzuständigkeit zurückgewiesen, da Verkaufsort ein anderer Bundesstaat war. (http://www.lawnewsnetwork.com/stories/A17537-2000Mar1.html; 6.4.2000).

5. AGB's

In vielen Fällen wollen Anbieter Verträge nur zu bestimmten Bedingungen abschließen. Um diese nicht jedesmal besonders vereinbaren zu müssen, existieren AGBs (Allgemeine Geschäftsbedingungen). Wann diese wirksamer Vertragsbestandteil sind, bzw. welche Teile davon, wird hier diskutiert.

5.1. Begriffsbestimmung

Bei AGBs handelt es sich um vorformulierte Vertragsbedingungen und Klauseln, die für eine Vielzahl von Verträgen verwendet werden. Typischerweise schließt ein Großteil aller Unternehmer nur zu ihren AGBs ab. Dies dient der Rationalisierung und Vereinheitlichung der Geschäfte, wird aber auch dazu verwendet, dem Kunden gegenüber nachteilige Bestandteile zu integrieren. Ein Problem ergibt sich daraus, daß die Kunden praktisch immer nur die eine Wahl haben, die AGBs entweder zu akzeptieren oder keinen Vertrag abschließen zu können. Von AGBs sind Vertragsformblätter zu unterscheiden, wo bis auf einige Bestandteile der komplette Vertrag fertig vorgedruckt ist. Sie sind jedoch genauso wie AGBs zu behandeln.

5.2. Wirksamkeit

Da der Unternehmer keine Möglichkeit hat, verbindliche Regeln für den Kunden aufzustellen, liegt der Rechtsgrund für die Wirksamkeit von AGBs ausschließlich in einer beiderseitigen Vereinbarung. Dies bedeutet jedoch auch, daß der Kunde explizit darauf hingewiesen werden muß, daß der Unternehmer nur unter seinen AGBs abschließen will und auch tatsächliche Einsichtnahme möglich ist[49]. Die oft geübte Praxis, daß AGBs auf der Rückseite der Rechnung oder von Lieferscheinen aufgedruckt sind, hat daher keine rechtliche Wirkung. Der Vertrag kommt zuerst zustande und anschließend wird eine Rechnung ausgestellt, weshalb die AGBs nicht Bestandteil des Vertrags wurden[50].

5.3. Ungültige Klauseln

Aufgrund der starken faktischen Benachteiligung von Konsumenten durch AGBs bestehen besondere Vorschriften, wonach einzelne Bestandteile ungültig sein können. Hier ist zu beachten, daß die normale Wirkung, daß der Vertrag anfechtbar oder anpassbar wird, nicht eintritt, sondern lediglich die verbotene Bestimmung automatisch nicht als Bestandteil des Vertrags angesehen wird (der Rest bleibt unberührt).

- § 864a ABGB: Nach diesem Paragraph sind AGB-Bestimmungen ungewöhnlichen Inhalts, die den anderen Vertragspartner benachteiligen, unwirksam, wenn er nicht mit ihnen den Umständen nach rechnen mußte. Sie können jedoch gültig enthalten sein, wenn besonders auf sie hingewiesen wird oder sie optisch hervorgehoben sind (z. B. Fettdruck). In langen Texten "verborgene" Bestimmungen sind daher unwirksam, wobei besonders auf die optische Gestaltung ("äußeres Erscheinungsbild") abgestellt wird.
- § 879 Abs. 3 ABGB: In AGBs enthaltene Bestimmungen sind jedenfalls nichtig, wenn sie unter Berücksichtigung aller Umstände einen Teil gröblich benachteiligen und nicht die Hauptleistungen (Kaufvertrag: Ware und Preis) betreffen. Eine solche Benachteiligung liegt dann vor, wenn ein

[49] Siehe dazu § 73 Abs. 1 GewO: AGBs müssen in den Geschäftsräumen ausgehängt werden.

[50] Eine Ausnahme besteht bei regelmäßiger Geschäftsbeziehung. Hier wird nach längerer Praxis (aufgrund der früheren Rechnungen) die Wirksamkeit bejaht.

grobes Mißverhältnis zwischen den gegenseitigen Leistungen besteht. Im Unterschied zum KSchG sind hier Hauptpunkte des Vertrages ausgeschlossen (also etwa auch Zahlungsort oder Währung beim Kauf, da diese einen der Hauptpunkte betreffen!).

- § 915 HS 2 ABGB: Hier ist eine Unklarheitenregel festgelegt: Bedient sich eine Seite einer unklaren Formulierung, so wird sie zu seinen Ungunsten ausgelegt. Dies wird insbesondere bei AGBs sehr streng angewendet.
- § 6 Abs. 3 KSchG: Unklare oder unverständliche Bestimmungen in AGBs oder Vertragsformblättern sind unwirksam. Dies betrifft jedoch nur Verbraucherverträge, während die obigen Bestimmungen grundsätzlich gelten.

5.4. Anwendbarkeit bei E-Commerce

Sollen AGBs bei E-Commerce wirksam verwendet werden, so ist es notwendig, explizit auf sie hinzuweisen, und zwar vor Vertragsabschluß. Dies bedeutet, daß der Kunde vor Abgabe seiner Erklärung (meist Bestellung = Anbot) darauf aufmerksam zu machen ist, daß AGBs Anwendung finden sollen. Weiters muß ihm die Einsichtnahme ermöglicht werden, z. B. durch einen Link auf eine entsprechende Seite. Nach der E-Commerce RL muß der Kunde die Möglichkeit haben, sie zu speichern und zu reproduzieren (was bei Webseiten immer gegeben ist). Es ist jedoch nicht notwendig, daß der Benutzer sich "durchklicken" muß, um die Bestellung abschicken zu können[51]. Ein expliziter Hinweis auf der letzten Webseite, von der aus die Erklärung endgültig abgeschickt wird, ist ausreichend und empfehlenswert. Auch hier sind ungewöhnliche Bestandteile optisch hervorzuheben, um sie gültig zu vereinbaren.

In Bezug auf die verwendete Sprache ist zu beachten, daß fremdsprachige AGBs nicht grundsätzlich unverständlich und ungültig sind. Es wird hier vielmehr vom Verständnis eines dieser Sprache Mächtigen auszugehen sein[52]. Insbesondere wird die englische Sprache in vielen Fällen zu akzeptieren sein. Es ist jedoch auf eine klare und einfache Abfassung zu achten. Sogenanntes "Legalese" kann dazu führen, daß eine sonst zumutbare Fremdsprache (aber auch deutsche AGBs bei verhältnismäßig stärkerer Ausprägung) nicht mehr gültig vereinbart werden können.

6. Literatur

6.1. Allgemein

Kilches, Ralph: Electronic Commerce Richtlinie. Medien und Recht 1/99 (17. Jahrgang) 3ff

Koziol, Helmut, Welser, Rudolf: Grundriß des bürgerlichen Rechts. Band I: Allgemeiner Teil und Schuldrecht. 10. Auflage. Wien: Manz 1995

Kresbach, Georg: E-Commerce. Nationale und internationale Rechtsvorschriften zum Geschäftsverlehr über elektronische Medien. Wien: Linde 2000

Mohr, Martina: KSchG-Novelle 1999 - Verbraucherschutz im Fernabsatz. Ecolex 11/1999, 755ff

[51] Siehe dazu [Wendel]: Im Internet hat der Kunde die Möglichkeit, die AGBs in Ruhe zu studieren, ohne zur Unterschrift gedrängt zu werden. Es sollte daher keine Verschärfung im Gegensatz zu Papier-Verträgen stattfinden.

[52] Ist die Webseite nur für Inländer gedacht, wird eine Beherrschung gleich der Muttersprache zur Auslegung zu verwenden sein. Sind die AGBs jedoch für internationalen Gebrauch bestimmt, so wird die Schwelle auf gute Kenntnisse als Fremdsprache festzulegen sein.

Mohr, Martina: Elektronischer Verkauf - Verbraucherschutz im Fernabsatz. Ecolex 4/1999, 247ff

Wendel, A. Dominik: Wer hat Recht im Internet? Ein juristischer Leitfaden. Aachen: Shaker Verlag 1997

6.2. Rechtsvorschriften

ABGB: Allgemeines bürgerliches Gesetzbuch (ABGB) vom 1. Juni 1811 JGS 946 idF BGBl I 1999/164

EVÜ: Europäisches Vertragsstatutübereinkommen. Übereinkommen über das auf vertragliche Schuldverhältnisse anzuwendende Recht BGBl III 1998/208

Konsumentenschutzgesetz: Bundesgesetz vom 8. März 1979, mit dem Bestimmungen zum Schutz der Verbraucher getroffen werden (Konsumentenschutzgesetz - KSchG), BGBl 1979/140 idF BGBl I 1999/185

UN-Kaufrecht: Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenkauf, BGBl 1988/96[53]

IPRG: Bundesgesetz vom 15. Juni 1978 über das internationale Privatrecht (IPR-Gesetz), BGBl 1978/304 idF BGBl I 1999/18

Fernabsatz-Richtlinie: Richtlinie 97/7/EG des Europäischen Parlamentes und des Rates vom 20. Mai 1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz. Amtsblatt der Europäischen Gemeinschaften ABl. L 144/19; 4.6.1997

E-Commerce Richtlinie: Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den elektronischen Geschäftsverkehr") ABl. L 178/1; 17.7.2000

[53] Beachte die Erklärung der Vereinigten Staaten, wonach das UN Kaufrecht in Beziehung auf die USA nur dann zur Anwendung kommt, wenn auch der andere Staat dem Übereinkommen beigetreten ist, aber nicht bei Verweisung durch das IPR auf das Recht eines Vertragsstaates.

V. Domain Names

Ein Hauptaspekt (aber nicht der alleinige) von E-Commerce sind Online-Shops. Diese bedürfen zur Auffindbarkeit im Internet eines Domainnamens, welcher weltweit eindeutig sein muß. Dies bringt besondere Probleme mit sich, da bisher viele Unternehmen mit gleicher Bezeichnung gleichzeitig bestehen konnten, solange sich ihre Geschäftsbereiche oder ihr Einzugsgebiet nicht überlappten (und auch sonst in besonderen Fällen). Es kann daher für ein Unternehmen unmöglich sein, seinen eigenen Namen zu verwenden, da dieser bereits von jemand anderem registriert wurde. Es bestehen in diesem Fall zwei Möglichkeiten: Die Verwendung eines anderen Namens oder der Versuch, diesen Domainnamen zu erlangen. Letztere Variante hat auch praktisch eine große Bedeutung, da es viele Personen gibt, welche die Namen bekannter Firmen registriert haben, um diese zu einem späteren Zeitpunkt gehen hohe Summen an diese Unternehmen zu verkaufen.

1. Einleitung

Im ersten Abschnitt wird kurz der technische Hintergrund erläutert, anschließend dann die wichtigsten rechtlichen Aspekte: Namensrecht, Wettbewerbsrecht und Markenrecht. Mit ihnen ist es möglich, sich gegen Domain-Grabbing, dem „Wegschnappen“ eines Domainnamens, zu wehren. Im Anschluß werden noch einige besondere Aspekte untersucht, wobei insbesondere die Verwendung beschreibender Namen oder Gattungsbezeichnungen zur Zeit noch umstritten ist. Als Abschluß wird noch das Streitbeilegungsverfahren der ICANN erläutert, welches trotz seiner Neuigkeit von enormer praktischer Bedeutung hat (ca. 5000 Entscheidungen im ersten Jahr). Ob sein Anwendungsbereich, aber auch die davon erfaßten Fälle, ausgeweitet werden, wird sich erst in der Zukunft entscheiden.

2. Technische Realisierung

Das Domain Name System (DNS; [Mockapetris]) dient hauptsächlich dazu, Hostnamen in Internet-Adressen umzuwandeln, da Menschen sich Namen viel leichter merken als Zahlen. Es können jedoch auch noch andere Informationen gespeichert bzw. abgefragt werden. Ein Beispiel hierfür ist die Abfrage von Mailservern.

2.1. Aufbau von Domain Namen

Der Bereich aller Domain Namen ist hierarchisch in Form eines Baumes (directed acyclic graph) aufgebaut. Es handelt sich hier jedoch nur um eine logische Struktur, welche von der physikalischen Netzwerksstruktur vollständig unabhängig ist. Jeder Knoten dieses Baumes entspricht einer Menge an Ressourcen (welche auch leer sein kann) und besitzt einen Namen, der von allen Bruderknoten unterschiedlich ist. Der Namen eines Knoten kann zwischen 1 und 63 Zeichen enthalten, wobei nur Buchstaben (Groß-/Kleinschreibung wird ignoriert!), Ziffern und der Bindestrich erlaubt sind. Namen müssen mit einem Buchstaben beginnen sowie mit entweder einem Buchstaben oder einer Ziffer enden.

Ein Domain-Name setzt sich aus der Folge aller Knotennamen bis zur Wurzel des Baumes zusammen, wobei die Knoten von unten nach oben gelesen und durch einen Punkt getrennt werden. Gemeinsame Wurzel ist ein leerer Knoten (der einzige Knoten mit einem Namen der Länge 0). Wird der gesamte Weg angegeben (z. B. "www.fim.uni-linz.ac.at."), so spricht man von einem absoluten Namen, ansonsten von einem relativen (z. B. "www.fim"). Sie können dadurch unterschieden werden, daß absolute Namen immer mit einem Punkt enden. Bei relativen Namen wird zur Erzeugung vollständiger (=absoluter) die Standard-Domäne angehängt (z. B. ".uni-linz.ac.at.").

Auf der obersten Ebene (direkt unter dem gemeinsamen leeren Knoten) befinden sich die sogenannten "generic Top-Level Domains" (gTLD), von denen zur Zeit 7 Stück existieren (com, int, edu, gov, mil, org und net) sowie sehr viele Länder-spezifische (country-code: ISO-3166-1: at, us, de, ...; ccTLD) existieren. Zusätzliche TLDs wurden zwar bereits genehmigt (aero, biz, coop, info, museum, name, pro), doch existieren noch (Ende Jänner 2001) keine hierfür zuständigen/berechtigten Registrierungsstellen. Weitere TLDs wurden beantragt, aber entweder abgewiesen oder noch nicht darüber entschieden. Für deren Zulassung bzw. der Zuteilung von Registrierungsstellen ist die ICANN (siehe 2.5 und 7) zuständig.

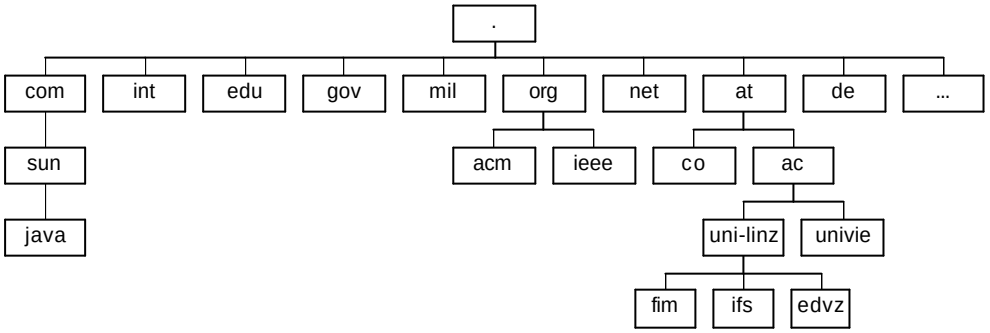


Abbildung 1: Der Domain Baum

2.2. Name Server

Name Server sind jeweils für einen Abschnitt des Domain-Baumes zuständig (für den sie "authoritative anwers" liefern; andere Server liefern lediglich zwischengespeicherte Daten) und speichern die zugehörigen Informationen. Diese Abschnitte ("zone") können sich nicht überlappen. Probleme ergeben sich an den unteren Schnittstellen: Befindet sich der Name-Server für den darunter liegenden Bereich in diesem Bereich, so hat die darüber liegende Zone zusätzliche Informationen zu speichern ("glue"). Typischerweise existieren für jede Zone zumindest zwei Name Server, wobei sekundäre Server ihre Daten in regelmäßigen Abständen vom primären Server beziehen.

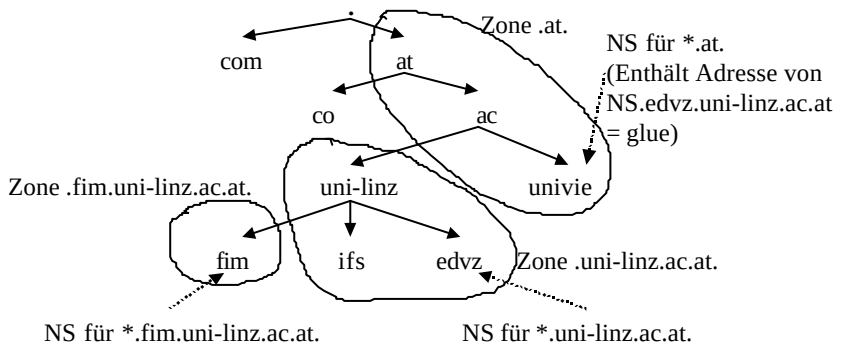


Abbildung 2: Zonenaufteilung des Domain Baumes

Für TLD stellt sich ein gewisses Problem: Woher erhält man die Adressen der für diese zuständigen Nameserver? Hierfür existieren mehrere Root-Nameserver, welche über die ganze Welt verteilt sind (13 Stück; 10 x USA, England, Japan und Schweden; a.root-server.net bis m.root-server.net). Diese werden (inhaltlich) von der ICANN kontrolliert.

Jede Domain muß bei der darüber liegenden Domain registriert werden (wofür Registrierungsstellen existieren, sowohl für generische TLDs als auch für nationale). Ein Firma hat sich daher an eine Registrierungsstelle zu wenden, um die Domain "gadget.com" zugeteilt zu erhalten. Für die Erstellung einer Subdomain ist die Genehmigung von höheren Domains jedoch **nicht** notwendig. So kann etwa die obige Firma mit dem Domain Namen "gadget.com" ohne Genehmigung ihres Providers oder der Registrierungsstelle die Domains "www.gadget.com", "production.gadget.com" oder "test.gadget.com" erzeugen[54].

2.3. Umwandlung Name ⇒ IP-Adresse

Hierbei handelt es sich um die häufigste Abfrage. Um sie durchführen zu können, muß ein Rechner zumindest einen einzigen Nameserver kennen (wird bei Konfiguration eingestellt). Kennt dieser Nameserver den gewünschten Namen, so liefert er sofort die Adresse zurück. Wenn nicht, so existieren zwei Möglichkeiten: Iterative und rekursive Suche:

- Iterative Suche: Der Nameserver liefert die Adresse eines anderen Nameservers zurück, welche dem gesuchten Namen seines Wissens nach am nächsten liegt. Im schlimmsten Fall ist dies einer der Root-Nameserver. Der Client muß sich dann mit seiner Anfrage selbst an diesen neuen Nameserver wenden. Diese Suche ist von jedem Nameserver zu implementieren.
- Rekursive Suche: Der Nameserver erkundigt sich selbst bei anderen Nameservern und liefert anschließend die Anwort an den Client zurück. Diese Suche ist optional. Nameserver weit oben in der Hierarchie führen meist keine rekursive Suche aus (z. B. top-level Nameserver, aber auch der NS der Universität Wien, welche für die Domain "at" zuständig ist).

2.4. WHOIS-Datenbank

Es handelt sich hierbei um eine Datenbank von **europäischen** Internet-Netzwerken (Zuteilung von IP-Adressen bzw. Adressräumen), deren Domain Namen, der zugehörigen Kontaktpersonen und Regeln für IP-Routing. Es handelt sich nicht um eine Registrierungsstelle; es werden keine Domain-Namen vergeben. Vielfach greift die zentrale Datenbank auf Sub-Datenbanken der einzelnen Länder zu, in welchen die lokalen Daten gespeichert werden (so sind etwa die Daten über .at bei der nic.at gespeichert).

Für Endbenutzer ist hauptsächlich die Abfrage nach einem Domain wichtig, etwa um herauszufinden, für wen dieser bei welcher Registrierungsstelle registriert ist

2.4.1. Beispiels-Abfrage: uni-linz.ac.at (Ausschnitt):

```
domain: uni-linz.ac.at
descr: [organization]:Johannes Kepler Universitaet Linz
descr: [street address]:Altenbergerstrasse 69
descr: [postal code]:A-4040
descr: [city]:Linz
```

[54] Unter Umständen benötigt sie jedoch die Mitarbeit des Providers, falls sich (wie oft der Fall) der Nameserver für die Domain „gadget.com" dort befindet.

```
descr: [country]:Austria
descr: [phone]:+43 732 2468
descr: [fax-no]:+43 732 2468 8688
descr: [e-mail]:domain-admin@uni-linz.ac.at
admin-c: WM554850-NICAT
tech-c: GH561572-NICAT
tech-c: FW731349-NICAT
zone-c: WM554850-NICAT
nserver: alijku01.edvz.uni-linz.ac.at
nserver: alijku02.edvz.uni-linz.ac.at
nserver: ns5.univie.ac.at
remarks: 140.78.2.62
remarks: 140.78.3.62
remarks: 193.171.255.77
mnt-by: AT-DOM-MNT
changed: 20010111 17:08:44
source: AT-DOM

person: Wilfried Maschtera
address: Johannes Kepler Universitaet Linz
address: Zentraler Informatik Dienst
address: Altenbergerstrasse 69
address: A-4040 Linz
address: Austria
phone: +43 732 2468.431
fax-no: +43 732 2468.9397
e-mail: Wilfried.Maschtera@zid.uni-linz.ac.at
nic-hdl: WM554850-NICAT
nic-hdl-ripe: WM164-RIPE
mnt-by: AS1205-MNT
changed: 20010111 17:08:36
source: AT-DOM
```

2.4.2. Beschreibung einzelner Felder

- Admin-c: Kaufmännische Ansprechperson
- Tech-c: Technische Ansprechperson für das Netzwerk der Domäne
- Zone-c: Technische Ansprechperson für den Betrieb der Nameserver
- Mnt-by: Wer für die Eintragung der Daten zuständig/berechtigt ist
- Nic-hdl: Eindeutige Kurzbezeichnung einer Person (unter diesem Kürzel gespeichert)

2.5. ICANN

Die ICANN (Internet Corporation for Assigned Names and Numbers) wurde im Oktober 1998 gegründet. Es handelt sich um eine gemeinnützige private Gesellschaft. Sie ist zuständig für:

- Das Internet Domain Name System
- Die Zuteilung von IP-Adressen / IP-Adress-Räumen
- Die Zuteilung von Protokoll-Parametern (z. B. feste Service-Nummern) und Standardisierung von Protokollen

- Management der Root-Nameserver (nur Daten; Hardware und Betrieb erfolgt durch verschiedenen Organisationen!)

Es werden jedoch keine konkreten Leistungen erbracht: Es können keine Domain Namen registriert werden, noch werden Streitigkeiten über solche vor ihr ausgetragen. Sie ist vielmehr hauptsächlich für die Erstellung von Standards und die Koordination zuständig.

Die Leitung besteht aus einem 19 Personen-Vorstand, wobei 9 (z. Z. nur 5) von den weltweiten Internet-Benutzern gewählt werden und die restlichen von drei Teilorganisationen (Address Supporting Organization, Domain Names Supporting Organization, Protocol Supporting Organization) ernannt werden.

3. Namensrechtlicher Schutz

Der namensrechtliche Schutz ist ein Persönlichkeitsrecht, das sowohl natürlichen als auch juristischen Personen zusteht. Nicht nur der eigentliche (bürgerliche) Name ist geschützt, sondern auch Decknamen und Etablissementbezeichnungen (aber auch Abkürzungen und Namensbestandteile sofern sie eigene Namensfunktion besitzen).

Rechtsfolgen der Verletzung sind ein Unterlassungsanspruch und bei Verschulden auch Schadenersatz. Obwohl nicht ausdrücklich erwähnt, wird auch ein verschuldensunabhängiger Beseitigungsanspruch enthalten sein ([Aicher]).

Zuerst stellt sich die Frage, ob die Verwendung einer Zeichenfolge als Domainname überhaupt in den Schutzbereich des Namensrechtes fällt. Vor allem in Deutschland (durch Gerichte; in Österreich aber auch durch einen Teil der Lehre) wurde die Meinung vertreten, daß Domainnamen nicht mit dem bürgerlichen Namen zu vergleichen sind, sondern eher mit Telefonnummern und daher keinen Schutz genießen. Domainnamen dienen jedoch vor allem auch dazu, die hinter den Webseiten stehende Person zu identifizieren und werden auch vielfach so verwendet (etwa durch Eingabe eines vermuteten Domainnamens durch einen suchenden Benutzer, welcher vom Firmennamen abgeleitet ist). Sowohl in Deutschland wie auch in Österreich ist nun aber die Namensfunktion von Domainnamen allgemein anerkannt ([Schanda 1998], [Schanda 2000 § 43]).

3.1. Namensgebrauch

Das Namensrecht schützt sowohl gegen den Gebrauch des Namens durch jemand anderen, als auch gegen die Bestreitung der Rechtmäßigkeit der Führung des eigene Namens. Entgegen manchen Auffassungen (Siehe OLG Düsseldorf in [Schanda 1999]) kann meines Erachtens in der Anmeldung eines Domainnamens keine automatische Leugnung des Namensrechts Dritter gesehen werden. Es ergibt sich lediglich eine tatsächliche Ausschlußwirkung von der Verwendung im Internet, doch wird in der Regel damit nicht das Recht jemandes Anderen bestritten, diesen Namen berechtigterweise zu führen. Andernfalls wäre es unmöglich, einen Namen als Domainname zu verwenden, welcher von zwei Personen geführt wird, da jeder von ihnen automatisch das Recht des Anderen bestreiten würde. Es bleibt daher nur der tatsächliche Gebrauch des Namens als Verletzungshandlung übrig.

Ein Name wird nur dann gebraucht, wenn er zum fraglichen Namen entweder identisch oder zumindest ähnlich ist. Die äußerste Grenze sind Namen, die lediglich einen ähnlichen Klang besitzen. Hier kommt es auf das Identitätsinteresse des Verletzten an: Er soll nicht mit dem Anderen

verwechselt werden und es soll keine wechselseitige Zuschreibung von Handlungen oder Leistungen erfolgen. Siehe dazu auch unten.

Ein Gebrauch eines Namens liegt zweifellos vor, wenn unter diesem Domainnamen eine Webseite erreichbar ist. Doch auch schon die Registrierung alleine ist ein Gebrauch ([Mayer-Schönberger/Hauer]), da der verwendete Name auf mehreren Rechnern eingetragen wird (z. B. WHOIS-Datenbank, aber auch auf den Nameservern). Dies ist analog zu dem Fall, daß ein Name als Markenzeichen registriert wird: Auch dort liegt schon bei der Registrierung, noch vor der Verwendung im Verkehr, ein Namensgebrauch vor.

3.2. Unbefugtheit

Unbefugt ist der Gebrauch eines Namens dann, wenn er nicht auf einem eigenen Recht beruht, das Recht von dem (oder einem) Berechtigten eingeräumt wurde, oder der eigene Name in unlauterer Absicht verwendet wird. Einschränkungen ergeben sich jedoch bei Wahlnamen (z. B. Decknamen, geschäftliche Kennzeichen): An diese werden strengere Anforderungen gestellt, da sie frei ausgewählt werden können. Sie sind daher Zwangsnamen (z. B. bürgerlicher Name) unterlegen. Zwischen Namen der gleichen Stufe (d. h. zwei Zwangsnamen oder zwei Wahlnamen) gilt das Prioritätsprinzip. Dies kann problemlos auf Domainnamen übertragen werden: Besitzen beide Parteien gleiche Berechtigung, so gewinnt derjenige, der diesen Namen zuerst eintragen ließ.

3.3. Beeinträchtigung schutzwürdiger Interessen

Ein Abwehranspruch ist nur dann gegeben, wenn der unbefugte Gebrauch des Namens auch schutzwürdige Interessen des Verletzten beeinträchtigt. Es ist jedoch schon eine ideelle Beeinträchtigung ausreichend (wirtschaftliche oder rechtliche Gefährdung muß nicht gegeben sein). Der Schutz soll zur Unterscheidung der Personen und dem Schutz ihrer Individualität dienen. Konkrete Verwechslungsgefahr ist nicht erforderlich, doch muß zumindest ein Anschein ideeller oder wirtschaftlicher Beziehungen bestehen. Entscheidend ist die Wirkung auf das Publikum, d. h. bei Domainnamen darauf, ob der "durchschnittliche"[55] Internet-Benutzer solche Beziehungen vermuten würde. Dieses Interesse muß auch schutzwürdig sein, was bei geschäftlichen Kennzeichen nur dann vorliegt, wenn es um Beeinträchtigungen von Geschäftsinteressen geht.

Ein besonderer Fall liegt noch bei besonders berühmten Namen vor: Eine berühmte Marke mit umfassendem Bekanntheitsgrad, die das Unternehmen selbst bezeichnet (und nicht nur Waren desselben), ist auch gegen Verwässerung geschützt (siehe dazu auch Abschnitt 5.3). Es kann daher einer gleichnamigen Person die Verwendung dieses Namens als Domainname untersagt werden, selbst wenn diese hierzu berechtigt ist. Dies wurde in Deutschland auch bereits zwei Mal entschieden: Sowohl Herr Krupp als auch Herr Shell mußten die Verwendung der Domains "krupp.de" bzw. "shell.de" unterlassen. Hier ist jedoch erforderlich, daß der eigene Name auf unlautere Weise verwendet wird oder es sich nur um einen ähnlichen Namen handelt, etwa um die Bekanntheit des Namens für sich auszunutzen. Ansonsten siehe den wettbewerbsrechtlichen Schutz, der freilich nur bei Handeln im geschäftlichen Verkehr und Gleichartigkeit der Waren greift!

[55] Ein deutsches Gericht führte aus, daß es keinen „durchschnittlichen" Internet-Benutzer gebe, da sehr viele verschiedene Benutzergruppen mit unterschiedlichem Verhalten existieren. Es verwendete daher zur Beurteilung eine mehr oder weniger beliebige Gruppe (und wendete die eigenen Gewohnheiten zur Beurteilung an).

4. Wettbewerbsrechtlicher Schutz

Für den wirtschaftlichen Bereich existiert ein eigener Schutz durch das Gesetz gegen den unlauteren Wettbewerb. Es wurde nicht für die Anwendung auf Domainamen geschaffen, doch ist es auch hierfür geeignet. Wichtig sind hier die § 1 (Generalklausel) und § 9 Abs. 1 (Schutz von Kennzeichen eines Unternehmens; siehe [Mayer-Schönberger/Hauer]).

4.1. Irreführung

Gemäß § 9 Abs. 1 UWG ist es verboten, im geschäftlichen Verkehr einen Namen, eine Firma, die besondere Bezeichnung eines Unternehmens, oder eine registrierte Marke so zu benützen, daß es zu einer Verwechslung mit dem Namen, der Firma oder der Bezeichnung eines anderen Berechtigten kommen kann. Die Rechtsfolge hierfür ist ein Unterlassungsanspruch und bei wissentlicher (oder fahrlässiger Unkenntnis) auch Schadenersatz.

Unter "geschäftlichem Verkehr" wird jede auf Erwerb gerichtete Tätigkeit verstanden. Eine Verwendung als Domainname reicht für die erforderliche kennzeichenmäßige Benützung aus, da der Name hierbei als Unternehmens- oder Dienstleistungsbezeichnung verwendet wird. Dies ist analog dazu zu sehen, daß ein Domainname Namensfunktion besitzt: Eine rein technische Adressierung wäre kein Gebrauch im Sinne dieses Gesetzes.

Letztes erforderliches Element ist die Verwechslungsgefahr. Hierfür muß der Name entweder identisch oder zumindest ähnlich sein. Zur Beurteilung ist auf den normalen Internet-Benutzer abzustellen. Die Verwechslungsgefahr ist jedoch ausgeschlossen, wenn sowohl Branche wie auch angebotene Waren bzw. Dienstleistungen völlig unterschiedlich sind, da der Konsument dann kaum irregeführt wird (zur Zeit umstritten!). Dies ist jedoch kein Freibrief, da auch der Anschein einer Nahebeziehung (z. B. selber Konzern; wirtschaftliche, aber auch organisatorischer Art) für eine Verwechslungsgefahr ausreicht, sodaß trotz unterschiedlichem Angebot Irreführungsgefahr vorliegen kann.

4.2. Behinderung und Domain-Grabbing ieS

Wird ein Domainname alleine zu dem Zweck registriert, damit er auf Grund der technischen Ausschlußwirkungen nicht von einem anderen Unternehmen verwendet werden kann, so ist dies sittenwidriger Behinderungswettbewerb. Es kommt hier insbesondere nicht darauf an, ob der von der Verwendung ausgeschlossene ein besonderes Recht an dem Namen besitzt oder nicht, schon ein begründetes Interesse ist ausreichend ([N. N.], [Schanda 2000 Ansprüche]). Der Beweis hierfür ist jedoch vielfach schwer zu erbringen, da meist ein eigenes Interesse ausgeführt (und auch zumindest in Ansätzen bewiesen) wird.

Wird ein Domainname deswegen reserviert, um ihn anschließend an jemand anderen zu verkaufen (insbesondere an den Berechtigten, aber etwa auch an Konkurrenten), so spricht man von Domain Grabbing im engeren Sinne. Auch dies fällt unter sittenwidrigen Wettbewerb und ist verboten. Auf Grund der viel einfacheren Beweisbarkeit sind diese Fälle viel häufiger (meistens erfolgt das Verfahren im Anschluß an Verhandlungen, in denen der Verkauf gegen eine hohe Geldsumme angeboten wurde). Dies verbietet zwar keinen Handel mit Domainnamen, schränkt ihn im Ergebnis jedoch sehr stark ein.

Auch hier ist ein Handeln im geschäftlichen Verkehr erforderlich, doch ist bereits die Anmeldung des Domainnamens ein solches (unabhängig davon, ob eine Webseite darunter veröffentlicht wird oder

sonst irgendeine Verwendung erfolgt!), wenn es zum Zwecke der Behinderung oder dem späteren Verkaufe erfolgt ([Gravenreuth]).

4.3. Abgrenzung zum Namensschutz

Der wettbewerbsrechtliche Schutz ist einerseits weiter als der Namensrechtliche, andererseits jedoch auch enger:

- Weiter: Nicht nur Namen und Geschäftskennzeichen mit Namensfunktion sind erfaßt, sondern auch sonstige Namen, Firmen, Unternehmens- oder Druckwerksbezeichnungen, Warenverpackungen bzw. -ausstattungen etc.
- Enger: Schutz besteht nur bei Verwendung des Namens durch den Verletzter im geschäftlichen Verkehr. Privater Gebrauch ist hier irrelevant.

5. Markenrechtlicher Schutz

Für Marken existiert ein eigener Schutz, welcher allerdings ausschließlich auf Handeln im geschäftlichen Verkehr beschränkt ist. Es sind zwei Fälle zu unterscheiden (§ 10 MSchG): Verwechslungs- und Verwässerungsgefahr. Zu beachten ist, daß auch bei einer eingetragenen Marke ältere Rechte bestehen können, welche vom Schutz nicht berührt werden. Grundsätzlich sind nur eingetragene Marken geschützt, doch sind diesen Kennzeichen gleichgestellt, welche aufgrund von Verkehrsgeltung Unterscheidungskraft besitzen.

Wichtig im Zusammenhang mit dem Markenschutz ist die Verwendung von Gattungsbezeichnungen als Domainnamen. Siehe dazu Abschnitt 6.1.

Es besteht, neben dem Unterlassungsanspruch, jedenfalls ein Anspruch auf Schadenersatz, angemessenes Entgelt und Herausgabe der Bereicherung. Ein Übertragungsanspruch, der bei Domainnamen besonders wichtig ist, ist nicht vorgesehen, kann aber u. U. durch Analogie gewonnen werden (§ 30a Abs. 3; Schutz ausländischer Marken). Ansonsten kann hier das UWG Anwendung finden.

5.1. Was ist eine “Marke”?

Marken können alle Zeichen sein, die sich graphisch darstellen lassen, insbesondere Wörter einschließlich Personennamen, Abbildungen, Buchstaben, Zahlen und die Form oder Aufmachung einer Ware, also auch Domainnamen. Diese Zeichen müssen aber geeignet sein, die Waren oder Dienstleistungen des Unternehmens von denjenigen anderer zu unterscheiden.

Eine Marke soll der Unterscheidung von Waren und Dienstleistungen dienen, sodaß der Kunde das Produkt eindeutig identifizieren und auf den Markeninhaber Rückschlüsse ziehen kann. Auf diesem Wege soll es ihm auch ermöglicht werden, die Beschaffenheit, Ausstattung und eventuell eingehaltene Qualitätsstandards schnell zu beurteilen.

5.2. Verwechslungsgefahr

Ein identisches Zeichen darf nicht für gleiche Waren verwendet werden, während gleiche oder ähnliche Zeichen nur bei Verwechslungsgefahr nicht verwendet werden dürfen. Diese besteht dann, wenn für das Publikum durch die Verwendung die Gefahr besteht, die beiden Produkte zu verwechseln oder mit dem anderen gedanklich in Verbindung zu bringen. Sind daher die Waren oder

Dienstleistungen völlig unterschiedlich, so besteht keine Verwechslungsgefahr und das selbe Zeichen kann für beide verwendet werden.

Umstritten ist hier, ob sich bei Domainnamen die Verwechslungsgefahr lediglich auf den Domainnamen bezieht, oder auch die darunter abrufbaren Webseiten (und damit die Angebotenen Waren) zu beachten sind. In einer deutschen Entscheidung (LG Düsseldorf "epson.de", [Brandl/Fallenböck]) wurde festgestellt, daß lediglich der Name relevant ist und es auf den dahinter stehenden Inhalt nicht ankommt. Hierfür spricht auch, daß man Domainnamen vielfach auch Offline begegnet, z. B. auf Briefpapier, Firmenwagen, etc. Dagegen spricht, daß der Domainname meist kein eigenes Produkt ist (außer z. B. bei reinen Online-Zeitschriften), sondern es um die darunter angebotenen Waren geht. Der OGH hat im Fall "sattler.at"[56] hingegen auf die völlige Branchenunterschiedlichkeit abgestellt, und damit die Verwechslungsgefahr (wenn auch nciht im Hinblick auf den Markenschutz) verneint. Da der Name identisch war, wurde offensichtlich auf den Inhalt der Webseiten abgestellt.

5.3. Verwässerungsgefahr

Besteht keine Ähnlichkeit der Produkte, so kann trotzdem ein Verbot möglich sein: Ist die Marke weit bekannt und die Verwendung eines gleichen oder ähnlichen Namens erfolgt, um die Unterscheidungskraft und Wertschätzung der Marke in unlauterer Weise auszunutzen oder sie ist geeignet, diese zu beeinträchtigen, so kann der Markeninhaber die Verwendung untersagen. Hier ist zusätzlich eine besondere Bekanntheit der Marke erforderlich.

6. Besondere Aspekte

In diesem Abschnitt werden verschiedene weitere Aspekte des Schutzes von Namen behandelt: Beschreibende Namen, an denen niemand ein besonderes Recht zusteht und daher auch kein individuelles Abwehrrecht möglich ist. Von geringerer Bedeutung in diesem Zusammenhang sind (und werden daher nur kurz behandelt) der firmenrechtliche und der urheberrechtliche Schutz. Abschließend wird noch kurz erläutert, wie ein Urteil auf Übertragung eines Domain auch durchgesetzt werden kann.

6.1. Beschreibende Namen

Sowohl Gattungsbegriffe als auch beschreibende Namen stellen ein besonderes Problem im Internet dar, da sie alle Mitbewerber von der Verwendung ausschließen ([Brandl/Fallenböck], [Hartmann]). Im Markenrecht ist daher festgelegt, daß solche Namen nicht als Marke reserviert werden können (§ 4 Abs 1 Z 5 MSchG), da ein allgemeines Freihaltebedürfnis vorliegt[57]. Im Gegensatz zu einer Marke ist bei einem Domainnamen jedoch der Hauptzweck die Identifizierung des Anbieters, und nicht des dahinterstehenden Angebotes und dessen Unterscheidbarkeit von ähnlichen Produkten. Auch kann das Markenrecht nicht analog angewendet werden, da dort für solche Fälle ein besonderes (hoheitliches) Verfahren zur Prüfung vorgesehen ist, welches bei Domainnamen jedoch fehlt.

---

[56] Gewerbliche Interessensvertretung der Lederwarenerzeuger, Taschner, Sattler und Riemer ⇔ Rechtsanwalt mit Familienname „Sattler";

[57] So würde etwa große Probleme entstehen, wenn jemand sich „Fernseher" oder gar „cm" oder „kg" als Marke eintragen ließe. Siehe jedoch auch „Walkman", was eine geschützte Produktbezeichnung von Sony ist, aber praktisch als Gattungsbegriff verwendet wird. Hieraus ergeben sich viele Probleme. Weniger Probleme verursacht etwa „Tixo" → „Klebeband".

Der Standardeinwand für die Möglichkeit der Reservierung solcher Namen ist, daß durch eine leichte Abwandlung jederzeit auch andere Unternehmen diesen Namen verwenden können. Da jedoch der normale Internet-Benutzer praktisch immer die einfachste Form verwenden wird, kann diesem Einwand wohl nicht gefolgt werden. Nur die wenigsten Benutzer werden noch abgewandelte Bezeichnungen versuchen, wenn sie mit der Grundform bereits Erfolg hatten[58]. Es erfolgt daher eine wettbewerbswidrige Kanalisierung der Kundenströme und die Verwendung eines solchen Namens ist daher verboten (§ 1 UWG; Ein Übertragungsrecht ist hier nicht enthalten, da es auch für den Kläger verboten wäre, diesen Namen zu verwenden!). Dieser Bereich ist jedoch noch umstritten.

6.2. Firmenrechtlicher Schutz

Der § 37 HGB schützt die Firma eines Kaufmannes, gewährt jedoch nur einen Unterlassungsanspruch (inklusive Beseitigung, also die Löschung bei Domainnamen, jedoch keine Übertragung). Mit der Firma wird ein vollkaufmännischer Unternehmensträger bezeichnet (nicht das Unternehmen selbst, sondern dessen Rechtsträger; nur Vollkaufleute können eine Firma besitzen und müssen diese auch verwenden).

Voraussetzung ist ein unbefugter Gebrauch der Firma (also der Bezeichnung als Firma, z. B. im Firmenbuch oder im Geschäftsverkehr), der jemanden in seinen Rechten verletzt. Nicht nur den Inhaber der Firma, sondern auch andere in ihren Rechten (z. B. dem Namensrecht) Verletzte können klagen. Auch die Verletzung rechtlicher Interessen wirtschaftlicher Art reichen aus, nicht jedoch bloß ideelle ([Schuhmacher]). Die Befugnis und der Gebrauch sind analog zum Namensrecht zu beurteilen.

6.3. Urheberrechtlicher Schutz

Der Titelschutz nach § 80 UrhG [Dillenz] schützt nur Werke der Literatur oder der Kunst, auch wenn für sie kein urheberrechtlicher Schutz (mehr) besteht. Es kommt hier darauf an, daß andere Werke gehindert werden, einen gleichen oder gleichartigen Titel oder Bezeichnung (aber auch die äußere Ausstattung eines Werkes, z. B. eine bestimmte Umschlaggestaltung) zu verwenden, die geeignet sind Verwechslungen hervorzurufen. Um geschützt zu sein, muß der Titel selbst (alleine, ohne Rest des Werkes) Kennzeichnungs- und Unterscheidungskraft besitzen.

Für Domainnamen bedeutet dies, daß Titel von Büchern oder Kunstwerken und ähnliche Bezeichnungen nur von Berechtigten als Domainnamen verwendet werden können. Der Name an sich ist wohl ohne Rücksicht auf eine etwaige Verwechslungsgefahr des Inhalts der Webseiten geschützt, da das Gesetz neben dem Titel auch explizit die äußere Ausstattung erwähnt. Hieraus läßt sich schließen, daß es mehr auf den äußeren Anschein ankommt, als was bei genauerer Betrachtung erkennbar wäre. Die Eingabe des Domainnamens im Internet entspricht etwa dem Aufschlagen des Buches und Lesen der ersten Seiten. Es kommt hier nicht auf eine Verwechslungsgefahr des Inhalts der Webseiten an, als vielmehr auf den ersten Blick. Dies um so mehr, als Domainnamen auch auf Papier (z. B. Briefen) vorkommen, und daher eine sofortige Prüfung des Inhalts unter Umständen nicht möglich ist.

[58] Außerdem: Auf welche Art sollte die Abwandlung erfolgen? Der Grundname ist relativ eindeutig, die (möglichen und sinnvollen) Abwandlungen in der Regel jedoch von sehr großer Zahl.

6.4. Übertragung von Domain Namen

Wurde vor einem österreichischen Gericht die Übertragung eines Domainnamens erreicht (oder ist ein entsprechendes ausländisches Urteil vollstreckbar), so stellt sich die Frage, wie es in die Realität umgesetzt werden kann. Problematisch ist hier der Punkt, daß das Urteil aus einem Streit zwischen dem derzeitigen Inhaber der Domain und einem (zukünftigen) neuen Domaininhaber erfließt. Nicht Partei des Verfahrens (und daher auch nicht an das Urteil gebunden!) ist die Registrierungsstelle. Da es sich bei der Domainregistrierung auch um einen privatrechtlichen Vertrag handelt, kann die Registrierungsstelle nicht einfach dazu gezwungen werden, einen Wechsel des Vertragspartners zu akzeptieren. Es bliebe daher nur eines übrig, den bisherigen Inhaber zur Löschung durch Nicht-Fortsetzung oder Beendigung des Vertrages zu zwingen. Befindet sich jedoch schon jemand Anderer auf der Warteliste für diesen Domainnamen, so führt dies zu keiner Übertragung der Domain.

Zur Lösung dieses Problems verpflichten sich die Registrierungsstellen (z. b. nic.at; AGB's 3.6), einen Domain auf Antrag des derzeitigen Inhabers auf jemand anderen zu übertragen und mit diesem einen Vertrag zu schließend, sofern er die allgemeinen Voraussetzungen (Volljährigkeit, Angabe der notwendige Informationen wie der IP-Adressen der Nameserver, etc.) erfüllt. Dieses Recht des Inhabers kann nun im schlimmsten Fall auf Grund des gegen ihn ergangenen Urteils nach Exekution vom Kläger selbst ausgeübt werden und es erfolgt eine Übertragung der Domain.

7. Das Streitbeilegungsverfahren der ICANN

Bei der "Uniform Domain Name Dispute Resolution Policy" handelt es sich um einen Modell-Vertrag, welcher von der ICANN ([ICANN]) erarbeitet wurde und von allen Registrierungsstellen für .com, .net und .org sowie verschiedenen country-code Registrierungsstellen verwendet wird. Sie wird Teil des Vertrages zwischen dem Domaininhaber und der Registrierungsstelle. Zur Zeit stehen 4 Organisationen zur Verfügung, welche Schiedsverfahren nach dieser Policy durchführen.

Ein Domaininhaber ist nur dann diesem Verfahren unterworfen, wenn er ihm entweder freiwillig zustimmt, oder er durch seinen Vertrag mit der Registrierungsstelle dazu verpflichtet ist.

7.1. Verpflichtungen der Registrierungsstelle

Eine Registrierungsstelle verpflichtet sich zur Vornahme von Änderungen ausschließlich in folgenden Fällen:

1. Aufforderung dazu durch den Domain-Inhaber
2. Entscheidung eines **zuständigen**[59] Gerichts- oder Schiedsgerichts
3. Entscheidung eines Verfahrens nach der Policy der ICANN, bei welchem der Domaininhaber Partei war
4. Sondervereinbarungen oder lokale Gesetze sehen dies vor

7.2. Streitgegenstand

Es werden nur sehr eng begrenzte Streitigkeiten nach dieser Policy ausgetragen. Der Beschwerdeführer hat nachzuweisen, daß alle drei der folgenden Elemente zutreffen:

[59] Nach eigener Beurteilung

1. Der Domainname ist identisch oder verwechslungsfähig ähnlich einem Warenzeichen oder einer Dienstleistungsmarke, auf das der Beschwerdeführer ein Recht hat
2. Der Domain-Inhaber hat kein Recht oder berechtigtes Interesse in Bezug auf den Namen
3. Der Domainname wurde bösgläubig registriert und wird bösgläubig verwendet.

7.3. Rechtsfolgen

Ausschließlich die Löschung oder der Transfer eines Domainnamens kommen als Folge eines Verfahrens in Frage.

7.4. Beispiele für bösgläubige Registrierung und Benutzung

Es ist erforderlich, daß **sowohl** die Registrierung (bzw. der Erwerb) **als auch** die Verwendung einer Domain bösgläubig erfolgen müssen. Fehlt einer der beiden Teile (z. B. bei gutgläubigem Erwerb), so ist abweisend zu entscheiden. Unter anderem in folgenden Fällen wird eine bösgläubige Registrierung und Benützung angenommen:

- Registrierung bzw. Erwerb erfolgten hauptsächlich für den Verkauf, Vermietung oder eine sonstige Übertragung des Domainnamens an den Inhaber des Warenzeichens oder der Dienstleistungsmarke oder einen Wettbewerber desselben, und zwar für eine Gegenleistung, welche die tatsächlichen Kosten übersteigt.
- Die Registrierung erfolgte, um den Inhaber der Marke an der Verwendung des Domainnamens zu hindern und dies erfolgt regelmäßig.
- Die Registrierung erfolgte hauptsächlich, um einen Wettbewerber zu schädigen.
- Die Verwendung des Domainnamens erfolgt wissentlich, um einen geschäftlichen Nutzen durch Besucher der Webseite zu erzielen, indem die Wahrscheinlichkeit einer Verwechslung mit der Marke des Beschwerdeführers, dessen Mitarbeit oder dessen Verbindung zu dieser Webseite, einem Produkt oder einer Dienstleistung hergestellt wird.

7.5. Beispiele für berechtigte Interessen

Mögliche berechtigte Interessen für die Verwendung eines Domainnamens sind u. A.:

- Vor dem Bekanntwerden der Streitigkeit wurde der Domainname bereits für echte Angebote für den Verkauf von Waren oder Dienstleistungen verwendet oder es bestanden nachweisbare Vorbereitungen für eine solche Verwendung.
- Der Beschwerdegegner ist als Person, Unternehmen oder Organisation unter dem Domainnamen bekannt, auch wenn hierfür kein Markenrecht besteht.
- Der Domainname wird für einen berechtigten nicht-kommerziellen oder erlaubten Zweck verwendet und es besteht keine Absicht, wirtschaftlichen Gewinn aus der Umleitung von Kunden zu ziehen oder die Marke zu verwässern.

7.6. Wichtige Elemente des Prozesses

Die Entscheidung erfolgt durch einen einzelnen Schiedsrichter oder, auf Verlangen einer der Parteien, aus einem Senat von drei Schiedsrichtern, wobei jede Partei einen Dreiervorschlag für jeweils einen Richter erstellen kann. Die konkrete Auswahl erfolgt jedoch durch die Streitschlichtungsstelle, die diese Vorschläge nach Möglichkeit befolgen soll. Die Parteien haben kein Ablehnungsrecht; Richter

haben etwaige Umstände, welche auf eine mangelnde Unparteilichkeit hinweisen, der Streitschlichtungsstelle mitzuteilen, welche dann eigenständig über eine Auswechslung entscheidet.

Es handelt sich in der Regel um ein reines Aktenverfahren. Eine mündliche Verhandlung (auch per Videokonferenz, Telephon, etc.) ist nur in Sonderfällen und ausschließlich auf Anordnung des Schiedsgerichts hin vorgesehen. Das Schiedsgericht kann den Gang des Verfahrens frei bestimmen, hat jedoch auf Gleichheit der Parteien und einen raschen Gang des Verfahrens zu achten. Es besteht freie Beweiswürdigung.

Die Sprache des Verfahrens ist die Sprache des Registrierungsvertrages, sofern dort, oder mittels Parteienvereinbarung, nicht eine andere vorgesehen wird.

Versäumt eine Partei eine Frist, so hat das Schiedsgericht ein Versäumnisurteil zu fällen, wobei keine Wiedereinsetzung vorgesehen ist (aber über die allgemeine Verfahrensgewalt wohl möglich ist).

Es existieren keine Zwangsmöglichkeiten; kommt eine Partei einer Aufforderung des Schiedsgerichts (z. B. zur Vorlage bestimmter Dokumente) nicht nach, so hat das Schiedsgericht sich damit zu begnügen und daraus seine Schlüsse zu ziehen.

Für die Kommunikation zwischen den Parteien, der Registrierungsstelle und dem Schiedsgericht bestehen besondere Vorschriften, welche genau zu beachten sind. So ist z. B. keine “geheime” Kommunikation einer Partei mit dem Schiedsgericht erlaubt, sondern alle Mitteilungen sind immer sowohl an das Schiedsgericht als auch an die Gegenpartei zu richten.

Bei der Einbringung einer Beschwerde muß eine Unterwerfungserklärung unter einen “gemeinsamen Gerichtsstand” für Streitigkeiten über ein abänderndes Urteil (Entzug oder Transfer eines Domainnamens) abgegeben werden. Hierbei handelt es sich in Sonderfällen um den Hauptsitz der Registrierungsstelle, bei welcher der Domainname registriert wurde und sonst um die Adresse des Domaininhabers nach der Datenbank der Registrierungsstelle zum Zeitpunkt der Einbringung der Beschwerde.

7.7. Gerichtsentscheidungen

Ein Verfahren nach dieser Policy schließt ein normales Gerichtsverfahren zu keinem Zeitpunkt aus. Nach der Entscheidung bleiben 10 Werktage, um ein solches Verfahren anhängig zu machen. Erfolgt dies innerhalb dieser Frist und wird dies der Registrierungsstelle mitgeteilt, so wird die Entscheidung des Schiedsgerichts bis zur Entscheidung des Gerichts nicht umgesetzt.

7.8. Kosten

Alle Kosten der Verfahrens trägt der Beschwerdeführer, außer wenn der Beschwerdegegner einen Dreiersenat wählt, obwohl der Beschwerdeführer nur einen Einzelrichter verlangte. In diesem Fall werden die Gesamtkosten gleichmäßig (50:50) geteilt.

8. Literatur

8.1. Rechtsvorschriften

ABGB: Allgemeines bürgerliches Gesetzbuch (ABGB) vom 1. Juni 1811 JGS 946 idF BGBl I 1999/164

UWG: Bundesgesetz gegen den unlauteren Wettbewerb 1984 – UWG. BGBl 448/1984 idF BGBl I 55/2000

MSchG: Markenschutzgesetz 1970 BGBl 260/1970 idF BGBL I 191/1999

HGB: Handelsgesetzbuch vom 10. Mai 1897 dRGBl S 219/1897 idF BGBl I 142/2000

UrhG: Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (BGBl 1936/111 idF 1998/25)

8.2. Allgemein

Aicher, Josef in Rummel, Peter: Kommentar zum ABGB[2], Wien: Manz 1990, I/§ 43

Bettinger, Torsten: ICANN's Uniform Domain Name Dispute Resolution Policy, CR 4/2000, 234-239

Dillenz, Walter: Praxiskommentar zum österreichischen Urheberrecht und Verwertungsgesellschaftenrecht. Wien: Springer 1999

Gravenreuth, Günter Frhr. von: OLG Dresden: "cyberspace.de" CR 9/1999, 589-592

Hartmann, Matthias: OLG Hamburg: Branchenbezeichnung als Domain-Name. CR 12/1999, 779-783 ("mitwohnzentrale.de")

Helm, Günther: Domain Grabbing und andere Tatbestände im Internet. Diplomarbeit. Universität Linz, 2000.

The Internet Corporation for Assigned Names and Numbers (ICANN): http://www.icann.org/ (17.1.2001)

Liste der Schiedsgerichts-Organisationen: http://www.icann.org/udrp/approved-providers.htm (17.1.2001)

Mayer-Schönberger, Viktor, Hauer, Karin: Kennzeichenrecht & Internet Domain Namen. Ecolex 1997, 947-951

P. Mockapetris: Domain Names - Concepts and Facilities (RFC 1034) http://www.faqs.org/rfcs/rfc1034.html (16.1.2001)

N. N.: "Domain-Grabbing" als sittenwidriger Behinderungswettbewerb. ecolex 1999, 559f

Schanda, Reinhard: Internet Domain Names haben Namensfunktion, ecolex 1998, 565

Schanda, Reinhard: Internet Domain Names und Namensrecht, ecolex 1999, 703-705

Schanda, Reinhard: § 43 ABGB bietet Anspruchsgrundlagen gegen Domain-Namen, ecolex 2000, 215

Schanda, Reinhard: Ansprüche gegen fremde Domain-Namen-Registrierung, ecolex 2000, 132f

Schuhmacher, Wolfgang in Straube, Manfred: Kommentar zum Handelsgesetzbuch[2], Wien: Manz 1995, I/§ 37

Thiele, Clemens: Privatrechtlicher Schutz von Ortsnamen im Internet. Österreichische Gemeindezeitung 11/99, 4-13

WHOIS Abfrage: RIPE http://www.ripe.net/cgi-bin/whois (18.1.2001)

8.3. Ausgewählte österreichische Urteile zu Domain Names

jusline I: OGH 24.2.1998, 4 Ob 36/98 t ([Schanda 1998])

jusline II: OGH 27.4.1999, 4 Ob 105/99 s ([ecolex 1999])

ortig.at: OGH 21.12.1999, 4 Ob 320/99 h ([Schanda 2000 § 43])

sattler.at: OGH 13.7.1999, 4 Ob 140/99 p ([Schanda 1999])

format: OGH 13.9.1999, 4 Ob 180/99 w ([Schanda 2000 Ansprüche])

8.4. Registrierungsstellen

nic.at (*.at): http://www.nic.at/ (18.1.2001)

Network Solutions (*.com, *.net, *.org, *.tv): http://www.networksolutions.com/ (18.1.2001)

eNIC (*.cc): http://www.nic.cc/ (18.1.2001)