Verbraucherkommission Bayern

Empfehlungen zum Thema

Sicherheit von Verbraucherdaten im Internet

Übergabe an Frau Staatsministerin Dr. Merk am 27. März 2012

I. **Präambel**

In zahlreichen Bereichen des täglichen Lebens nutzen immer mehr Menschen das Internet – und hinterlassen dabei ständig Datenspuren, die im Netz bestehen bleiben. Dies gilt insbesondere für den Bereich der **Sozialen Netzwerke**. In solchen Onlineplattformen können Nutzer u.a. ihre eigenen Homepages gestalten und entwickeln. Die oftmals Jugendlichen haben hier unter anderem die Möglichkeit, persönliche Informationen mittels Statusnachrichten oder Profilbildern mit anderen Netzwerkmitgliedern zu teilen; dabei bestimmen sie selbst über die Sichtbarkeitseinstellungen.

Portale wie Facebook setzen sich das Ziel, durch ihre globale ‚Online Community' die Welt offener und vernetzter zu machen. Die Statistik des Bundesverbandes für Informationswirtschaft, Telekommunikation und neue Medien bestätigt dies: Drei Viertel aller deutschen Jugendlichen im Alter von zehn bis achtzehn Jahren nutzen aktiv soziale Netzwerke; des Weiteren geben Jugendliche die Internetnutzung als eine ihrer bevorzugten Freizeitbeschäftigungen an.

Diese gesteigerte soziale Vernetzung birgt aber auch Gefahren. Oftmals besteht bezüglich der Erhebung, Verarbeitung und Nutzung von Daten keine oder mangelhafte **Transparenz**. Der Verbraucher wird nur ungenügend darüber aufgeklärt, was mit den von ihm bereitgestellten Daten geschieht. So ist etwa im Fall sozialer Netzwerke mitunter unklar, inwieweit dort eingegebene personenbezogene Daten auch kommerziell genutzt werden.

Damit ist die **Datenhoheit** des Verbrauchers vielfach nicht gewährleistet. Über die Nutzung der Daten kann keine ausreichende Kontrolle mehr ausgeübt werden. Dies ist insbesondere bedenklich, da 42 % der jugendlichen Nutzer sozialer Plattformen ihre persönlichen Informationen wie Namen, private Fotos oder Auskünfte über Vorlieben im Internet freigeben.

An diese Probleme knüpfen sich Fragen an die **Mündigkeit des Verbrauchers** an: Kann es den (insb. jugendlichen) Nutzern selbst überlassen sein, für die Sicherheit ihrer Daten zu sorgen? Reicht eine Verbraucherbildung aus, damit sie sich bewusster mit den Risiken des Internets auseinander setzen? Oder müssen die Nutzer angesichts der übermächtigen technischen Möglichkeiten verstärkt gesetzlich geschützt werden bzw. welche weiteren Maßnahmen wie z.B. Selbstverpflichtungen sind denkbar?

Vor diesem Hintergrund hat sich die Verbraucherkommission mit Fragen des Schutzes von Verbraucherdaten bei Internetangeboten auseinandergesetzt. Im Zuge dessen wurde u.a. eine Stellungnahme beim Präsidenten des Landesamtes für Datenschutzaufsicht angefordert, deren Inhalte in der Stellungnahme berücksichtigt worden sind.

Die Regelungen des Datenschutzes für den nichtöffentlichen Bereich finden sich im Wesentlichen im Bundesdatenschutzgesetz (BDSG) und im Telemediengesetz (TMG).
Die im Folgenden unter Punkt II. dargelegten Empfehlungen stellen Ansätze dar, einen verbesserten Datenschutz - auch auf Länderebene - zu ermöglichen. Es geht zum einen darum, was Bayern konkret umsetzen kann (z. B. in den Bereichen Bildung, Datenschutzaufsicht, Best Practice, bessere Koordinierung der mit der Rechtsdurchsetzung beauftragten Institutionen) und zum anderen um Einwirkungsmöglichkeiten auf nationale und EU-weite Regelungen. Hierbei ist das Zusammenspiel des Datenschutzrechts mit der Technik, der Wirtschaft und dem Bürger zu gestalten. Eine solche gesamtgesellschaftliche Lösung vermag die Herausforderungen einer modernen Datenschutzkultur am besten zu bewältigen.
Neben den Risiken stellt die Entwicklung des Internets aber auch mitunter eine Chance dar – unter Punkt II. 1. soll auf die Möglichkeiten eingegangen werden, die sich aus der **Wechselbeziehung von Sicherheit und Technik** ergeben.

II. Einzelheiten

1) Wechselbeziehung von Sicherheit, Technik und Recht

a) Verbesserung von Datenschutz/Datensicherheit durch technische Entwicklungen

Durch die technische Entwicklung des Internets ergeben sich auch Chancen. So lassen sich beispielsweise Straftaten durch die Auswertung der vom Täter im Internet hinterlassenen Spuren vermeiden oder aufklären. Technische Möglichkeiten (Bsp. ‚Watermarking') erlauben das Erkennen von Manipulationen oder das Aufdecken von Fälschungen.
Allerdings bestehen noch viele technische Herausforderungen (zu Privacy by Design siehe unten 1) b)); zudem lassen sich Missstände nicht allein durch verbesserte Technik beheben. Vielmehr bedarf es der Schaffung einer ‚Sicherheitskultur', das heißt das Bewusstsein des Verbrauchers für Datenschutz- und Datensicherheit muss gefördert werden. Im Zusammenspiel von verbesserter Verbraucherkompetenz, klarer gesetzlicher Vorschriften und Berücksichtigung der technischen Möglichkeit, lässt sich hier aus Sicht der Verbraucherkommission eine deutliche Verbesserung der derzeitigen Situation erzielen, was auch durch Maßnahmen auf Landesebene wesentlich unterstützt werden kann.

b) Privacy by Design

Dieser Ansatz zielt auf die Einbindung der Hersteller und Entwickler in den Datenschutz ab. Er wird gestützt durch die Überlegung, dass ein Entwickler einer Software – die oft weltweit eingesetzt wird – Datenschutz und Datensicherheit oft weitergehend beeinflusst als ein nati-

onaler Gesetzgeber („code is law“). Reduziert etwa ein Programmierer das „Datensammeln“ in einer Software, kann damit global oft ein signifikanterer Effekt für besseren Datenschutz erzielt werden, als das ein nationaler Gesetzgeber könnte. Die Einflussnahme auf die Ersteller von Software und Websites durch Politik und Gesellschaft ist daher global von erheblicher Bedeutung.
Die Verbraucherkommission fordert deshalb, das Prinzip Privacy by Design weitestgehend umzusetzen.
Unter Berücksichtigung der Interessen der Wirtschaft macht es allerdings keinen Sinn, die Verarbeitung sämtlicher Daten von vornherein zu verhindern. Es ist durchaus ein Anliegen von Teilen der Wirtschaft, ein hohes Datenschutzniveau zu erreichen (zu Selbstkontrolle der Wirtschaft, siehe unten Punkt 2)). Reine Vorgangsdaten jedoch, die keinen persönlichen Bezug aufweisen, können für statistische Zwecke wertvoll sein. Eine Erhebung und Verwendung von Daten, die den Verbraucher nicht in seiner grundrechtlich geschützten informationellen Selbstbestimmung tangieren können, sollte nicht durch Privacy by Design ausgeschlossen werden.

c) Datenschutzfreundliche Voreinstellungen (Privacy by Default)[1]

Technische Systeme werden immer komplexer und Datenverarbeitungen immer unübersichtlicher. Die Voreinstellungen vieler Produkte und Dienste sind nicht datenschutzfreundlich gestaltet. Datenschutzgesetze sollen regeln, dass zusätzlich zur Beachtung des Prinzips Privacy by Design bei der Programmierung die Grundeinstellungen von Produkten und Diensten bei der Anwendung so gestaltet sind, dass so wenig personenbezogene Daten wie möglich erhoben und verarbeitet werden. Die Verbraucher haben dann die Entscheidung zusätzliche persönliche Informationen preiszugeben.

2) Selbstkontrolle der Wirtschaft

a) Allgemeiner Grundgedanke

Aufgrund der eingangs beschriebenen begrenzten Möglichkeiten des bestehenden Datenschutzrechts weist dieses nur eine geringe Kontrolldichte auf. Daher ist es unter anderem sinnvoll, eine Eigenkontrolle der Wirtschaft zu unterstützen. Dazu muss Datenschutz von den verantwortlichen Unternehmen als eigenes Anliegen aufgefasst werden; ein geeigneter Ansatz, um dies zu bewirken, liegt in der Etablierung von **Datenschutz als Wettbewerbsvorteil**.

---

[1] siehe Petition des Verbraucherzentrale Bundesverband und der Verbraucherzentralen zum Thema „Datenschutzfreundliche Voreinstellungen“

In diesem Zusammenhang ist ein Vergleichstest der am Markt befindlichen Produkte und Dienstleistungen hinsichtlich des Datenschutzes positiv zu bewerten (näher zur Initiative Stiftung Datenschutz unter 2) b)); es läge dann in der eigenen Verantwortung der Unternehmen, sich durch ein hohes Schutzniveau attraktiver zu machen.
Die Unterstützung von Selbstregulierungsmechanismen auf Landes- und Bundesebene (wie z.B. die Stiftung Datenschutz) halten wir für zielführend. Diese sollte die Entwicklung geeigneter Kontrollstrukturen umschließen, die auch die Unternehmen selbst einbinden (näher unter 8).

b) Initiative ‚Stiftung Datenschutz'

Der Koalitionsvertrag zwischen CDU, CSU und FDP sieht die Einrichtung einer ‚Stiftung Datenschutz' vor (S. 106 des Koalitionsvertrages). Dieses Vorhaben ist mittlerweile durch ein Eckpunktepapier der FDP-Vizefraktionsvorsitzenden Gisela Piltz konkretisiert worden.
Der Aufgabenbereich der Stiftung Datenschutz lässt sich in vier Teilbereiche zergliedern: Die Stiftung soll zunächst Gütesiegel für datenschutzfreundliche Unternehmen verleihen, sowie Audits durchführen. Daneben sollen datenschutzrechtlich relevante Produkte und Dienstleistungen mittels Testverfahren miteinander verglichen werden. Zusätzlich kommen die Bereitstellung von Bildungsangeboten und die Forschung und Weiterentwicklung des Datenschutzrechts zu den Aufgaben hinzu.
Der Begriff lehnt sich an die Stiftung Warentest an; diese hat insbesondere mit den Merkmalen absoluter Neutralität, keiner staatlichen Einflussnahme auf die Testergebnisse, sowie der organisatorischen Einbindung der gesellschaftlich relevanten Gruppen bislang große Erfolge verzeichnen können.
Die Stiftung Datenschutz weicht allerdings in wichtigen Punkten vom Vorbild der Stiftung Warentest ab. Die Letztere prüft in erster Linie Produkte und Dienstleistungen auf dem Markt, welche auch ohne Mitwirkung des entsprechenden Anbieters einem Testverfahren zugänglich sind. Dieses Vorgehen lässt sich nur teilweise auf die Ebene des Datenschutzes übertragen. Die Qualität des Datenschutzes hängt maßgeblich von der Konfiguration der internen Datenverarbeitungsprozesse ab. Eine Einsicht in diese Prozesse ist jedoch nur mit der Mitwirkung der geprüften Anbieter möglich. Eine Beschränkung auf die Prüfung öffentlich verfügbarer Informationen (Bsp. Datenschutzerklärungen) könnte jedenfalls den Ansprüchen einer ernsthaften Prüfung nicht gerecht werden.
Dadurch wird allerdings bewirkt, dass sich nur die Unternehmen prüfen lassen, die auch ein gesetzeskonformes Datenschutzkonzept aufweisen. Damit können zwar datenschutzfreundliche Produkte und Dienstleistungen ausgewiesen werden, die ‚schwarzen Schafe' in der IT-Branche werden jedoch nicht erfasst. Diesbezüglich sollte eine Regelung getroffen werden, die festlegt, wie mit nicht-kooperativen Unternehmen zu verfahren ist. In Einklang mit der Meinung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, sowie

den Datenschutzbeauftragten der Länder begrüßt auch die Verbraucherkommission die Stiftung Datenschutz. Die Organisation muss unabhängig arbeiten und mit den bestehenden Aufsichtsbehörden kooperieren. Dabei gilt insbesondere zu beachten, dass die Stiftung weder personell noch finanziell von der IT-Wirtschaft und sonstigen Stellen abhängen darf. Dies ist bei der Zusammensetzung der Mitglieder sowie der finanziellen Ausstattung zu berücksichtigen.
Durch Kooperation mit den Aufsichtsbehörden sollen diese ihre langjährige Erfahrung mit der Prüfung von Unternehmen in die Entwicklung der Verfahren einbringen. Zudem ist durch die Zusammenarbeit mit den Aufsichtsbehörden zu gewährleisten, dass es nicht zu sich überschneidenden Zuständigkeitsbereichen und einer daraus resultierenden negativen Öffentlichkeitswirkung kommt; die Stiftung Datenschutz soll die Arbeit der Behörden entlasten, diese aber nicht ersetzen. Vielmehr ist auf einen möglichst positiven Synergieeffekt hinzuwirken.

c) Best Practices

Zu empfehlen ist weiterhin die Unterstützung der Entwicklung von Best Practices im Bereich Datenschutz. Dadurch wird ein einheitlicher Standard im Datenschutz gefördert.
Zu unterstützen ist etwa das Vorgehen des Bayerischen Landesamtes für Datenschutzaufsicht, in ihrem jeweiligen Jahresbericht für bestimmte, kürzlich geprüfte Bereiche die Ergebnisse und gesetzeskonforme Vorgehensweisen zu veröffentlichen, an denen sich Unternehmen orientieren können. Ebenfalls regt die Verbraucherkommission an, durch eine wissenschaftliche Untersuchung und Kategorisierung von Best-Practice Beispielen, Impulse und Benchmarks für den verantwortungsbewussten Umgang mit Verbraucherdaten in Onlinediensten zu geben.

3) Erhöhung der Datenkompetenz

Ein Tätigwerden auf Landesebene ist insbesondere dort sinnvoll, wo lokales Handeln in Hinblick auf den Datenschutz eine weitreichende Wirkung hat. Ein zentraler Punkt ist hier die Förderung der Datenkompetenz, das heißt die Kenntnis der eigenen Rechte und Möglichkeiten, sowie die Sensibilisierung für die Risiken im Umgang mit dem Internet.

Denn wer sensibler hinsichtlich der Verarbeitung personenbezogener Daten ist,

- kann bewusster entscheiden, ob er eine Einwilligung in eine Datenverarbeitung erteilt oder nicht,
- erkennt auch den wirtschaftlichen Wert seiner Daten und kann somit Kosten und Nutzen seiner Einwilligung besser abwägen,
- kann unseriöse Anbieter besser erkennen,
- erkennt ein hohes Datenschutzniveau als Qualitätsmerkmal eines Anbieters an, womit eine Selbstregulierung honoriert wird.

Auf diese Weise kann eine Förderung auf Landesebene auch Auswirkungen hinsichtlich internationaler Anbieter haben.
Diese Datenkompetenz kann auf Landesebene auf unterschiedliche Weise gesteigert werden. Da insbesondere **jugendliche Nutzer** Opfer der Gefahren des Internets sind – mit zunehmendem Alter steigt auch die Häufigkeit negativer Erfahrungen – gilt es vor allem bei dieser internetaffinen Gruppe anzusetzen. Wie eingangs beschrieben, sind Jugendliche besonders stark in sozialen Netzwerken aktiv, häufig unter Preisgabe persönlicher Informationen; hier ist die Stärkung der Sensibilität für potentielle Risiken besonders wichtig.
Mit der Bildung als Ländersache kommt dabei den Bundesländern der Großteil der Verantwortung zu. Ein möglicher Ansatz wäre ein altersgerechtes Aufarbeiten dieser Thematik in gesonderten Unterrichtseinheiten.

Bei **Erwachsenen** sollte im Rahmen entsprechender Maßnahmen auch ein Fokus auf die Aufklärung über bestehende Verbraucherrechte (z. B. § 35 BDSG – Benachrichtigung, Sperrung, Löschung) gelegt werden.
Insofern begrüßt die Verbraucherkommission die Richtlinie für die ökonomische Verbraucherbildung an bayerischen Schulen (Feb. 2010), die auch Datenkompetenzen berücksichtigt, und die Zusammenarbeit mit dem Bayerischen Volkshochschulverband, im Kontext des lebenslangen Lernens auch den Bereich Internet und Datenkompetenz zu schulen.

Bei der Förderung sollte mit dem Datenschutzbeauftragten und anderen Stellen (Verbraucherkommission, Stiftung Datenschutz) zusammengearbeitet werden, die bei der Erstellung von Schulungskonzepten oder Informationsmaterial ihre bewährte Erfahrung einbringen können.
Die Förderung eines sensiblen und informierten Verbrauchers, der seine Rechte bewusst wahrnimmt, ist somit eine wirkungsvolle Möglichkeit zur Durchsetzung von Datenschutz auf Länderebene.

4) Rechte des Betroffenen (Rechtliche Fragen der Einwilligung)

Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nur zulässig, soweit das Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Damit ist die Einwilligung (§ 4a BDSG) ein wichtiges Instrument, mittels dessen der Verbraucher selbst über die Verarbeitung seiner Daten bestimmen kann.

Die Einwilligung muss der Datenverarbeitung vorangehen (vergleichbare Regelung im BGB); eine nachträgliche Genehmigung ist nicht wirksam. Aufgrund der Rechtsnatur der Einwilligung als Realakt, ist ein natürlicher Wille dazu ausreichend. Dies bedeutet in der Konsequenz, dass auch beschränkt Geschäftsfähige (Minderjährige) in die personenbezogene Datenverarbeitung einwilligen können. Voraussetzung bleibt allerdings eine nötige Einsichtsfähigkeit, das heißt der Betroffene muss die Tragweite seiner Entscheidung erkennen können.

a) Einwilligung auf informierter Grundlage

Das BDSG und das TMG fordern, dass der Betroffene auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen ist. In diesem Zusammenhang stellt sich die Frage nach dem Umfang dieser Informationspflicht.
Insgesamt ist eine informierte Grundlage somit unerlässliche Voraussetzung einer wirksamen Einwilligung. Die Anbieter von Produkten und Dienstleistungen haben dies zu berücksichtigen. Wo eine umfängliche Information aufgrund der Sachlage nicht zweckmäßig ist, sollte eine Aufklärung über die wichtigsten Konsequenzen der Einwilligung ausreichen. Dies lässt die Pflicht zu tiefer gehender Information bei Interesse des Betroffenen jedoch unberührt.
Die gesetzlichen Regelungen in diesem Bereich sind aus Sicht der Verbraucherkommission ausreichend. Auf Grund der Bedeutung der Einwilligung für die Datenhoheit des Verbrauchers ist darüber hinaus eine intensive Kontrolle durch die Aufsichtsbehörden angezeigt.

b) Kontrolle des Verbrauchers über seine Daten

Auch nach der Einwilligung in die Verarbeitung personenbezogener Daten hat der Betroffene Rechte, über seine Daten zu bestimmen.
Insbesondere durch den Widerruf kann der Betroffene sein Recht auf informationelle Selbstbestimmung, als verfassungsrechtliche Grundlage des deutschen Datenschutzrechts, geltend machen. Die Wirkung des Widerrufs entfaltet sich für die Zukunft; ab dem Zeitpunkt des

Widerrufs ist die verarbeitende Stelle nicht mehr berechtigt, die Daten zu nutzen. Diese sind dann nach §§ 20 Abs. 2 Nr. 1, 35 Abs. 2 Nr. 1 BDSG zu löschen.

c) Zeitliche Begrenzung der Einwilligung

Zeitlich gilt die Einwilligung grundsätzlich für die Dauer der konkreten Datenverarbeitung. Im Rahmen der Dauer der konkreten Datenverarbeitung kommt der Grundsatz der Zweckbindung zum Tragen, § 4a Abs. 1 Satz 2 BDSG. Die Daten müssen immer dann gelöscht werden, wenn der vorher festgelegte Zweck erreicht wurde, dies ergibt sich aus § 20 Abs. 2 Nr. 1 und § 35 Abs. 2 Nr. 1 BDSG.

Diese Regelungen allein reichen jedoch nicht, einen wirksamen Datenschutz zu gewährleisten. Die Verbraucherkommission regt deshalb an, über eine generelle zeitliche Befristung von Einwilligungen nachzudenken. Zumindest bei Jugendlichen und Heranwachsenden bis zum 21. Lebensjahr sollte eine Einwilligung maximal zwei Jahre wirksam sein und automatisch nach dem Ablauf von z.B. zwei Jahren erlöschen mit der Folge, dass alle gespeicherten Daten dann rückwirkend wieder zu löschen sind. Der Auffassung, dies würde Unternehmen unangemessen belasten, kann die Verbraucherkommission nicht folgen. Für Unternehmen ist dies ohne erheblichen Mehraufwand vor Ablauf der Frist möglich, beim Kunden eine neue Einwilligung einzuholen. Auch in anderen Bereichen wurden vergleichbare Modelle über Jahrzehnte hinweg erfolgreich praktiziert. So mussten Privatanleger beim Abschluss von Börsentermingeschäften von 1. August 1989 bis 1. November 2007 mit einer gesonderten Risikoinformationsschrift, die vom Kunden zu unterzeichnen war, über die besonderen Risiken solcher Geschäfte aufgeklärt werden. Diese Risikobelehrung musste nach der ersten Belehrung bereits nach Ablauf von zehn bis zwölf Monaten wiederholt werden und musste sodann alle drei Jahre erneut unterzeichnet werden. Die Verbraucherkommission empfiehlt die zeitliche Begrenzung der Einwilligung bei jugendlichen Internetnutzern gesetzlich vorzuschreiben.

5) Kontrolle der Einhaltung gesetzlicher Regelungen

In Bayern ist das Landesamt für Datenschutzaufsicht für die Einhaltung des Datenschutzrechts im nicht-öffentlichen Bereich zuständig. Damit ist die unabhängige Behörde mit einem weiten Tätigkeitsfeld befasst. Die Arbeit ist nicht nur auf die lokale IT-Branche zugeschnitten, sondern richtet sich ebenfalls auf die Einhaltung des Datenschutzes durch internationale Unternehmen. Kürzlich hat etwa der Behördenleiter Thomas Kranig ein Verfahren gegen den Apple-Konzern angestrengt, da dessen Mobiltelefone ungefragt den Aufenthaltsort ihrer Besitzer speicherten.

Allerdings weist die Behörde nur eine Personalstärke von zwölf Personen auf. Eine Unterbesetzung angesichts des oben geschilderten Einsatzbereiches ist damit aus Sicht der Verbraucherkommission kaum von der Hand zu weisen.
Eine solche ist aber durchaus problematisch. Damit gesetzliche Vorgaben in der Praxis eingehalten werden, bedarf es vor allem einer kontrollierenden Instanz, die Fälle der Nichteinhaltung gegebenenfalls auch sanktionieren kann. Wird diese ihrer Funktion nicht gerecht, besteht die Wahrscheinlichkeit, dass Unternehmen von den gesetzlichen Vorschriften abweichen. Dies erzeugt ein Ungleichgewicht auf dem Markt, da andere Anbieter mit gesetzeskonformen Produkten/ Dienstleistungen möglicherweise einen Nachteil haben. Um wettbewerbsfähig zu bleiben, entsteht ein Druck auf sie, ebenfalls gesetzliche Regelungen zu vernachlässigen.
Eine nicht ausreichende personelle Aufstellung des Landesamtes für Datenschutzaufsicht bewirkt also, dass noch so gute gesetzliche Vorgaben möglicherweise ins Leere laufen. Dadurch entsteht eine kritische Unausgewogenheit von Gesetz und Kontrolle.
Im Ergebnis ist daher der Ruf nach immer schärferen gesetzlichen Auflagen zurückzuweisen, wenn gleichzeitig keine geeignete Kontrollinstanz besteht, die die Einhaltung dieser Auflagen gewährleisten kann.

6) Privatrechtliche Mechanismen

Neben den bereits dargestellten Maßnahmen halten wir die Stärkung und erleichterte Durchsetzung von privaten Rechten (Private Enforcement) für notwendig, um den Verbraucherschutz im Bereich des Datenschutzes zu verbessern. Wir halten es für sinnvoll, die bisher bestehenden Anspruchsgrundlagen der §§ 7 und 8 BDSG grund-legend zu reformieren und daraus eine praxistauglichere Schadenersatzanspruchs-grundlage zu kreieren. In dieser Schadenersatznorm sollte hinsichtlich der für Verbraucher kaum zu beweisenden haftungsbegründenden und haftungsausfüllenden Kausalität mit gesetzlichen Vermutungen gearbeitet werden. Dadurch könnte zu Gunsten des Verbrauchers vermutet werden, dass bei einem Verstoß gegen eine datenschutzrechtliche Bestimmung stets auch in Rechte eines Verbrauchers eingegriffen wird und dadurch ein Schaden entstanden ist. Ein Schaden in Höhe von EUR 50,00 pro Verstoß halten wir insoweit für angemessen. Der Nachweis eines höheren Schadens im Einzelfall sollte davon unberührt bleiben. Ein Unternehmen, das beibeispielsweise ohne die Einwilligung seiner Kunden 50.000 Adressdaten an Dritte verkauft, hat damit einen Schaden von 2.500.000 EUR verursacht, den betroffenen Kunden ersetzt verlangen können. Allein die Gefahr, durch einen datenschutzrechtlichen Verstoß sich auf der Basis einer in der Praxis durchsetzbaren Schadenersatznorm schadenersatzpflichtig zu machen, wird signifikant dazu beitragen, dass Unternehmen sich eher als bisher gesetzeskonform verhalten.

Dies allein wird als privatrechtliche Maßnahme aber nicht ausreichen. Denn bei geringen Streuschäden machen Verbraucher schon allein aufgrund der hohen Prozesskostenrisiken ihre Rechte nicht geltend. Deshalb sollte den betroffenen Verbrauchern ein geeignetes kollektives prozessuales Instrument an die Hand gegeben werden. Zu denken wäre an ein bereits in der gerichtlichen Praxis in Deutschland bewährtes Prozessrechtsregime. Als von der Grundkonzeption geeignet erachtet wird insoweit das Spruchverfahren, dessen Ursprünge schon bis 1936 zurückreichen. Das heute gültige Spruchverfahrensgesetz (SpruchG) trat am 1. September 2003 in Kraft und ist anwendbar für Verfahren im Zusammenhang mit Abfindungen und Kompensationen bei Unternehmensumstrukturierungen. Das Spruchverfahrensgesetz weist die Besonderheit auf, dass nicht nur diejenigen Betroffenen vom positiven Ausgang eines Verfahrens profitieren, die einen Antrag eingereicht haben, sondern auch alle anderen, die keinen Antrag gestellt haben. Für diese bestellt das zuständige Landgericht den sog. gemeinsamen Vertreter, der damit also die Rechte der „passiv gebliebenen“ vertritt.

Elemente dieses Verfahrensgesetzes die für die Durchsetzung von Ansprüchen im Bereich des Datenschutzgesetzes geeignet erachtet werden sind:
- Zuständigkeit des Landgerichts als Erstinstanz (vgl. § 2 SpruchG)
- die Bestellung eines geeigneten gemeinsamen Vertreters durch das Landgericht für all diejenigen geschädigten Verbraucher, die nicht selbst eine Klage einreichen (vgl. § 6 Abs. 1 SpruchG)
- Vergütung und Ersatz der Auslagen des gemeinsamen Vertreters auf der Basis des Rechtsanwaltsvergütungsgesetzes (vgl. § 6 Abs. 2 SpruchG)
- Wirkung der gerichtlichen Entscheidung für und alle, die von einem bestimmten Verstoß betroffen sind (vgl. § 13 SpruchG).

7) Beschlüsse der Verbraucherschutzministerkonferenz (VSMK)

Die Verbraucherkommission unterstützt die Beschlüsse der VSMK vollumfänglich. Eine zeitnahe Umsetzung der Beschlüsse der VSMK 2011 durch Bundesregierung wird empfohlen (siehe vorläufiges Protokoll der 7. VSMK zum Thema Datenschutz, TOP 23).

8) Verzahnung

Die primäre Verantwortung für die Durchsetzung der Datenschutzregeln liegt bei den Unternehmen. Die staatliche Verantwortung ist gleich mehrfach geteilt, zwischen dem Bund und den Ländern. In Bayern kommt dem Landesamt für Datenschutzaufsicht eine zentrale Aufgabe zu. Die Verbraucherorganisationen tun das ihre um die Einhaltung derjenigen Regeln zu überwachen, die für die Verbraucher von unmittelbarem Interesse sind. Mittels der AGB- bzw. UWG-Unterlassungsklage haben sie einen Rechtsbehelf zur Verfügung, mittels dessen sie die Marketingpraktiken und in die Ausgestaltung der AGB eingreifen können.

Notwendig und geboten ist eine stärkere institutionelle Verzahnung der verschiedenen Verantwortungsträger. Hier kann der Freistaat Bayern eigene und neue Wege beschreiten, ohne dass es zu einem Kompetenzkonflikt mit dem Bund oder dem EU-Gesetzgeber kommt.

Konkret schlägt die Verbraucherkommission vor, dass der Freistaat Bayern den Verbraucherorganisationen das Recht einräumt, sich mit einer Beschwerde an das Landesamt zu wenden, das gesetzlich verpflichtet werden sollte, dieser Beschwerde nachzugehen und im Falle der Ablehnung einen mit Gründen versehenen Bescheid zu verfassen, der der judiziellen Überprüfung zugänglich ist.

Gleichfalls regt die Verbraucherkommission an, dass bei der auf Bundesebene zu initiierenden Ausarbeitung von Selbst-Kontrollmaßnahmen sichergestellt ist, dass die Unternehmen verpflichtet werden, über die Maßnahmen jährlich Bericht zu erstatten, die sie ergriffen haben, um dem zu erarbeitenden Kodex Genüge zu tun und dass diese Berichte öffentlich zugänglich gemacht werden (im Internet).