DGRI e. V. • Emmy-Noether-Str. 17 • D-76131 Karlsruhe

Bundesministerium der Justiz und für
Verbraucherschutz
Frau Silvia Bartodziej
Mohrenstraße 37
10117 Berlin

Dr. Anselm Brandi-Dohrn, maître en droit
1. Vorsitzender
Rechtsanwalt
Oranienstraße 164, D-10969 Berlin

Telefon: +49-30-61 68 94 09
Telefax: +49-30-61 68 94 56
E-Mail: abrandi-dohrn@boetticher.com

Berlin, 15. August 2014

Entwurf eines Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts

Hier: **Stellungnahme der Deutschen Gesellschaft für Recht und Informatik e.V. (DGRI e.V.)**

Ihr Zeichen: I B 1 - 3420/12-1-3-3 – 11 785/2014

Sehr geehrte Damen und Herren,

die *Deutsche Gesellschaft für Recht und Informatik e.V.* (DGRI) bedankt sich für die Gelegenheit zur Stellungnahme zu oben genanntem Gesetzesentwurf.

I.

Die ***Deutsche Gesellschaft für Recht und Informatik e.V. (DGRI)*** ist eine neutrale, unabhängige, wissenschaftliche Vereinigung. Sie befasst sich mit Fragen im Bereich der Schnittstelle zwischen Informatik und EDV-Technik einerseits sowie Recht und Wirtschaft andererseits. Sie hat sich die Förderung der Zusammenarbeit von Lehre, Forschung und Praxis in den Bereichen

- Rechtsfragen der Informationsverarbeitung,
- Einsatz der Informationstechnik im Rechtswesen und
- Schaffung der rechtlichen Rahmenbedingungen für die Informationstechnik

zur Aufgabe gestellt. Ansprechpartner der Gesellschaft sind Wissenschaftler und Praktiker in dem so beschriebenen Tätigkeitsfeld sowohl aus dem Gebiet der Rechtswissenschaften als auch der Technik. Mit ihnen sucht die Gesellschaft den Austausch von Wissen, Erfahrungen und Meinungen.

II.

Der „Fachausschuss Datenschutz" der Gesellschaft hat sich mit dem Gesetzgebungsvorhaben befasst; in der nachfolgenden Stellungnahme beschränkt sich die Gesellschaft jedoch bewusst auf den zentralen Aspekt: Die Aufnahme von Datenschutzverstößen in das UKlaG in Form der Änderung des § 2 Abs. 2 UKlaG sowie das Einfügen eines Beseitigungsanspruchs in § 2 Abs. 1 UKlaG, wie in Art. 3 des Gesetzesentwurfs in Ziffer 1. c) vorgesehen:

> *b) Absatz 1 wird wie folgt geändert:*
>
> *aa) In Satz 1 werden nach den Wörtern „auf Unterlassung" die Wörter „und Beseitigung" eingefügt.*
>
> *c) Absatz 2 wird wie folgt geändert:*
>
> *aa) In Nummer 10 wird der Punkt am Ende durch das Wort „und" ersetzt.*
>
> *bb) Folgende Nummer 11 wird angefügt:*
>
> *„11. die Vorschriften, die für die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten eines Verbrauchers durch einen Unternehmer gelten."*

Mit der Änderung in Absatz 2 soll erreicht werden, dass die anspruchsberechtigten Stellen nach § 3 Abs. 1 S. 1 UKlaG auch Datenschutzverstöße, die in Zusammenhang mit der Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten von Verbrauchern begangen werden, verfolgen können. Der neu in Absatz 1 eingefügte Beseitigungsanspruch soll sicherstellen, dass ein Recht auf Löschung durchgesetzt werden kann.

Wir nehmen dazu wie folgt Stellung:

- **Datenschutz ist Persönlichkeitsschutz, kein Verbraucherschutz**

  Der Datenschutz ist ein aus dem Grundgesetz, nämlich Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG, abgeleitetes Recht.

  Nach ständiger Rechtsprechung des Bundesverfassungsgerichts ist das sog. „Recht auf informationelle Selbstbestimmung" Ausfluss des allgemeinen Persönlichkeitsrechts (grundlegend erstmals im *Volkszählungsurteil* erwähnt, BVerfG, Urteil v. 15.12.1983, Az. 1 BvR 209/83 u.a., BVerfGE 65, 1 ff., Rz. 146). Insbesondere soll der Einzelne selbst entscheiden können, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.

  Sämtliche datenschutzrechtlichen Prinzipien, wie z.B. das Verbot mit Erlaubnisvorbehalt, der Grundsatz der Zweckbindung, der Grundsatz der Verhältnismäßigkeit, der Grundsatz der Transparenz etc. fußen letztlich auf diese Erwägungen. Dies gilt auch im Verhältnis zwischen Privaten, denn auch wenn Grundrechte in erster Linie Abwehrrechte des Einzelnen gegen den Staat sind, entfalten sie zwischen Privaten mittelbare Drittwirkung, d.h. zivilrechtliche

Ansprüche sind im Lichte der Grundrechte auszulegen (grundlegend: *Lüth*-Urteil des BVerfG vom 15.01.1958, Az. 1 BvR 400/51, BVerfGE 7, 198ff.).

Diese grundrechtliche Herkunft und Ausprägung des Datenschutzes findet sich auch auf EU-Ebene wieder, siehe Art. 8 der EU-Grundrechtscharta:

> *Artikel 8 Schutz personenbezogener Daten*
>
> *(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.*
>
> *(2) Diese Daten dürfen nur 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."*

Ebenso wie das Bundesverfassungsgericht und die EU-Grundrechtscharta geht auch der Europäische Gerichtshof für Menschenrechte (EGMR) davon aus, dass der Datenschutz Persönlichkeitsschutz ist und dabei immer in Abwägung mit anderen (Grund-)Rechtspositionen steht (vgl. EGMR vom 07.02.2012, Az. 40660/08, GRUR 2012, 745 – *Veröffentlichung von Fotos aus dem Privatleben Prominenter*). **Dabei kommt es gerade nicht darauf an, ob jemand als Verbraucher betroffen ist oder als Unternehmer oder sonst als Person des öffentlichen Lebens.** Es bedarf **stets** einer Abwägung der Grundrechtspositionen im Einzelfall.

Der DGRI ist daher der Auffassung, dass es systemfremd ist, den Datenschutz nunmehr dem Verbraucherschutz gleich zu stellen. Denn:

Ziel des Verbraucherschutzes ist es, für „faire" Marktverhältnisse zu sorgen.

Ziel des Datenschutzes ist dagegen, der Notwendigkeit gerecht zu werden, dass der Einzelne als am Sozialleben Teilhabender zwangsläufig Daten preisgibt, andererseits aber in seinen Persönlichkeitsrechten geschützt sein soll.

Die dabei erforderliche Interessenabwägung ist nicht die Aufgabe von Verbraucherschutzverbänden, welche als „Parteivertreter" auftreten.

- **Das Verfolgen von Datenschutzverstößen ist Sache unabhängiger Aufsichtsbehörden**

Sowohl im BDSG (§ 38 BDSG) wie auch in Art. 8 Abs. 3 der EU-Grundrechtscharta und der EU-Datenschutzrichtlinie 95/46/EG ist vorgesehen, dass die Kontrolle der Einhaltung der Datenschutzgesetze den Behörden obliegt und zwar solchen, die „unabhängig" sind.

§ 38 Abs. 1 S. 1 BDSG lautet wie folgt

> *„Die Aufsichtsbehörde kontrolliert die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5.“*

Die zugrunde liegende EU-Vorschrift findet sich in Art. 28 Abs. 1 der EU-Datenschutz-Richtlinie 95/46 EG:

> *(1) Die Mitgliedstaaten sehen vor, dass eine oder mehrere öffentliche Stellen beauftragt werden, die Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen. Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr.*

Es gibt ferner genaue Regelungen, wie sich ein Betroffener der Hilfe der Datenschutzbehörde bedienen kann, etwa in Abs. 4 des Art. 28 der EU-Datenschutz-Richtlinie 95/46/ EG

> *(4) Jede Person oder ein sie vertretender Verband kann sich zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an jede Kontrollstelle mit einer Eingabe wenden.*
>
> *Die betroffene Person ist darüber zu informieren, wie mit der Eingabe verfahren wurde.*
>
> *Jede Kontrollstelle kann insbesondere von jeder Person mit dem Antrag befasst werden, die Rechtmäßigkeit einer Verarbeitung zu überprüfen, wenn einzelstaatliche Vorschriften gemäß Artikel 13 Anwendung finden. Die Person ist unter allen Umständen darüber zu unterrichten, dass eine Überprüfung stattgefunden hat.*

Sowohl auf EU- wie auch nationaler Ebene ist die Kontrolle der Einhaltung der Datenschutzvorschriften damit bewusst und gezielt in die Hände einer „Datenschutz-Kontrollbehörde“ gelegt. Besondere Eigenschaft dieser Behörde ist – dies ist hervorzuheben –, dass sie ihre Aufgaben in „völliger Unabhängigkeit“ wahrnimmt.

In Deutschland nehmen diese Aufgaben die Aufsichtsbehörden für den Datenschutz wahr, die in jedem Bundesland existieren. Aufgrund des EuGH-Urteils vom 09.03.2010 (Rs. C 518/07), das gegen die Bundesrepublik Deutschland erging, war die Bundesrepublik Deutschland verpflichtet, die Datenschutzaufsicht in Deutschland für den nicht-öffentlichen Bereich neu zu organisieren. Dies führte in der Folgezeit zu einer erheblichen Umgestaltung.

Nach Erfahrung der DGRI sind die deutschen Aufsichtsbehörden für den Datenschutz fachlich sehr kompetent. Sie üben nicht nur Kontrolltätigkeit aus, sondern stehen auch beratend zur Verfügung, sowohl Betroffenen wie auch Unternehmen. Aufgrund dieser Beratungstätigkeit verfügen sie ferner über vertiefte Kenntnisse, was betriebswirtschaftlich und technisch sinnvoll ist, um personenbezogene Daten angemessen zu schützen.

Die Aufsichtsbehörden werden auch von sich aus tätig und nehmen Überprüfungen wahr, wie etwa in den letzten Jahren das bayerische Landesamt für Datenschutzaufsicht in einer groß angelegten Aktion, um Apps für Handys und Smartphones auf ihre datenschutzrechtliche Zulässigkeit zu überprüfen:

> ***„Erneute App-Prüfung zeigt weiterhin erhebliche Mängel beim Datenschutz***
>
> *Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat erneut im Rahmen einer internationalen Prüfungsaktion 60 Apps bayerischer und internationaler Anbieter überprüft und dabei wiederum erhebliche Mängel bei der Information über den Umgang mit Daten festgestellt. Hinsichtlich der bayerischen Apps ist die Festsetzung von Bußgeldern geplant.*
>
> *Weitere Informationen finden Sie in der Pressemitteilung."*
>
> (Zitat von der Webseite des LDA / Pressemeldung)

- **Rolle und Funktion des betrieblichen Datenschutzbeauftragten**

Daneben gibt es als - weitere - Kontrollinstanz in Deutschland den betrieblichen Datenschutzbeauftragten:

Dessen Aufgabe ist nach § 4 g Abs. Abs. 1 BDSG, auf die Einhaltung der Datenschutzgesetze bei den verantwortlichen Stellen hinzuwirken. Er ist neutral und weisungsfrei sowie der Bedeutung der Thematik wegen direkt der Geschäftsleitung unterstellt, § 4 f BDSG. Er muss die erforderliche Fachkunde aufweisen.

Die DGRI hält die Funktion des Datenschutzbeauftragten für essentiell, denn er ist in die betrieblichen Abläufe eines Unternehmens eingebunden, kennt die IT-Infrastruktur und kann so frühzeitig auf die Umsetzung datenschutzrechtlicher Themen im Unternehmen achten. Seine Tätigkeit zu fördern dient den Interessen des Datenschutzes.

- **Mit den Datenschutz-Kontrollbehörden und den betrieblichen Datenschutzbeauftragten bestehen ausreichende Kontrollmechanismen**

Die Praxis zeigt, dass der Datenschutz eine komplexe Querschnittsmaterie ist, bei der nicht nur persönlichkeitsrechtliche, sondern vor allem auch technische Aspekte, insbesondere der Datensicherheit, ebenso wie betriebswirtschaftliche Belange (die Geschäftsprozesse betreffend, die die Verarbeitung personenbezogener Daten beinhalten) miteinander in Einklang zu bringen sind.

Ausgehend davon, dass jedes Erheben oder Verwenden von personenbezogenen Daten einen Eingriff in Persönlichkeitsrechte darstellt, ist es nach Ansicht der DGRI also richtig, dass die Kontrolle der Einhaltung der diesbezüglichen Gesetze staatlichen unabhängigen Stellen, den Aufsichtsbehörden für den Datenschutz, unterliegt.

Diese verfügen nicht nur über das erforderliche Know-how in rechtlicher und technischer Hinsicht, sondern sind aufgrund ihrer Unabhängigkeit in der Lage, die unterschiedlichen Interessen angemessen in Ausgleich zu bringen. Finanzielle Interessen(-konflikte) gibt es nicht - etwa verhängte Bußgelder fließen in den allgemeinen Haushalt und kommen nicht einer bestimmten Aufsichtsbehörde zugute.

Ferner ist es nach Auffassung des DGRI sinnvoll, dass über den betrieblichen Datenschutzbeauftragten eine Selbstkontrolle der Unternehmen besteht. Dabei unterfällt der Datenschutz und dessen Kontrolle der unternehmensinternen Compliance, die Einhaltung der entsprechenden Gesetze wird damit auch über die Compliance-Organisation im Unternehmen mit überwacht.

Im Ergebnis stellt die Kombination aus Datenschutz-Kontrollbehörden und betrieblichen Datenschutzbeauftragten einen umfassenden Kontroll- und Schutzmechanismus dar, der der Bedeutung des Datenschutzes als grundrechtsgleichem Recht entspricht. Der Aufwand ist hoch, aber dem Schutzgut angemessen.

- **Die Rechtsinstrumente zur Verfolgung datenschutzrechtlicher Verstöße sind ausreichend**

Ist ein Betroffener der Ansicht, seine personenbezogenen Daten seien unzulässigerweise erhoben oder verwendet worden, kann er sich an die zuständige Datenschutzbehörde wenden. Diese klärt den Fall weiter auf, ergreift gegebenenfalls die ihr zustehenden Mittel nach § 38 BDSG, was bis zur Verhängung von Bußgeldern von bis zu € 300.000 gehen kann - bei einer grundsätzlichen persönlichen Haftung desjenigen, der den Datenschutzverstoß zu verantworten hat.

Die Praxis der Mitglieder der DGRI, ebenso wie die von allen deutschen Datenschutzbehörden alle 2 Jahre veröffentlichen Tätigkeitsberichte zeigen, dass dieses Mittel häufig gewählt wird: Zahlreiche Betroffene wenden sich in Fragen oder mit Beschwerden an die Datenschutzbehörden, die sodann ermitteln.

Das jüngste Beispiel ist die Entscheidung des VG Ansbach vom 12.08.2014 zur datenschutzrechtlichen Zulässigkeit von sog. *Dashcams*, also an der Windschutzscheibe privater Kfz angebrachte Kameras, die das Verkehrsgeschehen fortwährend mitfilmen, um im Falle eines Unfalls o.Ä. auf den Film zu Beweiszwecken zugreifen zu können.

Solche Beschwerden sind für die Betroffenen in der Regel nicht mit finanziellem Aufwand verbunden, so dass insofern keine Hemmschwelle besteht.

Die Sanktionen des Datenschutzrechts sind dabei durchaus erheblich:

- Neben dem schon erwähnten Bußgeld bis zu € 300.000 ist seit 01.09.2009 eine Gewinnabschöpfung im BDSG vorgesehen,
- in bestimmten Fällen liegt sogar ein Straftatbestand vor, § 44 BDSG.
- Daneben gibt es in Form des § 42 a BDSG den sog. „Datenschutzpranger“, also eine Selbstanzeigepflicht, die in einzelnen Fällen dazu führen kann, dass ein Unternehmen seinen Datenschutzverstoß in zwei bundesweit erscheinenden Tageszeiten in zwei

halbseitigen Anzeigen kundtun, sich also an den „Pranger“ stellen muss.

- Ferner kann schon heute auf der Grundlage des UWG gegen Datenschutzverstöße vorgegangen werden. Es handelt sich dabei zwangsläufig um Einzelfallentscheidungen, in denen aufgrund des wettbewerbsrechtlichen Bezugs die Entscheidung durch ein Zivilgericht erfolgt; der Blickwinkel ist dabei immer ein wettbewerbsrechtlicher, kein datenschutzrechtlicher. Dies ist solange zulässig, wie es – auch – um eine Wettbewerbsverletzung geht, da insofern eine Schnittmenge zwischen UWG und BDSG besteht, die es rechtfertigt, den nach § 8 UWG Berechtigten die Aktivlegitimation zuzuerkennen.

  Voraussetzung ist aber stets der wettbewerbsrechtliche Bezug; dieser sorgt zugleich dafür, dass im Ergebnis nicht der Schutz der Persönlichkeitsrechte des Einzelnen im Vordergrund steht, sondern der Schutz des Marktes und des lauteren Wettbewerbs; der Persönlichkeitsrechtsschutz ist dabei nur Mittel zum Zweck, den Markt im Sinne eines fairen Verhaltens zu regeln.

Diese Rechtsinstrumente sind nach Ansicht der DGRI ausreichend, um hinreichenden Datenschutz sicherzustellen. Ein - lediglich behauptetes - Vollziehungsdefizit durch das Einschalten von Verbraucherschutzverbänden zu kompensieren ist nicht zielführend.

Die Praxis zeigt, dass Datenschutzverstöße in der Regel nicht zielgerichtet begangen werden, sondern auf Unwissenheit oder Unachtsamkeit Einzelner beruhen. Hier kann die Bedeutung der Aufsichtsbehörden in der Aufklärung nicht hoch genug eingeschätzt werden.

Wesentlich erfolgversprechender als das Schaffen einer neuen Verfolgungsinstanz ist daher eine Stärkung der personellen Ressourcen der bestehenden Aufsichtsbehörden.

- **Die Grenze der möglichen Klagebefugnis bleibt völlig unklar, Rechtsunsicherheit wäre die Folge**

Nach dem Gesetzesvorschlag nimmt § 2 Abs. 2 Nr. 11 UKlaG auf die Datenschutzbestimmungen insgesamt Bezug. Dabei bleibt unklar, was mit dem Bezug gemeint ist:

Kann etwa ein Verbraucherschutzverband nunmehr behaupten, dass ein betrieblicher Datenschutzbeauftragter nicht „fachkundig“ im Sinne von § 4f Abs. 2 Satz 1 BDSG ist? Oder kann er monieren, dass das Unternehmen nicht die gem. § 9 BDSG erforderlichen technischen und organisatorischen Maßnahmen ergriffen hat? Kann er Unterlassung fordern, wenn ein Hinweisschild für eine Videokamera, die auch Verbraucher erfasst, nach Ansicht des Verbraucherschutzverbandes 3 cm zu klein ist?

Wer einmal in einem Unternehmen den Datenschutz begleitet hat, weiß wie komplex seine Umsetzung ist. Auf der einen Seite steht der Schutz der Betroffenen vor einer übermäßigen Verdatung, daneben auch der Schutz der Daten selbst – oftmals ohnehin schon im Fokus der IT-Sicherheit -, ebenso wie die IT-technischen Möglichkeiten und erforderlichen Kosten auf Seiten der Unternehmen.

Hier zeigte sich bisher, dass eine Abstimmung mit dem betrieblichen Datenschutzbeauftragten

und/oder der zuständigen Aufsichtsbehörde zu den bestmöglichen Lösungen führt. Es gibt selten „die eine rechtmäßige“ Lösung; nicht zuletzt aus diesem Grund ist es schwer vorstellbar, dass ein Verbraucherschutzverband diesbezüglich ein Klagerecht besitzen soll.

Verbraucherschutzverbände haben primär ein Interesse, Unterlassungsansprüche geltend zu machen. Die Datenschutzbehörden dagegen unterstützen auch, zulässige Alternativen zu finden und zu implementieren. Dies ist etwas, was ein Verbraucherschutzverband weder leisten will noch kann.

Ferner ist zu beachten, dass Verbraucherschutzverbände im Regelfall den Weg des einstweiligen Verfügungsverfahrens wählen. Es kann einem Unternehmen also eine Untersagungsverfügung drohen in Bezug auf eine bestimmte IT-technische Umsetzung mit weitreichenden Konsequenzen auch für andere Datensätze, ohne dass das Unternehmen vor Erlass einer solch potentiell einschneidenden Entscheidung überhaupt gehört wurde.

Der Datenschutz ist in vielen Punkten auch zu komplex, um ihn im Rahmen eines einstweiligen Rechtsschutzverfahrens sachgerecht beurteilen zu können.

Die DGRI ist daher der Auffassung, dass es nicht richtig ist, wenn Verbraucherschutzverbände *umfassend* Datenschutzverstöße verfolgen können, also weit über den Bereich von Verstößen hinaus, die wettbewerbsrechtliche Relevanz haben. Weder ist dies ihre Aufgabe noch entspricht dies dem Schutzgedanken des Datenschutzes durch staatliche Stellen. Vielmehr ist die derzeitige Rechtslage ausreichend, nach der bei bestimmten wettbewerbsrechtlichen Bezügen auch durch Verbände ein Vorgehen möglich ist - aber eben nur bei solchen wettbewerbsrechtlichen Bezügen und nicht generell bei Datenschutzverstößen.

- **Die Missbrauchsgefahr ist hoch mit weitreichenden Konsequenzen für die Unternehmen**

Die Praxis der letzten Jahre zeigt zudem, dass das Missbrauchsrisiko im Abmahnbereich ganz erheblich ist: Gerade mit dem Mittel einstweiliger Verfügungen im Datenschutz könnten Unternehmen empfindlich geschädigt werden. Wird die Verfügung später aufgehoben, stellt sich die Frage, an wem sich das Unternehmen schadlos halten soll.

So sieht die DGRI eine ganz erhebliche Gefahr, dass der Datenschutz zum einseitigen Druckmittel wird. Bereits jetzt tragen Veröffentlichungen von Aufsichtsbehörden dazu bei, Unternehmen in der Öffentlichkeit unter erheblichen Druck zu bringen. Dies ist gerechtfertigt, wenn der Sachverhalt klar ermittelt und die Rechtslage eindeutig ist, aber nicht, wenn es um eine „Verdachtsberichterstattung“ von Verbraucherschutzverbänden geht.

- **Der neue Beseitigungsanspruch führt zu Rechtsunsicherheit und ist im Hinblick auf die Löschung nicht erforderlich**

Nach der Gesetzesbegründung zielt der Begriff „Beseitigung“ offenbar darauf ab, dass unbefugt erhobene oder genutzte Daten gelöscht oder gesperrt werden.

Der Entwurfswortlaut formuliert eine solche Eingrenzung jedoch nicht, sondern spricht allgemein von „Beseitigung“. Daten können jedoch nicht „beseitigt“ werden – und entsprechend kennt auch das BDSG diesen Betriff nicht; sollten die Maßnahmen des BDSG gemeint sein, wäre angezeigt, dieselbe Terminologie zu benutzen.

Dazu kommt, dass dem klagenden Verbraucherschutzverband etwaige bestehende Aufbewahrungspflichten des beklagten Unternehmens nicht bekannt sein können; so entsteht ganz erhebliche Rechtsunsicherheit darüber, was alles von einer Beseitigung umfasst sein soll und wie eine „Daten-Beseitigung“ konkret aussehen bzw. wie ein Zivilgericht sie konkret tenorieren soll.

Abgesehen davon, dass schon die Erweiterung des UKlaG auf die Unterlassung von Datenschutzverstößen gegenüber Verbrauchern – siehe ausführlich oben – nach Ansicht der DGRI nicht sachgerecht ist, gilt dies umso mehr für den allgemeinen Beseitigungsanspruch.

Zudem bestünde für einen ergänzenden Lösch-/ Sperranspruch keinen Bedarf, denn dieser ist ausreichend und wirksam in § 35 BDSG geregelt:

Der Betroffene kann sich mit seiner Forderung nach Löschung oder Sperrung direkt an das Unternehmen wenden. Zeigt dies keine sofortige Wirkung, kann er jederzeit die Aufsichtsbehörden einschalten. Die Erfahrung zeigt, dass es spätestens mit Einschaltung der Aufsichtsbehörden zu einer Löschung/Sperrung kommt. Im Zweifelsfall kann die Aufsichtsbehörde eine Löschung auch direkt anordnen. Ein solches Verfahren ist in der Praxis effektiver als der Gang zu Gericht.

Zudem stehen dem Betroffenen umfangreiche Auskunftsansprüche nach § 34 BDSG gegenüber dem Unternehmen zu, die in der Regel auch kostenlos vom Unternehmen zu erfüllen sind.

- **Es ist zweifelhaft, ob der Gesetzesentwurf europarechtskonform ist**

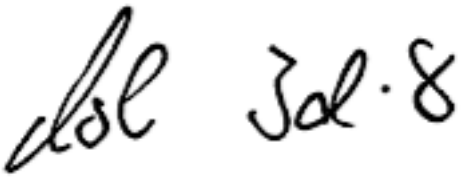
Der Datenschutz wurde in Europa mit der Richtlinie 1995/46/EG harmonisiert. Es ist deshalb zweifelhaft, ob das Einräumen einer Klagebefugnis für Verbraucherschutzverbände, welche nicht in der Richtlinie vorgesehen ist, europarechtskonform ist.

Aus Sicht des DGRI widerspricht die geplante Klagebefugnis für Verbraucherschutzverbände der Vorgabe des Art. 28 Abs. 1 der Richtlinie 1995/46/EG, der europaeinheitlich vorsieht, dass die Einhaltung des Datenschutzes durch unabhängige Kontrollstellen wahrgenommen wird.

Dem widerspricht eine Übertragung von Überwachungsbefugnissen auf private Verbraucherschutzverbände.

Zusammenfassend

- darf der Datenschutz nicht mit dem Verbraucherschutz gleichgesetzt werden, da er ein grundrechtsgleiches Recht ist und eine Abwägung von Grundrechtspositionen erfordert;
- dementsprechend muss die Überwachung des Datenschutzes unabhängigen Kontrollstellen vorbehalten sein, nicht Verbraucherschutzverbänden mit kommerziellen und/oder einseitig dem Verbraucherschutz untergeordneten Interessen;
- sind die bisherigen Rechtsinstrumente zur Verfolgung datenschutzrechtlicher Verstöße ausreichend und wäre einem behaupteten Vollzugsdefizit allenfalls durch Verbesserung der Ausstattung der Aufsichtsbehörden zu begegnen;
- schafft der Gesetzesentwurf Rechtsunsicherheit, weil nicht klar ist, für welche Datenschutzverstöße eine Klageberechtigung besteht und was von einem Beseitigungsanspruch erfasst sein soll;
- besteht eine erhebliche Missbrauchsgefahr, da (Massen-)Abmahnungen zunehmend zu einem speziellen Geschäftsmodell werden und das Thema Datenschutz für die Unternehmen aufgrund der Öffentlichkeitswirksamkeit ein großes Druckpotential aufweist;
- dürfte der Gesetzesentwurf nicht europarechtskonform sein, da er entgegen Artikel 28 der EU-Richtlinie 1995/46/EG die Überwachung des Datenschutzes nicht unabhängigen Kontrollbehörden zuweist.



- an der Unterschrift gehindert -

Dr. Anselm Brandi-Dohrn
Vorsitzender der DGRI e.V.

Dr. Sybille Gierschmann LL.M.
Leiterin FA Datenschutz

Dr. Robert Selk LL.M.
Leiter FA Datenschutz