KARSTEN KINAST / MARKUS SCHRÖDER

Audit & Rating: Vorsprung durch Selbstregulierung

Datenschutz als Chance für den Wettbewerb

Selbstregulierung
Audit
Rating
Wettbewerb
Datenschutzstandards

■ Das Datenschutzrecht befindet sich gegenwärtig im Umbruch. Auf europäischer Ebene hat die EU-Kommission kürzlich den Entwurf einer Datenschutz-Grundverordnung vorgelegt. Doch auch auf nationaler Ebene werden verschiedene Ansätze, die von einer BDSG-Reform bis zur Stiftung Datenschutz reichen, diskutiert. So begrüßenswert diese Ansätze sind, so unbefriedigend bleiben sie vor allem in einem Punkt: der Förderung von selbstregulatorischen Ansätzen. Schließlich bieten diese die Möglichkeit, den Datenschutz als Qualitätsmerkmal und damit als Wettbewerbsvorteil zu etablieren. Dieser Beitrag zeigt Möglichkeiten auf, durch eine Selbstregulierung mittels Datenschutzaudits und -ratings den Datenschutz als Wettbewerbsvorteil nutzen zu können.

■ Data protection law is currently in turmoil. On a European level, the EU Commission recently presented a draft of a data protection basic regulation. However, also on the national level, different basic approaches are being discussed which reach from a reform of the BDSG to the Stiftung Datenschutz. As laudable as these approaches are, they all remain unsatisfactory in one aspect: the promotion of self regulatory approaches. Ultimately, these approaches grant the possibility of establishing data protection as a quality characteristic and, thus, as a competition advantage. This article will depict possibilities on how to use the data protection as a competition advantage through self regulation with the help of data protection audits and ratings.

I. Bestehende Datenschutzpflichten für Unternehmen – Mehr Qual als Wahl

Jegliches Unternehmen, das personenbezogene Daten mittels Computertechnik erhebt, verarbeitet oder nutzt, unterfällt den Regelungen des BDSG. Neben der Einhaltung der Regeln, die die Datenverarbeitung als solche betreffen,[1] gilt es, eine Vielzahl weiterer Datenschutzpflichten einzuhalten. So muss, wenn mehr als neun Arbeitnehmer im Unternehmen mit der automatisierten Datenerhebung und -verarbeitung beschäftigt sind, ein Beauftragter für Datenschutz bestellt werden (§ 4f BDSG). Alternativ bestehen Meldepflichten an die zuständige Aufsichtsbehörde. Weiterhin existieren weitgehende Vorabkontrollpflichten, etwa dann, wenn die Datenverarbeitung besondere Risiken für die Rechte des Betroffenen mit sich bringt (§ 4d Abs. 5 BDSG) oder personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung erhoben und genutzt werden. Der Arbeitgeber muss die Mitarbeiter zur Beachtung des Datengeheimnisses während und nach Beendigung der Tätigkeit im Unternehmen individuell verpflichten, § 5 BDSG. Die verantwortliche Stelle treffen weiterhin Benachrichtigungs- und Auskunftspflichten gegenüber dem Betroffenen, §§ 33, 34 BDSG. Eine Übersicht über Dateien und Datenverarbeitungsanlagen ist aktualisiert vorzuhalten und auf Anfrage jedermann in geeigneter Weise verfügbar zu machen, § 4g Abs. 2 Satz 2 BDSG.

Das alles – und noch viel mehr. Eine Frage stellt sich den Unternehmen in der Praxis vor diesem Hintergrund oft: Wenn denn nun schon ein solcher Aufwand zu betreiben ist – führt das zu einem adäquaten Datenschutz, der auch vom Betroffenen wahrgenommen wird und der so darstellbar ist, dass der Betroffene Marktteilnehmer in deren Datenschutzbestrebungen vergleichen kann? Stimmt also das Preis-Leistungs-Verhältnis gleichsam für den Datenschutzverpflichteten wie für den -berechtigten?

II. Nicht vorgesehen: Datenschutzstandards selbst mitgestalten, vergleichbar machen

Datenschutz-Rentabilität im vorbenannten Sinne ist in der Tat bisher kein rechtlich oder tatsächlich vorherrschendes Prinzip. Es gibt derzeit keine etablierten Möglichkeiten für jedwede verantwortliche Stelle, das eigene Bemühen um den Datenschutz durch für den Betroffenen leicht verständliche Maßnahmen, die auf praktikablen und verantwortungsvoll selbst mitgestalteten Bedingungen fußen, nach außen transparent zu machen.

Zwar gibt es durchaus gesetzliche Grundlagen für orientierungsgebende Datenschutzmaßnahmen (§§ 9a, 38a BDSG), einige Prüfansätze und -siegel (EuroPriSe, Grundschutz-Handbuch des *BSI*) und weitere datenschutzpolitische Intentionen (*Stiftung Datenschutz*, Feststellungen der *Art. 29-Datenschutzgruppe*). Doch hat sich keiner der bestehenden Ansätze durchgesetzt und nicht einer erfüllt die Kriterien der nachhaltigen Transparenzschaffung für den Betroffenen bei gleichzeitiger (Mit-)Gestaltungsmacht der verantwortlichen Stelle:

■ § 9a BDSG ermöglicht es dem Unternehmen, Konzepte, Programme und Systeme abstrakt auditieren zu lassen, jedoch nicht deren Anwendung im Einzelfall[2] – worauf es jedoch gerade ankommen dürfte. Schließlich will ein Betroffener sicher sein können, dass „sein" Unternehmen den Datenschutz ihm gegenüber einhält und nicht etwa nur abstrakt datenschutzkonforme Produkte verwendet. Weiterhin mangelt es an einem Bundes-Audit-Gesetz gem. § 9a Satz 2 BDSG oder einer entsprechenden Verordnung.[3] Datenschutzauditverordnungen auf Landesebene gibt es zwar vereinzelt,[4] eine befruchtende Wirkung für ganz Deutschland hat jedoch bislang nicht stattgefunden.

■ § 38a BDSG erlaubt es Berufsverbänden oder ähnlichen Gruppierungen, den Aufsichtsbehörden selbstregulatorische

1 Etwa Datenvermeidung und Datensparsamkeit gem. § 3a BDSG; Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung gem. § 4 BDSG; Rechtmäßigkeit der Datenübermittlung gem. § 4b BDSG.

2 Weiterentwicklung des Datenschutzrechts aus Sicht des *Bundesbeauftragten für Datenschutz*; Rede von *Peter Schaar* anlässlich einer Informationsveranstaltung des *Gesamtverbands der Versicherungswirtschaft* am 18.2.2004 in Bonn, abrufbar unter: http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/RedenUndInterviews/Archiv/PM04-04WeiterentwicklungDesDatenschutzrechtsAusSichtDesBfD.html?nn=409346.

3 Vgl. *Grentzenberg/Schreibauer/Schuppert*, K&R 2009, 535, 541 f.; vgl. auch die Stellungnahme der *Deutschen Vereinigung für den Datenschutz* (*DVD*) *e.V.*, abrufbar unter: http://www.datenschutzverein.de/Themen/DVD-Stellungnahme%20AuditDSG.pdf und der *Deutschen Gesellschaft für Recht und Informatik* (*DGRI*) *e.V.*, abrufbar unter: http://dgri.de/index.php/fuseaction/download/lrn_file/stellungnahme_070907_auditgesetz.doc.

4 Etwa Bremische Datenschutzaudit-Verordnung von 2004 (Brem. GBl., S. 515) oder Schleswig-Holsteinische Landesverordnung über ein Datenschutzaudit von 2009 (GVBl. 2008, S. 562, 2009, S. 742).

Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen vorzulegen. Dies stellt sich jedoch als theoretische Möglichkeit dar, die einer wirklichen Selbstregulierung keinen Raum lässt.[5] Datenschutz-Kodizes sind existent, beinhalten aber nicht einmal den Begriff BDSG oder dessen § 38a.[6] EuroPriSe, das Siegel-Projekt der Europäischen Union, das eine europäische Datenschutz-Zertifizierung von IT-Produkten und -Dienstleistungen etabliert, dürfte als tatsächlich operierendes Beispiel durchaus als Beweis dafür dienen, dass Datenschutz ein Wettbewerbsfaktor sein kann. Doch ist die Anwendbarkeit auf Produkte und Dienstleistungen begrenzt und gerade für Produkte kann hier keine definitive Compliance mit den rechtlichen Vorgaben attestiert werden, sondern „nur" die Eigenschaft des Produkts.[7] Das dieses Produkt einsetzende Unternehmen kann sich also allenfalls mittelbar mit dem Ergebnis schmücken. Auch insoweit haben wir es naturgemäß mit einer abstrakten Datenschutzaussage zu tun, die den Verbraucher für seine konkrete Situation nicht darüber aufklärt, ob seine personenbezogenen Daten tatsächlich rechtmäßig gehandhabt werden. Auch selbstverpflichtende Elemente sind nicht gegeben. Vielmehr wird im Zuge der Prüfung auf die europäische Datenschutzgesetzgebung, insbesondere die RL 95/46/EG, abgestellt, was nicht automatisch bedeutet, dass das Produkt den nationalen Maßgaben genügt.

- Der IT-Grundschutz-Katalog des *BSI* ist zwar umsetzungsorientiert, bezieht sich jedoch primär auf die Datensicherheit und nicht auf eine Umsetzung des Datenschutzes. Auch hier fließen keine selbstregulatorischen Elemente ein. Der *BSI*-Grundschutz spielt nicht nur daher in der Praxis fast überhaupt keine Rolle – nur wenige Unternehmen entscheiden sich für diese Variante der Zertifizierung nach ISO 27001.[8]
- Die *Stiftung Datenschutz für mehr Sicherheit im Internet*, eine öffentlich-rechtliche Einrichtung, soll den praktischen Aspekt der Datenschutz-Regulierung zukünftig vorantreiben. Dabei ist noch nicht klar, ob es, wie bei EuroPriSe, koalitionsvertragsgemäß um das Testen von Produkten und Verfahren oder deren Anwendung vor Ort beim Unternehmen und deren Dienstleistern gehen soll.[9] Auch ist nicht abschließend geklärt, ob die Aktivitäten auf den Internet-Datenschutz beschränkt bleiben. Weiterhin wurde der Start der *Stiftung Datenschutz* nach Beteuerungen des *Bundesinnenministeriums* in 2011, noch im laufenden Jahr die Arbeit aufzunehmen,[10] auf 2012 unbestimmt verschoben[11] und bleibt in Bezug auf die diskutierte Finanzierung u.a. durch Unternehmen, die bisher nicht durch ein adäquates Vorgehen in Datenschutzfragen aufgefallen sind,[12] im Fokus kritischer Berichterstattung[13] und politischer Diskussion.[14]
- Die Darstellungen der *Art. 29-Datenschutzgruppe* sind deutlich: Datenschutz müsse sich mit dem Ziel, Datenschutzgrundsätze umzusetzen, „von der Theorie zur Praxis" bewegen,[15] es müsse sichergestellt werden, dass Rechtspflichten in tatsächliche Datenschutzmaßnahmen übersetzt würden.[16] Dritte sollten Auditmaßnahmen bei der verantwortlichen Stelle durchführen,[17] um eine adäquate Umsetzung der Datenschutzgesetzgebung zu überprüfen.[18] Immer wieder fällt dabei der Begriff der Accountability, der Rechenschaftspflicht, in dessen Zentrum der Gedanke steht, Verantwortlichkeit umzusetzen und erkennbar und überprüfbar zu machen,[19] und bemüht dabei diesen immer wieder als konturlos kritisierten Begriff,[20] den schon die *OECD*-Richtlinien 1980 verwendeten.[21] Doch kann es i.E. kaum der *Art. 29-Datenschutzgruppe* obliegen, konkrete, verbindliche und marktorientierte Regelungen zu setzen oder vorzuschlagen. Dies widerspräche deren vornehmlich beratenden Funktion.

In der Folge lässt sich festhalten: Es besteht durchaus der politische Wille, neben den bereits zumindest grundsätzlich etablierten Instrumentarien der §§ 9a, 38a BDSG weitere Elemente der Selbstregulierung im System des Datenschutzrechts zu etablieren. Auf nationaler Ebene ist in diesem Zusammenhang nochmals auf die Einführung des Datenschutzaudit-Gesetzes hinzuweisen, welche nach wie vor aussteht.[22] Diesbezüglich wird ebenfalls wie dargestellt über die Einführung der *Stiftung Datenschutz* diskutiert. Diese sollte nach dem zwischenzeitlichen Leerlaufen des § 9a BDSG insbesondere für ein bundeseinheitliches Datenschutzzertifizierungsverfahren sorgen.[23] Dies könnte insbesondere durch vergleichende Prüfungen, Studien und Bewertungen geschehen.[24] Doch auch dieser Ansatz wird momentan nicht nachvollziehbar weiterverfolgt und es lässt sich auch nicht abschätzen, ob eine Etablierung der *Stiftung Datenschutz* überhaupt erfolgen wird. Aber auch auf europäischer Ebene finden sich verschiedene Ansätze der Selbstregulierung. Zwar verneinte die *Art. 29-Datenschutzgruppe* kürzlich die Datenschutzkonformität des *IAB*-Selbstregulierungskodizes. Dennoch gehen die *Art. 29-Datenschutzgruppe* selbst als auch der Vorschlag für die DS-GVO von einer notwendigen Stärkung der Selbstregulierung aus. So verwarf die *Art. 29-Datenschutzgruppe* zwar den *EASA/IAB*-Kodex in seiner konkreten Ausgestaltung, zeigte jedoch gleichzeitig den Weg zur Schaffung eines

5 Weiterführend *Kinast*, in: Taeger/Gabel (Hrsg.), BDSG, 2010, § 38a BDSG, insb. Rdnr. 21 f.

6 Vgl. etwa den Entwurf des Datenschutz-Kodex Geodatendienste, abrufbar unter: http://www.bitkom.org/files/documents/Datenschutz_Kodex.pdf oder den Verhaltenskodex für Betreiber von Social Communities bei der *FSM*, die der *Düsseldorfer Kreis* in seinem B. v. 8.12.2011 begrüßt und auch in die Nähe von § 38a BDSG gebracht hat („(Der Düsseldorfer Kreis) unterstreicht, dass eine Anerkennung von Selbstverpflichtungen durch die Datenschutzaufsichtsbehörden gemäß § 38a Bundesdatenschutzgesetz (BDSG) die Gewähr dafür bietet, dass die Anforderungen des geltenden Datenschutzrechts erfüllt werden und ein Datenschutzmehrwert entsteht."), was jedoch keiner Anerkennung nach § 38a BDSG gleichkommt.

7 Weiterführend *Meissner*, in: Bogendorfer (Hrsg.), Datenschutzgespräche 2011 – Datenschutz im Unternehmen. Das Spannungsfeld der einzelnen Interessen, S. 95, 100.

8 Vgl. *Reppner*, BSI-Grundschutz: zu komplex, zu aufwändig, zu deutsch, abrufbar unter: http://www.zdnet.de/magazin/41525300/bsi-grundschutz-zu-komplex-zu-aufwaendig-zu-deutsch.htm.

9 Vgl. Koalitionsvertrag, abrufbar unter: http://www.cdu.de/doc/pdfc/091026-koalitionsvertrag-cducsu-fdp.pdf, S. 106: „Darüber hinaus werden wir eine Stiftung Datenschutz errichten, die den Auftrag hat, Produkte und Dienstleistungen auf Datenschutzfreundlichkeit zu prüfen, Bildung im Bereich des Datenschutzes zu stärken, den Selbstdatenschutz durch Aufklärung zu verbessern und ein Datenschutzaudit zu entwickeln. Wir sind überzeugt, dass mit dieser Lösung auch der Technologiestandort Deutschland gestärkt wird, wenn datenschutzfreundliche Technik aus Deutschland mit geprüfter Qualität weltweit vertrieben werden kann."

10 http://www.heise.de/newsticker/meldung/Bundesinnenminister-will-strengen-Datenschutz-im-Internet-1345763.html.

11 http://www.heise.de/newsticker/meldung/Stiftung-Datenschutz-verzoegert-sich-weiter-1367366.html.

12 So der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, *Wagner*, in einer Presseerklärung v. 8.9.2010, abrufbar unter: http://www.datenschutz.rlp.de/de/presseartikel.php?pm=pm2010090801.

13 *Beuth*, Stiftung Datenschutz ist auf dem Weg zum Papiertiger, Zeit online v. 10.11.2011, abrufbar unter: http://www.zeit.de/digital/datenschutz/2011-11/stiftung-datenschutz-start-verschoben; s. auch Mitteilung des *ULD*, ZD-Aktuell 2012, 02803.

14 *Schaar*, Diskussionspapier für eine Konzeption der Stiftung Datenschutz, abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/KonzeptionStiftungDatenschutz.pdf?__blob=publicationFilehttp://gruen-digital.de/2011/10/stiftung-datenschutz-kommt-vielleicht-2012-und-entpuppt-sich-als-bmi-marionette/.

15 *Article 29 Data Protection Working Party*, WP 173, Opinion 3/2010 on the principle of accountability, S. 3.

16 *Article 29 Data Protection Working Party*, WP 168, 12/2009, Future of Privacy, S. 20.

17 *Article 29 Data Protection Working Party* (o. Fußn. 15), S. 6, 9.

18 *Article 29 Data Protection Working Party* (o. Fußn. 15), S. 6.

19 *Article 29 Data Protection Working Party* (o. Fußn. 16), S. 20; *Article 29 Data Protection Working Party* (o. Fußn. 15), S. 7.

20 So etwa *Haug*, JurPC Web-Dok. 160/2011, Abs. 4.

21 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Paragraph 14.

22 Vgl. hierzu *Grentzenberg/Schreibauer/Schuppert*, K&R 2009, 535, 541.

23 Vgl. hierzu *Wagner*, RDV 2011, 229, 230.

24 *Wagner*, RDV 2011, 229, 231, 232, der jedoch bereits den Nutzen der *Bundesstiftung Datenschutz* aus rechtspolitischer Sicht bezweifelt.

datenschutzkonformen Kodizes auf.[25] Die DS-GVO[26] wiederum regelt in Art. 38 die Schaffung von Selbstregulierungskodizes sowie in Art. 39 die Schaffung von Mechanismen zu Datenschutzzertifizierungen. Leider sind die dort getroffenen Aussagen nur vage und treffen keine verbindliche Regelung zu zertifizierenden Stellen, Zertifizierungsverfahren, anzulegenden Kriterien sowie den Rechtsfolgen der Zertifizierung.[27] Genannt werden dabei ausdrücklich Datenschutzsiegel („seals") und -benotungen („marks"). Diese sollen sektorspezifisch vergeben werden. So ermutigend diese Ansätze auch sind, bleibt jedoch auch hier die Effektivität ihrer Durchsetzung abzuwarten.[28] Ein weiterer Ansatz auf europäischer Ebene ist, wie bereits angesprochen, der Grundsatz der Accountability. Dieser Grundsatz wurde von der *Art. 29-Datenschutzgruppe* in die Diskussion eingebracht.[29] Doch wurde schon durch den gesetzlichen Pflichtcharakter dieser Ansätze die Chance vertan, den Datenschutz als Wettbewerbsfaktor zu etablieren.[30]

III. Accountability derzeit darstellbar?

Nach alledem lässt sich festhalten: Die bestehenden Möglichkeiten, die eigenen Datenschutzbemühungen i.S.d. Accountability gut begreifbar und gewinnbringend darzustellen, sind unterentwickelt. Sie mögen teilweise gesetzlich angelegt, aber nicht nachhaltig geregelt sein. Sie sind, soweit punktuell vorhanden, an der Datensicherheit, nicht am Datenschutz ausgerichtet. Weiterhin werden sie politisch nicht nachhaltig betrieben. Sie sind, so zeigt es die *Art. 29-Datenschutzgruppe* oder auch die grundsätzliche Einigkeit des gesamten politischen Spektrums über die Sinnhaftigkeit einer *Stiftung Datenschutz* per se, gewünscht, aber nicht gegeben. Der deutsche Datenschutz tut sich schwer mit selbstregulatorischen Akten. Zwar existiert mit § 42a BDSG eine Norm, die es deutschen Unternehmen indirekt aufgibt, die eigene Datenschutzorganisation voranzutreiben. Doch zeigt sich auch: Selbstregulierung verbleibt im Repressiven. Es droht die Selbstanzeigepflicht. Proaktive Gestaltung ist zulässig und materiell-rechtlich angezeigt, wird jedoch gesetzlich derzeit nicht gefördert.

Das erscheint problematisch. Der Gesetzgeber hat es selbst bisher nicht überzeugend geschafft, die sperrige, häufig als veraltet empfundene, inzwischen wieder heftig diskutierte Materie „Datenschutz" in die Umsetzung zu treiben.[31] Die Zuständigkeitsbereiche der deutschen Datenschutzaufsichtsbehörden, die die Überprüfung der Umsetzung bislang primär sicherzustellen haben, sind schon die Unternehmenszahlen betreffend immens. Das hat lange Zeit wenige Unternehmen gestört, sondern vielleicht eher beruhigt. Inzwischen haben die Unternehmen aber, und das zeigt sich nicht zuletzt an der Aufmerksamkeit, die Unternehmen dem novellierten § 11 BDSG entgegenbringen, verstanden, dass ein guter Datenschutz unabdingbar ist. Erkennbar gelebter Datenschutz ist ein Marktkriterium geworden. Abgrenzung gegenüber schwarzen Schafen ist gewünscht. Dazu kommt die allerorts im Munde geführte Welle der „Compliance". Unternehmen wünschen es, insgesamt rechtmäßig zu agieren und wollen dies darlegen und auch positiv für sich nutzen können. Ist dem nicht so, können Unternehmen zwar auch erfolgreich am Markt agieren, das Fehlen datenschutzrechtlicher Rechtmäßigkeit ist jedoch mehr als ein geringfügiger Makel. Das zeigen die Wiener Auskunftsverlangen gegen *Facebook*.[32] Andererseits bestehen eben derzeit keine Möglichkeiten, gelebten Datenschutz gewinnbringend und mit Signalwirkung in die Öffentlichkeit zu tragen. Solange es nur die Gefahr gibt, negativ aufzufallen, nicht aber die verhältnismäßige Möglichkeit, gestaltend und in positiver Manier aktiv zu werden, wird das Datenschutzrecht in der Umsetzungsfalle sitzen. Einzig absehbarer Ausweg erscheint in dieser Situation die Selbstbestimmung.

IV. Thesen für einen selbstbestimmten und transparenten Datenschutz

Wie lässt sich nun vor dem soeben beschriebenen Hintergrund ein besserer Datenschutz sowohl für den einzelnen Teilnehmer am Wirtschaftsleben als auch für die Gesellschaft insgesamt erreichen?

1. Selbstverantwortung stärken

Das gesetzgeberische Vakuum und die datenschutzpolitische Unentschlossenheit könnten durch die Unternehmen selbst ausgefüllt werden. Dabei kommt ein Inhouse-Audit, etwa durch den betrieblichen Datenschutzbeauftragten, in Betracht, das klar nach außen transportiert, welche Kriterien dabei eine Rolle gespielt haben und welche Ergebnisse es gegeben hat. Eine Vergleichbarkeit für Dritte ist damit allerdings noch nicht gegeben. Alternativ kommen daher branchenspezifische Audits und ggf. Ratings[33] in Betracht, die z.B. von den in § 38a BDSG vorgesehenen Stellen, also den Berufsverbänden, aber auch von sonstigen Branchengruppierungen, entwickelt und durchgeführt werden, ohne dass dies nur einigen wenigen finanzstarken Unternehmensgruppen obliegt, die etwa die *Stiftung Datenschutz* finanziell fördern könnten, und ohne dass es eines formalen Verfahrens gem. § 38a BDSG bedürfte. I.E. bedeutete dies eine Stärkung der Selbstverantwortung.[34] Einer Oktroyierung eines wenig praktikablen Ansatzes, der sich aus der schwelenden politischen Diskussion um die *Stiftung Datenschutz* u.U. ergeben könnte, wäre damit Vorschub geleistet.

2. Unabhängigkeit und Interdisziplinarität stärken

Zur Realisierung eines solchen Ansatzes fehlen noch die unabhängigen Audit-, Rating- oder gar Zertifizierungsstellen. Diese dürften letztlich jedoch unproblematisch zur Verfügung stehen. Das zeigt etwa die rege EuroPriSe-Akkreditierung von technischen und rechtlichen Experten. Voraussetzungen für die allgemeine Akzeptanz einer solchen Stelle sind jedenfalls deren Unabhängigkeit, Fachkunde und Zuverlässigkeit. Diese hier bereits nachgewiesenen Kriterien gelten stets für eine objektive Bewertung des geregelten und gelebten Datenschutzes.[35]

Aus Qualitätsgründen müssen die Audits gleichermaßen in juristischer und praktisch-technischer Hinsicht durchgeführt werden. Dies ist durch ein Gremium aus Vertretern der Datenschutzwissenschaft und aus der Praxis sowie aus Juristen und Technikern zu gewährleisten, die für die vorherige Festlegung der Prüfkriterien und deren turnusmäßige Aktualisierung verantwortlich zeichnen. Diese unabhängigen Fachvertreter sollten, organisiert durch die in § 38a BDSG genannten Stellen, eine Führungsrolle

25 Vgl. *Schröder*, ZD-Aktuell 2012, 02742 zur Opinion 16/2011.
26 Abrufbar unter: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf.
27 *Hornung*, ZD 2012, 99, 103.
28 So auch *Kuner*, Privacy and Security Law Report 2012, 1, 9.
29 Zunächst wurde die Accountability im WP 168 (o. Fußn. 16) erwähnt und anschließend im WP 173 (o. Fußn. 15) behandelt.
30 So auch *Haug*, JurPC Web-Dok. 160/2011, Abs. 4; zum Datenschutz als Wettbewerbsvorteil vgl. auch *Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, Ein modernes Datenschutzrecht für das 21. Jahrhundert, S. 27, abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/79DSKEckpunktepapierBroschuere.pdf?__blob=publicationFile.
31 Zu Ansätzen einer Novellierung des BDSG vgl. *Schneider/Härting*, ZD 2011, 63.
32 http://europe-v-facebook.org/.
33 Vgl. hierzu *Kladroba*, DuD 2002, 335; *Kolter*, User-Centric Privacy, 2009. Ein Beispiel für branchenspezifische Ratings zur Produkt- und Dienstleistungsbewertung z.B. für die Versicherungswirtschaft ist die *Assekurata Assekuranz Rating-Agentur GmbH*.
34 So auch *Roßnagel*, Das Datenschutz-Audit, Ziff. 2.1, abrufbar unter: http://www.brandenburg.de/sixcms/media.php/2232/rossnag.pdf.
35 Vgl. hierzu auch *Bergt*, ITRB 2012, 45.

bei der Ausarbeitung des Auditierungsprozesses übernehmen, um die bereits thematisierte Unabhängigkeit zu gewährleisten und Interessenskonflikte zu verhindern. Beteiligte Datenschutzverbände wie der *Berufsverband der Datenschutzbeauftragten Deutschlands* (*BvD*) *e.V.* können für eine Verobjektivierung der Voraussetzungen, die die Prüfexperten zu erfüllen haben, sorgen. Auch Verbraucherinteressen müssen in die Abwägung einfließen, um das Ziel zu erreichen, unterstützt durch verbrauchernahe Datenschutzgruppen wie die *Deutsche Vereinigung für Datenschutz e.V.* So können allseits anerkannte de facto-Standards entstehen, ohne dass eine Reißbrettentscheidung zu befürchten wäre.

3. Stimulierung von Wettbewerb, Vergleichbarkeit und Kommunikation nach außen

Bei den Audits und Ratings ist zunächst von einem allgemeinen, branchenübergreifenden Datenschutz- und Datensicherheitsniveau auszugehen, das in einem ersten Schritt abzuprüfen ist. Hierbei geht es um die Erfüllung zumindest der allgemeinen Datenschutzregelungen wie unter Ziffer I. dargestellt. Das gesetzlich verbindliche Niveau muss erreicht sein. Es bedarf verbindlicher Datenschutzregelungen im Unternehmen, die auch dahingehend geprüft werden müssen, ob sie der Belegschaft und den Dienstleistern bekannt sind und auch gelebt werden. Daneben tritt ein weiterer branchenspezifischer Prüfungsteil, für den selbiges gilt. Gerade hier können sich die erforderlichen Vergleichsaspekte ergeben, die die gewünschte Außenwirkung und Vergleichbarkeit des Datenschutzniveaus herstellen helfen. Auf diesem Wege wird die größtmögliche Transparenz sowohl für die Unternehmen selbst als insbesondere auch für den Verbraucher erreicht.[36]

4. Konkret vs. abstrakt

Dadurch bilden die Audits idealerweise nicht allein die „Papierform" des auditierten Unternehmens ab. Vielmehr sorgen Audits für einen lebbaren und vor allen Dingen gelebten Datenschutz, da die tatsächlichen Prozesse abgebildet werden. In Ergänzung hierzu schaffen branchenseitig initiierte Ratings Vergleichbarkeit und Orientierung für den Verbraucher. Ein weiterer Vorteil dieser Mechanismen liegt darin, dass durch eine Anpassung der Audit- und Ratingpunkte an den jeweiligen Stand der Technik die aktuell zu fordernde Compliance abgebildet werden kann.

5. Gelebter Datenschutz entscheidet

Zu berücksichtigen ist bei allen Überlegungen, dass der Datenschutz eine lebendige Materie ist, die sich nur unzureichend in gesetzlichen Normen abbilden lässt. Es kommt eben nicht allein auf die abstrakte Erfüllung der gesetzlichen Pflichten an, da dies ohnehin von den Unternehmen verlangt werden muss.[37] Die beschriebenen Instrumentarien der Selbstregulierung gehen jedoch über diesen Mindeststandard hinaus und schaffen Anreize für Unternehmen, den Datenschutz als Asset ihres Unternehmens zu begreifen.

V. Ausblick

Durch eine an den skizzierten Prinzipien orientierte Durchführung von Audits und Ratings würde sich künftig ein Interessenausgleich zwischen der Wirtschaft und den Verbrauchern erreichen lassen. Begreift man das Potenzial, welches der Datenschutz im Wettbewerb bietet, profitiert der Verbraucher schon dadurch, dass bei den Unternehmen nicht mehr das häufig beklagte „Race to the bottom", sondern vielmehr ein „Race to the top" einsetzen würde. Ebenso profitieren die Unternehmen selbst, indem sie durch eine Verbesserung ihrer Wettbewerbsposition mit einem erheblichen „Return on investment" rechnen dürfen.[38]

Dr. Karsten Kinast, LL.M. (European Legal Informatics) ist Partner bei Kinast & Partner Rechtsanwälte, Externe Datenschutzbeauftragte in Köln, sowie Lehrbeauftragter für Zivil- und Medienrecht an der Hochschule Fresenius.

Markus Schröder, LL.M. (Informationsrecht) ist Rechtsanwalt und externer Datenschutzbeauftragter bei Kinast & Partner Rechtsanwälte, Externe Datenschutzbeauftragte in Köln, sowie Dozent für Datenschutzrecht an der Düsseldorf Law School.

36 So auch *Büllesbach*, in: Büllesbach/Dreier, Konvergenz in Medien und Recht, 2002, S. 213, 227.

37 So auch *Roßnagel* (o. Fußn. 34), Ziff. 2.3.

38 S. auch *Reding*, http://www.heise.de/newsticker/meldung/Reding-EU-muss-beim-Datenschutz-mit-einer-Stimme-sprechen-1476452.html: „Ein hohes Niveau beim Datenschutz stelle hier für die Wirtschaft nicht einen Kosten-, sondern einen Wettbewerbsfaktor dar."