
Stiftung Datenschutz

Eckpunktepapier

9. Dezember 2009

Mitglieder der Arbeitsgruppe:

Der Präsident des Deutschen Anwaltvereins,
RA Prof. Dr. Wolfgang Ewer, Kiel

RA Dr. Peter Bräutigam, München

RA Dr. Markus Brock, Berlin

RA Dr. Helmut Redeker, Bonn

RA Dr. Stephan Scherer, Mannheim

RA Prof. Dr. Jochen Schneider, München

zuständig in der DAV-Geschäftsführung:

RAin Tanja Brexl

Einleitung

Das BDSG ist zwar vor kurzem mehrfach novelliert worden. Durch die Novellen sind die Schwächen des Konzepts und dessen Veraltung eher noch deutlicher geworden. Entsprechend ist der Ruf nach grundlegender Reform eher noch stärker geworden. Eine Stiftung, deren Arbeitstitel "Stiftung Datenschutz" lautet, könnte dazu beitragen, zum einen die Durchsetzung der bestehenden gesetzlichen Anforderungen des Datenschutzes zu verbessern und unter Einsatz marktwirtschaftlicher Instrumente ("Datenschutz als Wettbewerbsvorteil") eine Optimierung des Datenschutzes oberhalb der gesetzlichen Mindeststandards zu fördern sowie die grundlegende neue Weichenstellung bei der Neuregelung des "Datenschutzes" und deren Umsetzung zu unterstützen.

Das Eckpunktepapier will die Aufgabenstellungen und Ausgestaltungen einer solchen Stiftung als neuer Einrichtung darstellen, dazu auch schon Details vorschlagen und diskutieren.

Der **Gang der Überlegungen** beginnt mit der naheliegenden Darstellung der *Stiftung Warentest* als möglichem Vorbild bzw. Modell, wobei zu prüfen ist, ob und ggf. inwieweit Parallelen zur Stiftung Warentest angestrebt und genutzt werden könnten (1.), inwieweit sich Unterschiede ergeben (1. und 2.).

Es folgen die möglichen Aufgaben einer *Stiftung Datenschutz* zu Prüfung und Bewertung (2.). Hier deutet sich schon an, dass die Stiftung aus ihrer Arbeit heraus wichtige Beiträge für die weitere Entwicklung des Datenschutzes und dessen Rezeption, aber auch Evolution beisteuern könnte.

Auch der nächste Abschnitt befasst sich mit der Leistung der Stiftung, nun v. a. vor dem Hintergrund der Kompatibilität des Datenschutzes in Europa bzw. weltweit und damit der Notwendigkeit, sich besonders mit der Gewinnung der Prüf- und Bewertungskriterien, insgesamt mit dem Instrumentarium des Datenschutzes zu befassen (3.).

Denkbar wäre die Verleihung von Gütesiegeln und/oder die Vergabe von Zertifikaten, evtl. (auch) für Prüf-Institute und Akkreditierungsstellen (4). Wie heikel allerdings die Thematik ist, zeigt sich in den Unterschieden der Bewertung von Audits bzw. der Vergabe von Prüfzertifikaten 1., 2. und 4.

Der Kreis schließt sich zur Ergänzung von 1. und 2. mit Behandlung der Fragen, wie eine solche Einrichtung, die nicht Stiftung i. S. des § 80 BGB sein muss, rechtlich ausgestaltet werden könnte und sollte (5.).

Die Darstellung versucht bereits, „Für“ und „Wider“, z. T. auch durch zwischengeschaltete Fragen und deren Beantwortung, abwägend darzustellen. Die einzelnen Abschnitte stammen von verschiedenen Autoren, was dazu führt, dass in einigen Fragen tendenziell unterschiedliche Auffassungen zu Tage treten. Dies kann in diesem frühen Stadium dazu beitragen, die Diskussion zu bereichern.

Gliederung

1. [Modell Stiftung Warentest als Ausgangspunkt](#)
RA Dr. Markus Brock
2. [Prüf- und Bewertungsaufgaben einer eventuellen Stiftung Datenschutz](#)
RA Dr. Helmut Redeker
3. [Mögliche Hauptleistung und zugleich Erarbeitung der Prüfkriterien der in Aussicht genommenen Stiftung](#)
RA Prof. Dr. Jochen Schneider
4. [Verleihung eines Gütesiegels im Zusammenhang mit der Stiftung Datenschutz](#)
RA Dr. Peter Bräutigam
5. [Zur rechtlichen Auskleidung der Stiftung Datenschutz](#)
RA Dr. Stephan Scherer
6. [Schlussenteil](#)

1. Modell Stiftung Warentest als Ausgangspunkt

In Bezug auf die geplante Stiftung Datenschutz bietet es sich an, als Ausgangspunkt für Überlegungen zu einer *Stiftung Datenschutz* zunächst die *Stiftung Warentest* genauer zu betrachten. Da es sich bei der *Stiftung Warentest*, welche am 4. Dezember 1964 durch die Bundesrepublik Deutschland – vertreten durch den Bundesminister für Wirtschaft – als Stiftung bürgerlichen Rechts errichtet wurde,¹ ohne jeden Zweifel um eine inzwischen **45-jährige Erfolgsgeschichte** handelt, stellt sie einen sehr guten Ausgangspunkt für die geplante *Stiftung Datenschutz* dar. Aus diesem Grunde soll im Folgenden überblicksartig erläutert werden, was genau der Gegenstand bzw. die Aufgabe der *Stiftung Warentest* ist und wie sie im Einzelnen organisiert ist. Im Anschluss daran soll der Frage nachgegangen werden, was die Stiftung Warentest so erfolgreich macht und welche ihrer Aspekte für die Stiftung Datenschutz gewinnbringend übernommen werden können. Den Abschluss unserer Ausführungen zur Stiftung Warentest sollen Überlegungen dazu bilden, wo die Stiftung Datenschutz aufgrund ihrer spezifischen Aufgabenstellung eigene Lösungsansätze finden muss, die sich von denen der Stiftung Warentest unterscheiden.

1.1. Was ist Gegenstand der Stiftung Warentest?

Wesentliche Aufgabe der Stiftung Warentest ist es, dem Verbraucher durch vergleichende Tests mehrerer Waren oder Dienstleistungen einer bestimmten Produktparte eine **unabhängige und objektive Unterstützung bei** der entsprechenden **Kauf-/Bezugsentscheidung** zu bieten. Insofern verweisen wir auf folgenden Auszug aus der Satzung der Stiftung Warentest:

"§ 2 Stiftungszweck

(1) Die Stiftung ist selbstlos tätig; sie verfolgt nicht in erster Linie eigenwirtschaftliche Zwecke. Ausschließlicher und unmittelbarer Zweck der Stiftung ist es,

¹ Satzung der Stiftung Warentest (Stand: 1. Januar 2008), abrufbar unter <http://www.test.de/unternehmen>.

- *die Öffentlichkeit über objektivierbare Merkmale des Nutz- und Gebrauchswertes sowie der Umweltverträglichkeit von Waren und privaten sowie individuell nutzbaren öffentlichen Leistungen zu unterrichten,*
- *der Öffentlichkeit Informationen zur Verfügung zu stellen, die zur Verbesserung der Marktbeurteilung beitragen,*
- *die Verbraucher über Möglichkeiten und Techniken der optimalen privaten Haushaltsführung, über eine rationale Einkommensverwendung sowie über von ihr als fundiert erkannte wissenschaftliche Erkenntnisse des gesundheits- und umweltbewussten Verhaltens aufzuklären."*

Was die von der Stiftung Warentest **getesteten Waren und Dienstleistungen** anbetrifft, so nehmen diese ein inzwischen recht **breites Spektrum** ein. Zu den getesteten Waren gehören beispielsweise solche aus den Bereichen Informationstechnik und Telekommunikation, Ernährung, Unterhaltungselektronik, Foto, Haushaltsgeräte und Körperpflege. Was die getesteten Dienstleistungen anbelangt, so stammen diese etwa aus den Bereichen Reise und Freizeit sowie – 1991 durch die separate Zeitschrift "Finanztest" hinzugekommen – aus den Rubriken Recht und Leben, Geldanlage und Altersvorsorge, Bauen und Wohnen, Steuern sowie Gesundheit und Versicherungen. Seit Juli 2002 werden darüber hinaus auch Tests von Weiterbildungsdienstleistungen durchgeführt.²

Die Waren- und Dienstleistungstests, die sich im Jahre 2007 insgesamt auf 187 Warentests mit insgesamt 2.157 überprüften Waren sowie 17 Dienstleistungs- und 73 Finanzdienstleistungstests beliefen,³ werden von der Stiftung Warentest nicht in eigenen Testlaboratorien durchgeführt, sondern vielmehr bei **unabhängigen Testinstituten** in Auftrag gegeben.

² Siehe Publikation der Stiftung Warentest "Auf einen Blick – Aktuell 2008", S. 5 f., abrufbar unter <http://www.test.de/unternehmen>.

³ Siehe Publikation der Stiftung Warentest "Auf einen Blick – Aktuell 2008", S. 4, abrufbar unter <http://www.test.de/unternehmen>.

1.2. Wie ist die Stiftung Warentest organisiert?

Gemäß § 5 der Satzung der Stiftung Warentest verfügt diese über drei Organe, namentlich den Vorstand, den Verwaltungsrat und das Kuratorium.

Der **Vorstand** vertritt die Stiftung Warentest gerichtlich und außergerichtlich und führt ihre Geschäfte (§ 6 Abs. 1 der Satzung). Gegenwärtiger Vorstand ist Herr Dr. Werner Brinkmann, der zusammen mit dem Bereichsleiter Publikationen, Herrn Hubertus Primus, die Geschäftsleitung der Stiftung Warentest bildet.⁴ Gemäß § 6 Abs. 4 der Satzung werden die Mitglieder des Vorstandes vom Verwaltungsrat im Benehmen mit der Stifterin – der Bundesrepublik Deutschland vertreten durch den Bundesminister für Wirtschaft – berufen.

Die wesentliche Aufgabe des **Verwaltungsrats** besteht darin, den Vorstand zu berufen und dessen Tätigkeit zu überwachen (§ 7 Abs. 1 der Satzung). Der Verwaltungsrat besteht aus sieben Personen, die von der Stifterin berufen werden. Gegenwärtig gehören ihm neben seinem Vorsitzenden Herrn Prof. Dr. Karl-Heinz Fezer u. a. der Vorstand Verbraucherzentrale Bundesverband, Herr Gerd Billen sowie der Präsident der Bundesanstalt für Materialforschung und -prüfung, Herr Prof. Dr. Manfred Hennecke, an.⁵

Das **Kuratorium** berät den Vorstand und den Verwaltungsrat insbesondere in allen Fragen von grundsätzlicher Bedeutung, die der Verwirklichung des Stiftungszwecks dienen (§ 8 Abs. 1 der Satzung). Ferner kann das Kuratorium Vorschläge für Untersuchungen einbringen oder auch einzelnen Untersuchungsvorhaben widersprechen.⁶ Es ist zusammengesetzt aus sechs Verbrauchervertretern, sechs Vertretern der anbietenden Wirtschaft und sechs neutralen Sachverständigen (§ 9 Abs. 4 f. der Satzung).

1.3. Was ist das "Erfolgsrezept" der Stiftung Warentest?

Gemäß einer von der Stiftung Warentest zitierten Forsa-Umfrage von Februar/März 2007 **kannten 94 % der bundesweit befragten Personen** (2.004 Bürger ab 18 Jahren) **die Stiftung Warentest.**⁷ Gemäß einem Artikel in "Welt Online" vom 30. Mai 2007 ergab

⁴ Siehe <http://www.test.de/unternehmen/stiftungsgremien>.

⁵ Siehe <http://www.test.de/unternehmen/stiftungsgremien/verwaltungsrat>.

⁶ Siehe <http://www.test.de/unternehmen/stiftungsgremien/kuratorium>.

⁷ Siehe Publikation der Stiftung Warentest "Auf einen Blick – Aktuell 2008", S. 2, abrufbar unter <http://www.test.de/unternehmen>.

diese Forsa-Umfrage, dass die Stiftung Warentest von den zwölf vorgegebenen Institutionen das **höchste Vertrauen der befragten Personen** genoss – vor der Polizei –, wobei knapp $\frac{3}{4}$ der Befragten die Stiftung Warentest als vertrauenswürdig einstufen.⁸ Dieses enorme Vertrauen, das der Stiftung Warentest seitens der deutschen Bevölkerung entgegengebracht wird, hängt wohl zuallererst mit dem anscheinend unerschütterlichen Glauben an die **Neutralität dieser Institution** im Allgemeinen sowie der von ihr durchgeführten Waren- und Dienstleistungstests im Besonderen zusammen. Um diese Neutralität der Stiftung Warentest sicherzustellen, sind ihr beispielsweise laut Satzung bestimmte Einnahmequellen verwehrt:

"§ 12 Beschränkung von Einnahmen

(1) Anzeigen gewerblicher Unternehmen oder von Vereinigungen solcher Unternehmen darf die Stiftung weder entgeltlich noch unentgeltlich veröffentlichen.

(2) Die Stiftung darf Zuwendungen Dritter annehmen, soweit dadurch die Unabhängigkeit ihrer Arbeit nicht gefährdet wird. Die Annahme bedarf der Zustimmung des Verwaltungsrates.

(3) Die entgeltliche wie die unentgeltliche Abgabe von bereits veröffentlichten Untersuchungsergebnissen und neutralisierten Prüfberichten ist der Stiftung gestattet."

Zur Kompensation der der Stiftung Warentest insoweit entgehenden Einnahmen erhält sie jährlich eine staatliche Ausgleichszahlung – beispielsweise im Jahre 2007 in Höhe von 6 Mio. Euro bei Gesamterträgen in Höhe von 50,98 Mio. Euro.⁹ Nichtsdestotrotz vermag es die Stiftung Warentest, ihren **Finanzbedarf zu einem Großteil** durch den Verkauf ihrer eigenen Publikationen (insbesondere der Zeitschriften "test" und "Finanztest") **selbst zu erwirtschaften**. Im Jahre 2007 beispielsweise machten Publikationsverkäufe rund 94 % der gesamten Umsatzerlöse der Stiftung Warentest in Höhe von insgesamt 41,02 Mio. Euro aus.¹⁰

⁸ Exler, Krieg zwischen Stiftung Warentest und Öko-Test, Welt Online, 30. Mai 2007, abrufbar unter http://www.welt.de/wirtschaft/article904772/Krieg_zwischen_Stiftung_Warentest_und_Oeko_Test.html.

⁹ Siehe Publikation der Stiftung Warentest "Auf einen Blick – Aktuell 2008", S. 2 f., abrufbar unter <http://www.test.de/unternehmen>.

¹⁰ Siehe Publikation der Stiftung Warentest "Auf einen Blick – Aktuell 2008", S. 4., abrufbar unter <http://www.test.de/unternehmen>.

1.4. Was kann von der Stiftung Warentest für die geplante Stiftung Datenschutz übernommen werden?

Obgleich an anderer Stelle noch detailliert dazu Stellung genommen werden soll, welche Regularien aus unserer Sicht für die geplante Stiftung Datenschutz sinnvoll wären (z. B. in Bezug auf Organisationsform, Prüfkriterien, Prüfabläufe, Gütesiegel etc.), soll bereits an dieser Stelle darauf hingewiesen werden, dass aus unserer Sicht insbesondere die Übernahme folgender Aspekte der Stiftung Warentest für die Stiftung Datenschutz in Betracht zu ziehen ist:

- Organisatorische sowie finanzielle Ausstattung, die eine **absolute Neutralität** der Stiftung Datenschutz und eine Verhinderung jeglicher Einflussnahme der Anbieter der zu testenden Waren und Dienstleistungen sicherstellt;
- Privatrechtliche Organisationsform, um zu gewährleisten, dass **keinerlei direkte staatliche Einflussnahme auf Testergebnisse** und mithin auf den freien Leistungswettbewerb stattfindet ("wettbewerbliche Neutralität des Staates");
- Organisatorische **Einbindung** der von der Tätigkeit der Stiftung Datenschutz **betroffenen gesellschaftlichen Gruppen** (Verbraucher, anbietende Wirtschaft etc.);
- Gewährleistung einer möglichst umfassenden **Selbstfinanzierung** der Tätigkeiten der Stiftung Datenschutz zur Verhinderung einer übermäßigen Belastung der öffentlichen Haushalte;
- Bemühung um eine möglichst hohe Bekanntheit der Stiftung Datenschutz sowie ihrer Testergebnisse als **Anreiz für Anbieter** betreffender Waren und Dienstleistungen, **freiwillig** – d. h. ohne legislativen oder aufsichtsbehördlichen Zwang – das eigene **Datenschutzniveau zu erhöhen** und durch das werbliche Herausstellen positiver Testergebnisse der eigenen Produkte einen Wettbewerbsvorteil zu erzielen.

1.5. Wo muss die Stiftung Datenschutz aufgrund ihrer spezifischen Aufgabenstellung eigene Lösungsansätze finden?

Zwar bildet unserer Auffassung nach die Stiftung Warentest einen sehr guten Ausgangspunkt für Überlegungen zur Schaffung einer neuen Stiftung Datenschutz. Gleichwohl gibt es jedoch auch einige Aspekte, bei denen die Stiftung Datenschutz aufgrund ihrer spezifischen Aufgabenstellung eigene Lösungsansätze finden muss.

Ein gewichtiger Unterschied zwischen der geplanten Stiftung Datenschutz und der Stiftung Warentest hängt beispielsweise mit dem konkreten **Prüfgegenstand** zusammen. Während sich die Stiftung Warentest bei den von ihr durchgeführten Tests von Waren und Dienstleistungen im Wesentlichen auf öffentlich zugängliche Informationen beschränken kann (Erwerb von im Handel frei erhältlichen Waren zu Testzwecken sowie Beurteilung veröffentlichter Vertragsbedingungen von Dienstleistungsanbietern) ist eine Prüfung von datenschutzrelevanten Dienstleistungen teilweise auch auf **nicht öffentlich zugängliche Informationen über interne Datenverarbeitungsprozesse** angewiesen. Hieraus ergibt sich ein gewisses **Grundproblem der geplanten Stiftung Datenschutz**, für das eine adäquate Lösung gefunden werden muss. Denn weder stehen der Stiftung Datenschutz staatliche Untersuchungsbefugnisse wie etwa den Datenschutzaufsichtsbehörden zu (vgl. etwa § 38 BDSG) noch wird sie ohne weiteres auf von den Anbietern der getesteten Produkte freiwillig offen gelegte Informationen zurückgreifen können, wie dies etwa bei Datenschutzaudit-Verfahren gem. § 9a BDSG oder dem Zertifizierungsverfahren gem. § 4 Abs. 2 Landesdatenschutzgesetz Schleswig-Holstein (LDSG-SH) der Fall ist. Im Gegensatz zu diesen Datenschutzaudit- und Zertifizierungsverfahren, bei denen die Initiative von den Anbietern betreffender Dienstleistungen ausgeht, die zur Erlangung eines entsprechenden Gütesiegels von sich aus an die Prüfstelle herantreten und ihr Einblicke in interne Datenverarbeitungsprozesse gewähren, testet die Stiftung Warentest "ungefragt" auf dem Markt angebotene Produkte. Soll dies auch bei der Stiftung Datenschutz der Fall sein – wofür unseres Erachtens einiges spricht –, dann muss für dieses Problem eine passable Lösung gefunden werden (s. a. zum Problem 2.2).

Denkbar wäre etwa, die Prüfung datenschutzrelevanter Produkte – wie bei der Stiftung Warentest – von vornherein **allein auf öffentlich zugängliche Informationen zu beschränken**. Ob die hierdurch erzielten Testergebnisse jedoch bei Datenverarbeitungsprozessen, die zum Großteil nicht-öffentlich stattfinden, sonderlich aussagekräftig wären, darf zumindest angezweifelt werden.

Eine weitere Möglichkeit bestünde darin, die **Kooperationsbereitschaft eines Unternehmens**, dessen Produkte von der Stiftung Datenschutz geprüft werden sollen, im Rahmen der Prüfung als **eines der Bewertungskriterien** einzeln auszuweisen und in die Gesamtwertung einfließen zu lassen. In einem solchen Fall müsste die Stiftung Datenschutz, nachdem sie sich für eine bestimmte Testreihe mit bestimmten Produkten entschieden hat, für deren Untersuchung die Kenntnis interner Datenverarbeitungsprozesse notwendig erscheint, an die Anbieter der betreffenden Produkte herantreten und sie etwa unter Fristsetzung zur freiwilligen Offenlegung bestimmter standardisierter Informationen auffordern.

Schließlich könnte die Stiftung Datenschutz **nur die Waren und Dienstleistungen solcher Anbieter testen, die sich freiwillig einem derartigen Test unterziehen** und mithin von sich aus Informationen zu ihren internen Datenverarbeitungsprozessen offen legen. Diesem Ansatz stehen jedoch in mehrfacher Hinsicht Bedenken gegenüber: Einerseits wäre bei einem solchen Vorgehen fraglich, ob man bei jeder Testreihe hinreichend viele Anbieter betreffender Produkte für eine Teilnahme gewinnen könnte, um einen aussagekräftigen Vergleich für eine bestimmte Produktparte zu erzielen. Gerade ein solcher aussagekräftiger Überblick über eine bestimmte Produktkategorie scheint jedoch eines der wesentlichen Erfolgsrezepte der Stiftung Warentest zu sein und sollte mithin auch von der Stiftung Datenschutz angestrebt werden. Andererseits bestünde bei einer Beschränkung der Tests auf solche Anbieter, die sich freiwillig zur Verfügung stellen, jedoch insbesondere die Gefahr, dass gerade "schwarze Schafe" einer Branche oder ggf. sogar gesamte Branchen, die datenschutzrechtliche Belange insgesamt nicht sonderlich ernst nehmen, ihre Mitwirkung verweigern würden, was den gesamten Sinn einer Stiftung Datenschutz in Frage stellen würde. Daher wird die Stiftung Datenschutz wohl nicht umhinkommen, sowohl mehrere vergleichbare Waren und Dienstleistungen in einer Testreihe gegenüberzustellen, als auch aussagekräftige Ergebnisse ihrer Tests trotz des Umstands sicherzustellen, dass die Anbieter der betreffenden Produkte letzten Endes nicht zur Offenlegung interner Datenverarbeitungsprozesse gezwungen werden können.

Ein weiterer Unterschied zwischen der Stiftung Warentest und der Stiftung Datenschutz könnte sich daraus ergeben, wessen Schutz Letztere dienen soll. Während die **Stiftung Warentest ausschließlich** dem Verbraucherschutz und damit dem "**B2C-Bereich**" dient, könnte eine **Stiftung Datenschutz** sehr wohl **auch für den "B2B-Bereich" relevant** sein. Denkbar wäre etwa, dass die Stiftung Datenschutz auch solche

datenschutzrelevanten Dienstleistungen getestet, welche von Unternehmen für Outsourcing-Projekte bzw. Auftragsdatenverarbeitungen gem. § 11 BDSG nachgefragt werden. Sollte eine derartige Ausdehnung des Aufgabenspektrums der Stiftung Datenschutz auf den B2B-Bereich gewünscht sein, so müsste dies sowohl im Rahmen der Organisation der Stiftung Datenschutz als auch bei der konkreten Ausgestaltung ihrer Prüfabläufe und -kriterien berücksichtigt werden. (zu Ansätzen des Vergleichs von Applikationen s.a. 2., auch zur Frage der Einbeziehung der Öffentlichen Verwaltung). Vergleichende Tests der Anwender würden mittelbar deren Kunden, also dem Verbraucher zu Gute kommen. Sollte hingegen eine Beschränkung des allgemeinen Prüfungsauftrags der Stiftung Datenschutz auf den B2C-Bereich angestrebt werden, so wäre insoweit ein Sonderweg der Stiftung Datenschutz gegenüber der Stiftung Warentest nicht erforderlich.

2. Prüf- und Bewertungsaufgaben einer eventuellen Stiftung Datenschutz

2.1. Welche Gegenstände sollen von der Stiftung Datenschutz untersucht werden?

2.1.1. Für eine datenschutzrechtliche Prüfung sind sehr unterschiedliche Produkte und Dienstleistungen interessant.

Zum einen kann es um umfassende Dienstleistungen, insbesondere im Internet gehen, bei denen Daten bewusst oder unbewusst vom Verbraucher preisgegeben, vom Anbieter erhoben und gespeichert und eventuell von Dritten ausspioniert werden. So ist es etwa bei einem Bestellvorgang im Internet selbst für herkömmliche Waren notwendig, dass z.B. Anschriften, Kontoverbindungen, Kreditkartennummern usw. gespeichert werden. Darüber hinaus müssen zur Erbringung der Dienste vorübergehend etwa IP-Adressen des Bestellers gespeichert werden, damit mit diesem kommuniziert werden kann. Es werden E-Mail-Adressen für die elektronische Korrespondenz gespeichert und vieles mehr.

Diese Daten werden vom Anbieter teilweise nur vorübergehend, teilweise über längere Zeit gespeichert. In vielen Modellen werden – zumindest bei Einverständnis des Nutzers - bestimmte Daten auf Dauer gespeichert, damit weiterhin etwa Werbe-E-Mails oder Werbefbriefe versandt werden können. Diese Daten dürfen mit Einwilligung des Kunden auch an Dritte weitergegeben werden. Sie können aber vom Provider selbst, von seinen Angestellten ohne seinen Auftrag oder auch von Dritten zweckwidrig und unter Verstoß gegen das Datenschutzkonzept verwendet werden.

Es gibt rechtliche und technische Maßnahmen, um dem vorzubeugen.

Ähnliches gilt auch für Daten, die von Unternehmen für ihre Leistungen an Kunden gespeichert werden, ohne dass die Kommunikation mit den Kunden elektronisch läuft.

Alle Unternehmen speichern ferner Daten von Arbeitnehmern und/oder Lieferanten. Auch diese Daten bedürfen des Schutzes.

Ein zweites Szenario ist, dass der Bürger selbst ein technisches Gerät kauft, auf dem er bewusst Daten speichert oder auf dem unbewusst Daten gespeichert werden. Dies gilt für jeden PC oder Laptop, auf dem der Benutzer in großem Umfang z.B. private Fotos, Adresslisten, Briefverkehr u. ä. speichert. Auf diesen Geräten werden aber auch vom Nutzer unbemerkt Daten über sein Kommunikationsverhalten gespeichert. Auch hier drohen Angriffe Dritter. Darüber hinaus können befugte Benutzer des Laptops bewusst oder unbewusst dort gespeicherte Daten einsehen und verwenden. Dies kann mit oder ohne Wissen des Eigentümers geschehen. Auch hier lassen sich rechtliche und technische Konzepte erarbeiten und prüfen, um dafür zu sorgen, dass dem Endnutzer bei der Benutzung dieses Gerätes keine überflüssigen Risiken entstehen.

Gegenstand solcher Untersuchungen ist kein dem Kunden erbrachter Dienst, sondern die Bewertung eines konkreten Produkts.

Darüber hinaus können auch technische Komponenten Prüfgegenstand sein, die vom Nutzer im Rahmen der eigenen Datenverarbeitung eingesetzt werden, bei der wiederum Daten Dritter gespeichert werden.

Nahezu alle Unternehmen setzen Hardware, Betriebssoftware und Anwendungssoftware ein, die in vielfältiger Weise personenbezogene Daten der Inhaber des Betriebes, seiner Mitarbeiter und seiner Kunden und Lieferanten verarbeiten. Hier muss geprüft werden, wieweit diese Geräte in der Lage sind, Datenschutzvorgaben umzusetzen, das Eindringen Dritter zu verhindern und die technischen Anforderungen an den Datenschutz zu erfüllen.

Alle diese Komponenten können für den Datenschutz von großer Bedeutung sein, weil auch das beste Datenschutz- und Datensicherungskonzept nichts nützt, wenn die eingesetzten Produkte nicht so sicher sind, wie dies z.B. vom Hersteller angegeben wird. Umgekehrt kann Datenschutz ohne entsprechende Konzepte nicht gewährleistet werden.

Die Stiftung Datenschutz muss sowohl die gesamten Dienstleistungen als auch die einzelnen Produkte prüfen können, ob sie den entsprechenden Anforderungen im Hinblick auf den Datenschutz genügen.

Es wird daher empfohlen, hier eine möglichst umfassende Prüfungsbefugnis der Stiftung Datenschutz für sämtliche Produkte und Dienstleistungen vorzusehen, die im Rahmen der Verarbeitung personenbezogener Daten eingesetzt werden oder eingesetzt werden können.

- 2.1.2. Zahlreiche in Deutschland genutzte Dienstleistungen, aber auch Lieferangebote für Produkte stammen von Anbietern, die nicht in Deutschland beheimatet sind.

Die Internationalität des Internets bietet viele Möglichkeiten, die zunehmend genutzt werden. Auch in deutscher Sprache angegebene Angebote sind keinesfalls alles Angebote deutscher Anbieter.

Diese Angebote unterliegen rechtlich jedenfalls in gewissen Umfängen nicht der Prüfung deutscher Datenschutzkontrollbehörden. Sobald diese Anbieter keine Niederlassung in Deutschland unterhalten, dürfte eine solche Prüfung auch faktisch unmöglich sein.

Dennoch besteht hier ein großes Bedürfnis, diese Angebote einer datenschutzrechtlichen Prüfung zu unterziehen.

Es wird eine der wichtigen Aufgaben der Stiftung Datenschutz sein, über deutsche Anbieter hinaus auch die Angebote ausländischer Anbieter, die für den deutschen Markt relevant sind, zu prüfen und zu bewerten.

- 2.1.3. „Dienstleistungen“ im weitesten Sinne werden nicht nur von Privaten, sondern auch von der öffentlichen Hand angeboten. Insoweit ist allerdings zu unterscheiden zwischen

- weitgehend spezialgesetzlich geregelten Aktivitäten im Rahmen staatlicher Verwaltungstätigkeit, also etwa der Verarbeitung von Daten im Bereich der Strafverfolgung, der Ordnungsverwaltung (z.B. Führerscheinwesen) oder der Gesundheitsverwaltung

und

- anderen Dienstleistungen der öffentlichen Hand, die keiner speziellen gesetzlichen Regelung unterliegen und teilweise auch im Wettbewerb mit gewerblichen Angeboten Dritter erbracht werden, wie z.B. den Informations- und Buchungsportale der Kommunen oder der Einrichtung von Diskussionsforen oder Blogs zu konkreten Themen durch verschiedene Behörden.

Für Aktivitäten im erstgenannten Bereich kommt ein Tätigwerden der Stiftung Datenschutz nicht in Betracht, weil es eine effektive Überwachung gibt, nämlich durch die Datenschutzbeauftragten des Bundes, der Länder und der Behörden selbst, durch die staatlichen Aufsichtsbehörden wie z.B. durch die Kommunalaufsicht und auch durch die Verwaltungsgerichte mit der dort geltenden Untersuchungsmaxime. Darüber hinaus unterliegt die Gestaltung dieser Datenverarbeitung einer intensiven öffentlichen Debatte, die einen weiteren Schutz gewährleistet.

Anders sieht dies bei den zusätzlichen, oft auch innovativen Angeboten aus, bei denen Kontrollmechanismen und insbesondere die speziellen gesetzlichen Regelungen fehlen. Dort ist eine Kontrolle und Bewertung durch die Stiftung Datenschutz sinnvoll. Dies gilt noch stärker bei öffentlich-rechtlichen Unternehmen mit eigener Rechtspersönlichkeit, die nicht den Regeln des Datenschutzrechts für die öffentliche Hand, sondern denen für Private unterliegen. Auch diese sollten von der Stiftung Datenschutz überprüft und bewertet werden.

2.2. Wie soll bewertet werden?

Hier stellt sich die Frage, ob Vergleichsbewertungen vorgenommen werden sollen, ein Gütesiegel vergeben werden soll oder ein Datenschutzaudit durchgeführt werden soll.

Die Stiftung Datenschutz soll sich ausdrücklich auch an den bisherigen Arbeiten der Stiftung Warentest orientieren. Zu deren erfolgreichen Testaufgaben gehört der Vergleich verschiedener Hersteller, die für den Verbraucher gleichwertig sind. Entsprechendes gilt im Hinblick für den Datenschutz z.B. für Buchungsportale verschiedener Fluglinien, Internetportale verschiedener Warenhäuser, Hotelreservierungssysteme oder auch Angebote von PCs verschiedener Hersteller.

Schwierig wird die Bewertung dann, wenn – wie in vielen Fällen – auf dem Markt nur sehr wenige oder gar nur ein Anbieter vorhanden sind bzw. ist. Dies gilt zunächst schon für Betriebssoftware für PCs. An Produkten der Firma Microsoft wird man als PC-Nutzer kaum vorbeikommen können, auch wenn man Microsoft kritisch gegenüber steht. Allenfalls Linux ist ein – für Endverbraucher möglicherweise wenig attraktives – Alternativangebot. PCs enthalten auch weitere Bestandteile, die für den Datenschutz

wichtig sind, die aber bei nahezu allen PCs gleich sind, so dass eine Vergleichsuntersuchung nur begrenzten Nutzen hat.

Allerdings kann eine öffentliche kritische Bewertung hier dennoch wichtig sein, weil der Hersteller z.B. seinen Ruf wahren will.

Ein weiterer Gesichtspunkt unterscheidet die Bewertungen der Stiftung Datenschutz von denen der Stiftung Warentest.

Für die bewerteten Produkte betrifft der Datenschutz nur auf einen Teilaspekt. Es kann nur entschieden werden, ob ein Produkt datenschutzrechtlich oder datenschutztechnisch besser ist als ein anderes. Die Gesamtbewertung des Produkts durch den Nutzer wird nicht nur diesen Aspekt mit einbeziehen. Angesichts der begrenzten Aufgabenstellung der Stiftung Datenschutz muss diese Situation aber hingenommen werden.

Insgesamt kann man daher sagen, dass eine **vergleichende** Bewertung sinnvoll erscheint, insbesondere dort, wo mehr als ein Anbieter auf dem Markt tätig ist.

Die hohe Sachkompetenz der Stiftung Datenschutz und auch die Erarbeitung von Bewertungskriterien, auf die noch zurückzukommen sein wird (3.), sprechen dafür, dass die Stiftung über die Vergleichsbewertung hinaus ggf. auch ein Gütesiegel (dazu 4.) verleihen oder gar Datenschutzaudits durchführen sollte.

Dagegen spricht aber, dass diese Dienstleistungen sinnvollerweise nur gegen Entgelt durchgeführt werden können, der vom jeweils Begünstigten bezahlt wird.

Die Stiftung soll aber unabhängig von solchen Einnahmen sein, um ihre Unabhängigkeit auch gegenüber den Herstellern der von ihr untersuchten Produkte und der Anbieter der von ihr untersuchten Dienstleistungen zu gewährleisten. Nur eine solche Unabhängigkeit kann gewährleisten, dass die Untersuchung der Stiftung auch in der Öffentlichkeit akzeptiert werden (vgl. 1.3.).

Von daher **verbietet** sich die Vergabe von Bescheinigungen und Siegeln, soweit diese die Unabhängigkeit der Stiftung Datenschutz in den Augen der Öffentlichkeit gefährden. Dies hindert nicht die unabhängige, von der Stiftung selbst finanzierte Einzelbewertung etwa von Monopolangeboten wie Windows.

Zu Gütesiegeln ist unter 4. Genauerer ausgeführt.

Diese Gefährdung der Unabhängigkeit der Stiftung **verbietet** aber auch die Durchführung von Datenschutzaudits.

Anders ist dies allerdings mit der Zertifizierung von Personen, die ihrerseits Gütesiegel vergeben oder Datenschutzaudits durchführen.

Diese Personen sind ja nicht selbst Produkthanbieter oder Dienstleistungserbringer, so dass eine solche Zertifizierung angesichts der hohen Sachkompetenz der Stiftung Datenschutz sinnvoll erscheint, auch wenn dafür Entgelte erhoben werden, die die zu Zertifizierenden zahlen.

Weiterhin soll die Stiftung Datenschutz Prüfkriterien entwickeln, nach denen solche Gütesiegel verliehen und Datenschutzaudits durchgeführt werden sollen. Schon dies spricht dafür, dass die Stiftung im Hinblick auf diese Kriterien Schulungsmaterial anbietet und Personen prüft und zertifiziert, die ihrerseits aufgrund der Basis der Bewertungskriterien der Stiftung Produkte und Dienstleistungen datenschutzmäßig bewerten.

Es kann daher empfohlen werden, eine Zertifizierung von entsprechenden Prüfern in den Aufgabenkatalog der Stiftung aufzunehmen.

2.3. Nach welchen Kriterien soll geprüft, bewertet und zertifiziert werden?

Die Stiftung Datenschutz braucht für alle ihre Untersuchungen Kriterien.

Als Bewertungskriterium bietet sich zunächst die Einhaltung der gesetzlichen Vorschriften an.

Diese sind klar definiert, müssen nicht eigens erarbeitet und von den Anbietern ohnehin eingehalten werden.

Daraus ergibt sich allerdings nur, dass zu den untersuchten Kriterien jedenfalls auch die Einhaltung der gesetzlichen Vorschriften gehört. Anbieter, die die gesetzlichen

Vorschriften nicht einhalten, können nur eine Bewertung „mangelhaft“ erhalten. Ihnen wird weder ein Gütesiegel verliehen werden dürfen noch können sie erfolgreich ein Datenschutzaudit durchlaufen.

Auch eine Datenverarbeitung, die die gesetzlichen Vorschriften einhält, kann aber Gefährdungen auslösen, die man durch Lösungen auf einem Datenschutzniveau oberhalb der gesetzlichen Vorschriften verhindern kann. Dies gilt z.B. für die Art und Weise, in der bestimmte Leistungen angeboten werden, oder bei den Einstellungen, die von Dienstleistern gewählt werden, wenn der Kunde keine konkreten Wünsche äußert.

Darüber hinaus stellt sich bei den zu untersuchenden ausländischen Anbietern auch die Frage, welche Datenschutzvorschriften sie einhalten müssen. Rechtlich verpflichtet sind diese Anbieter nur auf das Recht ihres Heimatlandes. Die Anforderungen dieses Rechts können höher oder niedriger sein als die des deutschen Rechts, sie können auch ganz anders sein und in dieser anderen Weise den hinter dem Datenschutz liegenden Persönlichkeitsschutz gewährleisten.

Hier wird einer der ersten Aufgaben der Stiftung sein, gerade in solchen Fällen selbstständig zu erarbeiten, welche Kriterien des deutschen Rechts z.B. zwingend auch für ausländische Anbieter bei der Bewertung durch die Stiftung Datenschutz zu übernehmen sind und welche ausländischen Kriterien möglicherweise auch in Deutschland eine Rolle spielen können.

Hier ist zu empfehlen, dass die Stiftung Datenschutz über den gesetzlichen Anforderungen hinaus weitere Kriterien entwickelt, die zu einer Höherbewertung der jeweiligen Dienstleistung führen. Es kann hier auch – insbesondere bei der Vergleichsbewertung mit Notenvergabe auch verschiedenen Niveaus des Datenschutzes geben, die zu einer jeweiligen Höherbewertung oder Niederbewertung oberhalb der Note „mangelhaft“ führen können.

Zu der Erarbeitung der Kriterien verhält sich insbesondere der Teil 3 dieser Stellungnahme. Darauf soll verwiesen werden. Es empfiehlt sich dringend, die Kriterien nach wissenschaftlichen Methoden auch aufgrund von internationalen Vergleichen zu erarbeiten und sie dann mit verschiedenen Schutzniveaus den Bewertungen zugrunde zu legen.

2.4. Mit welcher Prüftiefe soll geprüft werden?

Insbesondere bei Dienstleistungen gibt es zunächst ein Datenschutz- und Datensicherungskonzept, das der Anbieter erarbeitet und auf deren Basis er die Dienstleistung anbietet. Im Internet sind solche Datenschutzerklärungen und vergleichbare Darstellungen mittlerweile gängig.

Die Stiftung Datenschutz kann zunächst solche Konzepte untersuchen und vergleichsweise bewerten.

Dass dies eine der notwendigen Voraussetzungen einer solchen Prüfung durch die Stiftung Datenschutz ist, ist nicht zu bezweifeln.

Eine Bewertung einer Dienstleistung nur auf der Basis dieses Konzepts reicht allein aber nicht, besagt doch dieses Konzept noch nicht, dass der Hersteller sich tatsächlich an es hält und die dort ergriffenen Datenschutz- und Datensicherungsmaßnahmen konsequent ergreift und auch über die Dauer durchhält.

Es muss daher empfohlen werden, zwar solche Bewertungen, soweit möglich aber auch weitergehende Untersuchungen durchzuführen.

Das praktische Problem bei der vergleichenden Untersuchung der Produkte und Dienstleistungen besteht darin, dass zwar Produkte wie PCs oder Software von der Stiftung erworben und dann auf geprüft werden können, dass dies aber für die Dienstleistungen nicht gilt.

Die Dienstleistungen werden auf eigenen Anlagen des Anbieters oder auf von ihm zeitweilig oder ganz gemietete Anlagen erbracht. Eine Zugänglichkeit dieser Anlagen von außen ist – auch aus Datenschutzgründen – ohne freiwillige Mitarbeit des Herstellers nicht möglich. Eine Untersuchung der technischen Realisierung ist daher ohne Zustimmung des Anbieters nur schwer möglich.

Darüber hinaus ist eine solche Untersuchung insbesondere dann, wenn die Anlagen im weit entfernten Ausland stehen, auch finanziell ausgesprochen aufwändig.

Zwar lassen sich bestimmte Sicherungsmaßnahmen auch dadurch prüfen, dass Hackerangriffe u. ä. simuliert werden. Diese Mittel können aber nur begrenzt eingesetzt werden. Alle Maßnahmen, die die Stiftung Datenschutz ergreift, müssen ihrerseits gesetzlich zulässig sein. Der Stiftung Datenschutz können keine Befugnisse verliehen werden, die über das hinausgehen, was jeder andere Bürger auch darf. Ein Eindringen in eine IT-Anlage von außen ohne Zustimmung des Anbieters ist unzulässig, weil es sich um eine Straftat zumindest nach § 202c StGB handelt. Mit anderen Worten: Der Stiftung Datenschutz darf eine Online-Durchsuchung der Rechner irgendwelcher Diensteanbieter im Internet nicht gestattet sein.

Es wird ohne Einverständnis des Anbieters nur zu prüfen sein, ob das untersuchte Produkt schon von außen erkennbar Schwachstellen aufweist oder ob es z.B. im Internet Berichte über solche Schwachstellen gibt.

Eine vertiefte Prüfung des Herstellers ohne freiwillige Mitwirkung ist unmöglich.

Es muss daher – wenn man eine vertiefte Prüfung will – eine freiwillige Mitarbeit der Hersteller erreicht werden. Dafür muss der Stiftung Datenschutz gestattet sein, auf die mangelnde Mitarbeit der Anbieter hinzuweisen und dies in ihre Bewertungskriterien (auch als Negativmerkmal) aufzunehmen.

Die Stiftung Datenschutz muss außerdem Kriterien erarbeiten, wie tiefgehend solche Prüfungen im Einzelfall durchgeführt werden sollen. Hier müssen die finanziellen Ressourcen in einer Relation zu den für die Nutzer gebrauchten Ergebnissen gesetzt werden. Darüber hinaus muss sichergestellt sein, dass auch die Prüfungen datenschutzrechtlich zulässig sind. Der Stiftung Datenschutz stehen die besonderen Befugnisse der Datenschutzkontrollinstanzen für ihre Untersuchungen nicht zur Verfügung. Daher dürfte sich der Zugriff auf einzelne personenbezogene Daten im Rahmen dieser Untersuchungen verbieten. Zu den Aufgaben der Stiftung Datenschutz wird es gehören, zu untersuchen, wie eine erfolgreiche Prüfung trotz dieser Einschränkung möglich ist. Aus dem Ergebnis solcher Forschungen lassen sich auch Erkenntnisse für Datenschutzprüfungen anderer Institutionen ableiten.

3. Mögliche Hauptleistung und zugleich Erarbeitung der Prüfkriterien der in Aussicht genommenen Stiftung:

- Instrumentarium des Datenschutzes im internationalen Rahmen;
- Prüfung der Wirkung für Betroffene und für verarbeitende Stellen;
- Impulse seitens der Stiftung zu Harmonisierung und Fortentwicklung

3.1. Mit welchen Kriterien soll/kann geprüft werden?

Es gilt, einen Katalog von abstrahierten Instrumenten des Datenschutzes zu schaffen, angefangen von Begriff und Schutzgut bis zur Frage der Sanktionen. Diese werden von verschiedenen Datenschutzgesetzen unterschiedlich benutzt und ausgestaltet. Das jeweilige Ensemble der in Anspruch genommenen Instrumente ist z. B. in Deutschland nicht deckungsgleich mit der EU-Datenschutz-Richtlinie¹¹ und divergiert von Seiten der EU-Richtlinie gegenüber USA stark. Das gilt sogar hinsichtlich grundlegender Prinzipien. Die – unbedingt erforderlichen – Standards und Schnittstellen¹² sind nur schwer übernational vorstellbar, wobei genau dies zu leisten wäre.

Es gibt gewichtige Ansätze und Initiativen zu Reformen (auch in USA, s. Anhang) des Datenschutzrechts, insbes. BDSG¹³, aber auch EU¹⁴. Solche Reformen könnten die Voraussetzungen für die Entwicklung der Standards wesentlich verbessern.

3.2. Gegen vorstehenden Vorschlag spricht, dass Akkreditierungen u. Ä. nur national gelten.

Frage: soll deshalb der Wirkkreis entsprechend auf BDSG und entsprechende Regeln begrenzt werden? Dagegen spricht auch die Vielfalt der Anforderungen, denen international agierende Firmen ausgesetzt wären.

¹¹ Z.B. der Beauftragte für den Datenschutz, die Aufgliederung in öffentlich und nicht-öffentlich, auch bei den Aufsichtsbehörden, die listenmäßige Übermittlung, Anhang zu § 9, die IFG.

¹² Sogar das GG baut auf die Wirkung von Standards und Schnittstellen, Art. 91c GG. S. a. zum dazu gehörigen Planungsrat zu und zum Gesetz: Berlin, 04.11.2009-18:10 - Die **Bundesregierung** hat heute den vom **Bundesminister des Innern** vorgelegten Entwurf eines Gesetzes über die **Bund-Länder-Zusammenarbeit** im Bereich der **öffentlichen Informationstechnik** und die Errichtung des **IT-Planungsrates** beschlossen. (<http://www.portel.de/nc/nachricht/artikel/41027-kabinett-segnet-it-planungsrat-fuer-engere-bund-laender-zusammenarbeit-ab/>)

¹³ S. Ergebnisse der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2009 in Berlin: Neustart im Datenschutz jetzt – kein „Weiter so“!

¹⁴ S. „Madriider Erklärung“ v. 3.9.2009

Eine Bewertung von Datenschutzmaßnahmen bzw. -produkten muss sich allerdings einerseits in das Konzept des national gültigen Rechts einfügen (s. 2.), kann aber andererseits nicht die Datenschutzgesetze allein zum Maßstab machen. Z.. B. können persönlichkeitschützende Maßnahmen im Bereich der unverlangten Werbung greifen, die auch im UWG geregelt ist¹⁵.

„*Siegel*“, s. a. 4., und *Zertifikate* setzen **Standards** und standardisierte **Prüfkriterien** voraus. Diese können aus übergeordneten Kategorien wie „Sicherheit“ und „Transparenz“ abgeleitet werden. Techniken wie Benchmarking könnten in Zukunft auch auf Grund ihrer Verankerung im GG¹⁶ große Aufmerksamkeit und Akzeptanz finden.

Die Idee internationaler Standards scheint bereits akzeptiert:

Datenschützer weisen Weg hin zu internationalen Standards¹⁷

*„In Madrid fand diese Woche die **31. Internationale Datenschutzkonferenz**[1] statt. Mehr als 1000 Teilnehmer aus über 80 Ländern haben sich mit aktuellen Themen des Schutzes der Privatsphäre befasst. Im Mittelpunkt der Veranstaltung stand die Verbesserung der internationalen Zusammenarbeit. Dabei soll der gemeinsam mit Industrievertretern und Nicht-Regierungsorganisationen **erarbeiteten**[2] Resolution "**International Standards on the Protection of Personal Data and Privacy**"[3]" (PDF-Datei) besondere Bedeutung zukommen.“*

Hierzu erklärt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar¹⁸:

*„Im Zeitalter des Internet ist Datenschutz nicht allein durch nationale Gesetze oder regionale Übereinkommen zu gewährleisten. Deshalb sind die von der Konferenz beschlossenen **internationalen Standards** ein Meilenstein für einen zeitgemäßen Datenschutz. Es kommt jetzt darauf an, diese Standards im internationalen Recht zu verankern und mit Leben zu füllen.“*

¹⁵ Zum Prüfungsmaßstab BDSG bei formularmäßiger Einwilligung für Zusendung von Werbung s. BGH v. 11.11.2009 – VIII ZR 12/08 – HappyDigits, derzeit PM; zur Einwilligung im Rahmen UWG vor Novellierung BDSG s. BGH v. 16.7.2008 –VIII ZR 348/06 - payback

¹⁶ Resultat der Föderalismuskommission II, s. a. *Sichel*, DVBl 2009,1014 - 1021.

¹⁷ heise 08.11.2009 11:10

¹⁸ bfdi.bund.de:

Zugleich scheint auch die Notwendigkeit akzeptiert, **Sicherheit und Datenschutzkonformität** nicht (nur) nachträglich zu erprüren, sondern einzuplanen und konstruktiv bereits einzubauen:¹⁹

*Weitere wichtige **Konferenzthemen** waren: **Privacy by Design**, das heißt die frühzeitige Berücksichtigung von Datenschutzanforderungen bereits beim Entwurf informationstechnischer Systeme. Die Teilnehmerinnen und Teilnehmer waren sich darüber einig, dass bei elektronischen Diensten schon die **Voreinstellungen die Privatsphäre** der Nutzerinnen und Nutzer garantieren müssen.*

Ein Schwerpunktthema war auch der Datenschutz am Arbeitsplatz.

Deshalb die **Zusatzfrage**, die auch 3.3. und 3.4 betrifft:

Wie lassen sich Systeme und v. a. bereits deren Entwicklung proaktiv prüfen?

Dies erfordert, die Prozesse und Vorgehensmodelle wie auch Qualitätssicherung der Entwicklungsprojekte frühzeitig zu begleiten und zu bewerten, sodass neben Produkten auch Verfahren und Klassifizierungsschemata zu entwickeln sind – analog der Level bei **BSI** (Bundesamt für Sicherheit in der Informationstechnik).

Dazu ein Auszug von Leistungen im Angebot des BSI, die zum einen unmittelbar verwertet werden könnten (§ 9 BDSG und Anlage), zum anderen als Vorbild für analoge Datenschutz- Systematik dienen könnten²⁰:

Themen/Stichworte zu Leistungen des BSI

- IT-Grundschutz-Standards
- IT-Grundschutz-Kataloge mit Themen u. a..

- Modellierung, Bausteine, IT-Systeme, Netze, Anwendungen
 - Gefahrenpotentiale
 - Gefährdungskataloge
 - Maßnahmenkataloge
 - Rollendefinitionen

¹⁹ heise 08.11.2009 11:10

²⁰ www.BSI.de

- ...
- Risikoanalyse
- Schutzbedarfsfeststellung
- ...

Von daher erscheint noch mehr als die Stiftung Warentest die Funktion des BSI im Hinblick auf Kategorisierungen, Kriterien, Standards als Vorbild.

3.3. Kann man überhaupt ohne **Harmonisierung** übernational **prüfen**, bewerten und ranken?

Die Möglichkeit der Beurteilung von Verfahren und Produkten setzt wie auch die Zitate 3.2 ergeben, eine **Harmonisierung der Beurteilungskriterien** voraus. Zu dieser Leistung gehört auch eine Systematik bzw. ein Schema der Bedrohungsszenarien. Vom Wortlaut her umfasst das BDSG z.B. nur den Schutz vor Missbrauch der personenbezogenen Daten.

In Deutschland hat dies eine Fülle von daneben und darüber liegenden weiteren Schutzinstituten generiert bzw. die schon früher bestehenden weiter entwickeln lassen, so insbesondere allgemeines Persönlichkeitsrecht, Recht auf informationelle Selbstbestimmung, Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und natürlich Würde und Entfaltungsfreiheit, wobei letztere Aspekte sich z.B. stärker in der Menschenrechtskonvention widerspiegeln.

Konkreter noch gefragt: Wie lässt sich ein Ausgleich zwischen den Problemen der Staffelnung von Daten nach Kategorien ihrer Sensitivität zwecks Messung der Adäquanz des Schutzes einerseits und der Relativität des Schutzbedarfs schon je Einzelnem, erst recht im interkulturellen Vergleich herstellen?

„Global“ gültige Privacy-Kriterien wird es kaum geben können. Innerhalb der EU wäre das Ziel leichter erreichbar. Erforderlich ist aber auch die Kompatibilität zu USA und international. Die Stiftung könnte zu den Fragen der Vergleichbarkeit einen Beitrag leisten.

In 2.3 ist bereits dargelegt worden, dass ausländische Anbieter primär die Pflichten erfüllen müssen, die ihnen das Heimatland auferlegt. Dementsprechend sind die zu entwickelnden Kriterien abzustufen:

- in Deutschland gültige, sich aus den Gesetzen ergebende Anforderungen, die auch für ausländische Anbieter und Anwender in Deutschland und der EU gelten,
- Kriterien, die im Ausland mangels Konzernprivileg gelten

Durch Kriterien, die die Regelungen auch entfernter Rechtsordnungen vergleichbar machen, kann eine Beurteilung ermöglicht werden, ob

- insoweit evtl. Diskriminierungen drohen, die vermieden werden sollten,
- diese Ansätze nicht Vorzüge haben, die man in Deutschland bzw. der EU näher prüfen und ggf. übernehmen sollte/könnte.

3.4. Welche Rolle spielt das konkrete, durch ein Produkt oder Verfahren zu bannende Gefährdungspotenzial?

Auf einer konkreteren Stufe geht es um einzelne Techniken und deren Bedrohungsszenarien, etwa Videoüberwachung, RFID oder Data Mining und Profilbildung. S.a. oben 3.2. zu BSI- Kategorien und **Privacy by Design**.

Aber auch die Unternehmen haben gegen sich gerichtete Bedrohungsszenarien, insbesondere im Rahmen der Spionage bzw. des Geheimnisverrats bzw. generell Data Loss, wogegen sich die Unternehmen schützen wollen und müssen. Sowohl unter dem Aspekt der Lückenlosigkeit des Schutzes als auch unter wirtschaftlichen Gesichtspunkten erscheint es zwingend erforderlich, dass die Produkte und Maßnahmen, die als Realisierung des Datenschutzes technisch/organisatorisch vorgeschrieben bzw. empfohlen werden, zumindest nicht im Widerspruch zu den Sicherheitsinteressen der Firma stehen, am besten diesen Schutz/die Sicherheit im eigenen Interesse sogar noch effektuieren. Dabei wäre auch zu berücksichtigen, dass wiederum das Schutzgut eine Ausprägung erhalten muss, die technisch abbildbar ist (was derzeit mit dem Schutz personenbezogener Daten eigenartigerweise nicht möglich ist, wie zahlreiche Sonderregelungen belegen (etwa zu Scoring u.ä.)). Diese "Implementierung von Privacy" wäre international vermittelbar, wäre evtl. sogar messbar, wenn es entsprechende Standards gäbe, bis hin zu Penetrationstests und Benchmarking (s.a. 3.2), so dass die Stiftung auch für eine Art Höherentwicklung des Datenschutzes sorgen bzw. eintreten muss, die Prüfkriterien neutral und international anwendbar zu machen.

3.5. Empfiehlt sich eine Neutralisierung der Begrifflichkeit?

Schon hinsichtlich der Begrifflichkeit wäre deshalb grundsätzlich zu überlegen, ob "Datenschutz", der ohnehin in die Renovierung gehen soll, der geeignete Begriff bleibt. Es könnte sich also auch empfehlen, Neuerungen bereits mit anzudenken, die auch mit internationaler Kompatibilität des gesamten Systems zu tun haben. Dies könnte bewirken oder bedeuten, dass eher auf Begrifflichkeiten und Ziele wie Persönlichkeitsschutz, Persönlichkeitsrecht, informationelle Selbstbestimmung abzustellen wäre, kurz gesagt Privacy i. V. m. dem Persönlichkeitsrecht und nicht dem Schutz der Daten. Die neutrale Stiftung könnte „Datenschutz“ in einem größeren Zusammenhang („surveillance“ ./ . Freiheit) vorantreiben.²¹

3.6. Eine Beurteilung und insbesondere auch Verfahren könnte nicht an den Landesgrenzen stehen bleiben bzw. könnte sich nicht nur auf einen nationalen Einsatz beschränken. Es heißt zum einen, dass auch Produkte/Verfahren zu beachten sind, die etwa im Ausland im Einsatz sind und v. a. solche, die vom Ausland her etwa über internationale Firmen aus dem Ausland stammen, aber in Deutschland eingesetzt werden. Dies kann sich auf technisch-/organisatorische Maßnahmen ebenso erstrecken wie auf die Maßnahmen, die genau zum Datenschutzproblem führen, also etwa Produkte im Bereich bzw. mit der Ausstattung von RFID, Video, technischen Entwicklungen wie GRID und neuerdings Cloud bzw. Services wie etwa ASP i. V. m. Data Mining, Online-Banking u. Ä.

3.7. Welches Gewicht soll die **Betreuung der Unternehmen** haben, die die Produkte und Verfahren einsetzen? Sollen auch diese geprüft, evtl. nicht nur auditiert, sondern auch mit Preisen/Siegeln versehen werden?

Eine unabhängige Stiftung könnte etwa auch die Instrumentarien danach unterschiedlich einteilen, weil sie im Interesse des Unternehmens oder zumindest zugleich im Interesse des Unternehmens einzusetzen sind, nicht zuletzt im Hinblick auf Verfügbarkeit, Lückenlosigkeit, Kontrollierbarkeit u. ä. Das heißt, dass der Rahmen nicht allein durch den Datenschutz und dessen gesetzliche Regelung gesteckt ist, sondern die übrigen Maßgaben für die die Unternehmen, im weiteren Sinne also etwa Compliance mitberücksichtigen müsste. Dies gilt insbesondere für solche Unternehmen, deren EDV-Anwendungen die nationalen Regelungen verschiedener Länder zu berücksichtigen haben.

²¹ S. a. Anhang <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559597> zum Rating.

Allerdings sind Restriktionen zu beachten, dass die Stiftung ihre Unabhängigkeit unbedingt wahrt (s. 2.2) und ggf. nicht die Stiftung selbst die Prüfung gegen Entgelt des Geprüften und nicht die Vergabe von Bescheinigungen, s. dazu 4. vornimmt.

- 3.8.** Die **Pyramide des Instrumentariums** könnte sich v. a. auch dahingehend bewähren, dass durch die Abstraktion auch "gute" bzw. erfolgversprechende Produkte/Verfahren aus Bereichen, die nicht bereits konform ausgestaltet sind für die Erfüllung der Anforderungen der EU-Datenschutzrichtlinie bzw. nationalen Datenschutz regeln. Dabei wäre u. a. an Stärkung der Eigenverantwortlichkeit der Betroffenen i. V. m. einer technischen Absicherung zu denken, so etwa Services, die zentral Löschungsfristen beachten.

"Pyramide des Instrumentariums", Vorschlag für ein Raster der Vergleichbarkeitskriterien, hier nur eine Mini-Version zur Veranschaulichung (etwas stärker ausgearbeitet zu BDSG und EU s. sogleich):

	Ausprägung/Maximalkatalog	D/EU	USA (nur einige Beispiele)
Grundprinzip (Verbot)	Verbote, Zweckbindung,		
Spezialregelung oder Allgemein-Gültigkeit		X	FCRA, FoIA Sektoral: Fair Credit Reporting)
Subsidiarität		X	
Anwendungsbereich (un)abhängig von der Technik	RFID, Video, Scoring, Ausweise, Rasterfahndung, automatische Kennzeichen-, body mass, - und/oder Kennzeichenerfassung, body-scan, Profilbildung		
Materielles Schutzgut	Privatsphäre, Schutz vor Beobachtungsfreiheit, Selbststeuerung „e-Privacy“? ²²		„privacy“
Rechte des Betroffenen	Auskunft, Berichtigung, Sperrung, Löschung (Automatik)		v.a. FoIA
Pflichten der Datenverarbeiter	Zweckgebundene Verarbeitung, Verwertungsverbote,		
Einwilligung, Voraussetzungen der Online-Einwilligung			
Haftung, Gefährdungshaftung	Unzulässige DV Unrichtige DV Ersatz auch imm. Schadens, Gewinnabschöpfung u.ä.		
Technisch-/organisatorische Pflichten/Maßnahmen	Funktionale Sicherheitsvorgaben Standards		
Überwachungs-Möglichkeiten/Institutionen, Kompetenzen			
Skandalisierungspflicht/Öffentlichkeit			
Versicherbarkeit			
Sanktionen ²³	StrR, s. a. Haftung		

²² S.a. Press release EDPS Hustinx, **Brussels, Monday 9 November 2009**: The revised ePrivacy Directive

²³ S.a. Beckblog v. 11.11.2009: Die Regierung von Großbritannien hat ein neue Gesetzesinitiative gestartet, wonach bei "ernsten Verletzungen" des U.K. Data Protection Act u.a. eine erhebliche Geldstrafe von bis zu £500,000 - etwa € 530.000 verhängt werden kann. Die Datenschutzbehörde, das Information Commission Office (ICO), wird in diesem Fall, ähnlich wie in Frankreich, über der Verhängung der Strafen entscheiden. Beim ICO läuft in dieser Angelegenheit zur Zeit ein Konsultationsverfahren bis zum 21.12.09. Frage an alle: Sind die Strafen nach dem deutschen Datenschutzgesetzen zu niedrig?

Im Bereich des nationalen Rechts könnte die Stiftung zu einer Vereinheitlichung und damit Harmonisierung beitragen, die wiederum die Argumentierbarkeit des "Datenschutzes" nach außen erleichtern würde, indem etwa die Regeln aus den Bereichen BDSG (mit Landesdatenschutzgesetzen), Spezialnormen und v. a. auch i. V. m. TMG, TKG und evtl. sogar UWG als ein Komplex gesehen werden.

Die folgende, etwas erweiterte Übersicht bezieht die EU-DSchRL ein, könnte ausgebaut werden, auch um Defizite zu zeigen.²⁴

INSTRUMENT	BDSG	EU-RL	X
- Zweck und Anwendungsbereich	§§ 1, 12 und 27	Art. 1 I Gegenstand Art. 3 Anwendungsbereich	
- Adressaten, öffentliche und nicht-öffentliche Stellen	§§ 2, 12 und 27	Anw.-Ausn: Art. 3 II, u.a. „ausschließlich im Rahmen persönlicher oder familiärer Tätigkeiten“	
Schutzgut (es fehlen Recht auf informationelle Selbstbestimmung, Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ²⁵)	§ 1 Wortlaut: Daten, Ziel aber Schutz vor Beeinträchtigungen des Persönlichkeitsrechts bei Verarbeitung personenbezogener Daten)	Art. 1 I Schutz der Grundrechte und Grundfreiheiten, insbes. Schutz der Privatsphäre	? Neutral/Standard: „Privacy“/e-Privacy?
- Begriffsbestimmungen	§ 3	Art. 2	
- Prinzipien wie - Verbotprinzip - Datenvermeidung und Datensparsamkeit	§ 3 a	Art. 7 Verbotprinzip Art. 6 Qualitätsgrundsätze;	
- Einwilligung und Einwilligungsformen	§ 4 a (und TDSG) freie Entscheidung, Hinweispfl., Schriftform	Art 7 a) „ohne jeden Zweifel i.V.m. Art. 2 h) ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage	
- Datengeheimnis	§ 5		
- Rechte des Betroffenen	§ 6 – Auskunft (Einsicht) ²⁶ - Berichtigung - Löschung - Sperrung Widerspruch, z.B. § 28 Abs. 4	Art. 12 Auskunft, Berichtigung, Löschung oder Sperrung Art. 14 Widerspruch	

²⁴ Mit Ergänzungen aus: *Conrad/Schneider*, "Datenschutz", in: *Schwarz/Peschel-Mehner*, Recht im Internet, LBl., Kap. 15.

²⁵ Und weitere, vom BVerfG (hier 27.2.2009) entwickelte Ausprägungen, die auch den privaten Sektor tangieren.

²⁶ S. neuerdings google dashboard

INSTRUMENT	BDSG	EU-RL	X
- Pflichten der datenverarbeitenden Stelle, Haftung Löschung/Sperrung	Meldepflicht §§ 4 d, e Verbot der automatischen Einzelentscheidung § 6 a	Art. 10 f. Infopflichten Art. 18 Meldepflicht	
Informations-/ Skandalisierungs- pflicht	Neu § 42a bei unrechtmäßiger Kenntniserlangung		EU-Parlament
- Kontrolle, Institutionen, Aufgaben und Befugnisse	§§ 4 f, g, § 22 ff, Datenschutz Audit: § 9 a	Art. 28 Kontrollstell(n), völlige Unabhängigkeit Art. 29 f. Datenschutz- gruppe	
- besondere Rechte des Betroffenen, insbesondere Schadenersatz	§§ 7 und 8	Art. 23 Haftung	
SchE für Immaterielle Schäden			
Verschuldens(un)ab hängigkeit			
- technische und organisatorische Maßnahmen	§ 9 und Anlage	Art. 16 Vertraulichkeit Art. 17 Sicherheit	
- Abrufverfahren	§ 10		
- Auftrags - DV	§ 11, Anforderungen an Auswahl, Vertragsgestaltung	Art. 17. Abs. 3	
- Strafbarkeit/Bußgeld	§§ 43, 44	Art. 24 Sanktion	
- Zulässigkeitstatbest ände	§ 4, §§ 13 ff. öffentlich, §§ 28 ff. nicht-öffentlich	Art 7, u.a. Erforderlichkeit (b)), Art 8 besondere Arten	
- besondere technische Ausprägungen	- Video in öffentlichen Räumen § 6b - Mobile Speicher- und Verarbeitungs- medien § 6c, Scoring § 28b Screening MA § 32 Abs. 1 S. 2		Bodyscanner

3.9. Entwicklungszyklen und Trends

Eine Entwicklung im „Datenschutz“ geht hin zu mehr Selbststeuerung und Eigenverantwortung. Dazu muss der Einzelne unterstützt werden und Werkzeuge an die Hand (in den PC/ins mobile device) bekommen, die ihm die Gefährdungspotenziale transparent machen und die Handhabung der Maßnahmen erleichtern.

Die Frage ist: Kann die geplante Stiftung die Entwicklung solcher Techniken mit implementiertem Schutz besser durch Kontrolle oder durch Anreize/Förderung erreichen?

Angesichts der Produktentwicklungskosten und -zyklen, also auch der Innovationsgeschwindigkeit, erscheint nur der Weg über Anreize/Förderung gangbar.

4. Verleihung eines Gütesiegels im Zusammenhang mit der Stiftung Datenschutz²⁷

4.1. Welche Gütesiegel gibt es bereits, wofür werden sie eingesetzt und welche Kriterien werden überprüft (national, international)?

Im Folgenden werden zwei prominentere Datenschutzsiegel herausgegriffen, um Anwendungsbereiche und Wirkungsweisen beispielhaft darzustellen. Des Weiteren wird kurz auf den (bislang nicht umgesetzten) Entwurf eines Datenschutzauditgesetzes eingegangen.

4.1.1. Datenschutz-Gütesiegel des ULD



Das Datenschutz-Gütesiegel des Unabhängigen Landeszentrum für den Datenschutz Schleswig-Holstein („ULD“) kommt für Hardware, Software und automatisierte Verfahren in Betracht, die zum Einsatz bei öffentlichen Stellen geeignet sind. Es beruht auf dem Verleihungsprinzip: Der betreffende Hersteller bzw. das Vertriebsunternehmen lässt sein Produkt von einem zertifizierten Sachverständigen auf der Basis eines privatrechtlichen Vertrages schriftlich begutachten. Anschließend erfolgt der Antrag auf Erteilung des Gütesiegels beim ULD. Nach einer Plausibilitätsprüfung durch das ULD und ggf. weiteren Nachforschungen wird das Gütesiegel bei Vorliegen der Voraussetzungen erteilt.²⁸ Aus dem „Prüfschema des Gutachtens für die Produktzertifizierung“²⁹ geht hervor, dass die datenschutzrelevanten Eigenschaften eines Produktes den Anforderungen in adäquater Weise entsprechen, wenn die verwendeten technischen Lösungen die Umsetzung der gesetzlichen Vorgaben ermöglichen.

²⁷ Von Dr. Peter Bräutigam, in Zusammenarbeit mit Dr. Sabine Grapentin, LL.M., Rechtsanwälte und Fachanwälte für Informationstechnologierecht.

²⁸ Vgl. im Einzelnen die Broschüre „Welche Vorteile bringen mir Datenschutz-Behördenaudit & Datenschutz-Gütesiegel?“ des ULD (o.D.), S. 12, abrufbar unter <https://www.datenschutzzentrum.de/guetesiegel/allgemein.htm>

²⁹ Version 1.1, Stand 01.11.2005, S. 8, abrufbar unter https://www.datenschutzzentrum.de/guetesiegel/infos_gutachter.htm

4.1.2. European Privacy Seal



Hierbei handelt es sich um ein von der EU gefördertes Projekt. Auch dieses System basiert auf der Prüfung durch zertifizierte Sachverständige, deren Gutachten von einer Akkreditierungsstelle überprüft wird. Akkreditierungsstellen sind das ULD und die Datenschutzbehörde von Madrid. Das Europäische Datenschutz-Gütesiegel bescheinigt, dass ein IT-Produkt oder eine IT-basierte Dienstleistung eine Nutzung dieses Produkts oder dieser Dienstleistung erleichtert, die mit den Vorschriften des EU-Datenschutzrechts vereinbar ist (nicht jedoch notwendig mit denen eines nationalen Datenschutzrechts).³⁰

4.1.3. Konzeption des Entwurfs des Datenschutzauditgesetzes

Nach einem letztendlich nicht umgesetzten Gesetzesentwurf der Bundesregierung (nachfolgend auch „**DSAG-E**“)³¹ war das sog. „Datenschutzauditsiegel“ ausgerichtet auf private Anbieter von Datenverarbeitungsanlagen und -programmen, verantwortliche Stellen und öffentliche Anbieter, die am Wettbewerb teilnehmen. Als Prüfungsgegenstand waren Datenschutzkonzepte und informationstechnische Einrichtungen vorgesehen. Prüfungsmaßstab sollten u. a. die Gesetzeskonformität der Datenverarbeitung sowie die Einhaltung der Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit des „Datenschutzauditausschusses“ sein, eines 18-köpfigen Gremiums unter der Rechtsaufsicht des Bundesinnenministeriums. Als Kern des Kontrollsystems waren akkreditierte private Zertifizierungsstellen vorgesehen, die vom BfDI zugelassen und von Landesbehörden überwacht worden wären. Anders als bei den oben betrachteten bestehenden Gütesiegeln hätten Antragsteller das

³⁰ Definition der EuroPriSe-Projektpartner, vgl. Meissner, DuD 2005, 525, 526.

³¹ Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften, BT-Drs. 16/12011 v. 18.02.2009.

Datenschutzauditsiegel bereits ab der Bestellung einer Kontrollstelle und der erstmaligen Anzeige beim Bundesbeauftragten führen dürfen.³²

4.2. Worin unterscheiden sich Teststiftungen von Gütesiegeln?

Trotz des ähnlichen Anwendungsbereichs unterscheiden sich vergleichende Tests von Produkten oder Dienstleistungen nach dem Vorbild der Stiftung Warentest in entscheidenden Punkten von den bestehenden Datenschutz-Gütesiegeln. Vergleichende Tests weisen in der Regel die folgenden Eigenschaften auf:

- Nicht nur das Produkt eines Antragstellers, sondern mehrere Produkte/Dienstleistungen werden zu einem bestimmten Zeitpunkt parallel überprüft und anhand eines definierten Anforderungskatalogs verglichen.
- Die Initiative geht nicht von individuellen Antragstellern aus. Vielmehr entscheidet die Stiftung³³ über das Ob und Wie der Prüfung, d.h. insbesondere den Zeitpunkt, den Prüfungsgegenstand (z.B. bestimmte IT-Produkte, Internet-Dienste etc.) und die in die Überprüfung konkret einbezogenen Produkte/Dienstleistungen, die miteinander verglichen werden.
- Eine Stiftung kann daher auch Produkte und Dienstleistungen von Anbietern in die Prüfung einbeziehen, die dieses selbst nicht wünschen.
- Es besteht das Grundverständnis, dass das Testergebnis die Situation zu einem bestimmten Zeitpunkt widerspiegelt. Anders als bei Gütesiegeln ist es nicht erforderlich, nach Ablauf eines bestimmten Zeitraums eine Rezertifizierung vorzunehmen.

4.3. Welche Anforderungen/Kriterien könnten an die Verleihung eines Gütesiegels gestellt werden? Welche Maßstäbe sind hierbei anzulegen?

Sollte man erwägen – ungeachtet der bereits unter Ziffer 2.2 aufgeführten Bedenken –, der Stiftung eine Befugnis zur Verleihung eines Gütesiegels zu übertragen, so würde

³² Eine Berechtigung zur Führung des Siegels ab Anzeige mit anschließender Kontrolle durch akkreditierte Stellen wird nachfolgend „Anzeigemodell“ genannt, im Gegensatz zum „Verleihungsmodell“, bei dem die Siegelführung eine Prüfung durch akkreditierte Stellen voraussetzt.

³³ Der Begriff „Stiftung“ wird hier untechnisch i.S.v. der die vergleichenden Tests durchführenden Stelle verwendet.

sich zunächst die Frage nach den dafür maßgeblichen Anforderungen, Kriterien und Maßstäben stellen.

- Die oben betrachteten bestehenden Gütesiegel haben im Kern die Gesetzeskonformität zum Gegenstand. Eine darüber hinausgehende datenschutzfreundliche Gestaltung von Produkten und Dienstleistungen ist zwar angestrebt und kann im Prüfungsverfahren lobend erwähnt werden (z.B. durch die Einstufung als „den Anforderungen in vorbildlicher Weise entsprechend“)³⁴. Ein Gütesiegel mit Abstufungen gibt es bislang – soweit ersichtlich – jedoch nicht.
- Die Regelungen des Entwurfs des Datenschutzauditgesetzes, die in Form der „Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit“ einen höheren Maßstab zu schaffen beabsichtigten, waren unzureichend. Dieser Maßstab hatte – jedenfalls im Entwurfsstadium – keine zureichende Konkretisierung erfahren³⁵ und die Besetzung des mit der Erstellung der Richtlinien zu betrauenden Ausschusses war zudem höchst umstritten.
- Im Ergebnis dürfte daher die Einrichtung eines Gütesiegels, das den Anspruch erhebt, Aussagen zu treffen, die über eine reine Gesetzeskonformität hinausgehen, erhebliche praktische Schwierigkeiten aufwerfen, da diesbezüglich noch keine hinreichenden Erfahrungswerte bestehen.
- Eine Teststiftung hingegen ermöglicht eine differenzierte Beurteilung nach einem abgestuften Notensystem. Es genügt hier, dass man die Bewertungsfelder vorab festlegt. Den Grad der Erfüllung hingegen kann man der Praxis überlassen, er wird im Rahmen des Vergleiches lediglich bewertet. Bei einem solchen Produkt- und Dienstleistungsvergleich ist die Gesetzeskonformität zwar ein (wichtiges) zu prüfendes Kriterium, darüber hinaus können aber auch zusätzliche produktspezifische Eigenschaften verglichen und im Rahmen des Testberichtes hervorgehoben werden.
- Im Rahmen eines vergleichenden Testsystems werden in der jeweiligen Branche (bzw. für das jeweilige Produkt/die jeweilige Dienstleistung) vorhandene Lösungen verglichen und einander gegenüber gestellt. Aufgrund der hierdurch entstehenden

³⁴ Vgl. das „Prüfschema des Gutachtens für die Produktzertifizierung“, a.a.O. Fn. 28, S. 8.

³⁵ Zu § 11 DSAG-E s. auch die Stellungnahme Nr. 29/2009 des Deutschen Anwaltsvereins zum DSAG (i.d.F. v. 02.01.2009, BR-Drs. 4/09), Ziff. 7.

Erfahrungswerte kann die Entwicklung genereller Maßstäbe für datenschutzrechtliche Bewertungen ermöglicht oder zumindest gefördert werden, die über die reine Gesetzeskonformität hinausgehen und jedenfalls im Entwurfsstadium des Datenschutzauditgesetzes noch fehlten.

- Im Ergebnis sind der Ansatz und die Zielrichtung unterschiedlich und sollten nicht vermischt bzw. von derselben Stelle angeboten werden: Ein Gütesiegel misst individuelle Produkte anhand eines (mehr oder weniger) abstrakten Anforderungskataloges, während Testvergleiche von vorgefundenen Produkten und Dienstleistungen ausgehen. Die ergebnisoffene Ermittlung von Best Practices ermöglicht darüber hinaus auch die Entwicklung praxisnaher Bewertungsmaßstäbe.

4.4. Wie müsste ein Prozess zur Verleihung eines Gütesiegels aussehen? (Verleihungsmodell vs. Anzeigemodell³⁶)

Die bestehenden Gütesiegel folgen dem Verleihungsmodell und entsprechen damit auch den Erwartungen, die die Verkehrsteilnehmer mit entsprechenden Gütesiegeln verbinden. Das Anzeigemodell des Datenschutzauditgesetzes – wiewohl in der Entwurfsbegründung gerechtfertigt mit Erfahrungen aus dem ökologischen Landbau³⁷ – war vielfach kritisiert worden und dürfte die Gefahr eines Missbrauchs mit sich bringen, insbesondere wenn der bis zur Erstkontrolle maximal zu verstreichende Zeitraum nicht bestimmt wird.³⁸

4.5. Wer könnte überhaupt ein Gütesiegel vergeben und wie erfolgt die Finanzierung?

Von entscheidender Bedeutung sind außerdem die das Gütesiegel verleihende akkreditierte Stelle sowie die Finanzierung eines Gütesiegel-Systems.

- Die Qualität der verleihenden akkreditierten Stellen bzw. – im Falle eines Anzeigemodells – der akkreditierten Kontrollstellen bildet den Kern eines jeden Gütesiegel-systems. Die Überprüfung der akkreditierten Stellen und die

³⁶ Zur Terminologie s.o. Fn. 31

³⁷ Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften, BT-Drs. 16/12011 v. 18.02.2009, S. 11.

³⁸ Vgl. hierzu auch die Stellungnahme des Bundesrates vom 13.02.2009 zum Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften, a.a.O. Fn.36, Anlage 3, S. 42.

diesbezügliche Qualitätssicherung ist eine der wesentlichen Herausforderungen, auch im Hinblick auf die hierfür erforderlichen Ressourcen.³⁹

- Gütesiegel können – soweit sie keine anderweitige Finanzierung etwa durch staatliche Förderung erfahren – durch die Antragsteller (mit-) finanziert werden, die für die Begutachtung durch die akkreditierten Sachverständigen und die Begutachtung durch die Akkreditierungsstelle Gebühren zahlen.⁴⁰
- Inwieweit Stiftungen über die Verwertung und Publikation ihrer Ergebnisse hinaus Einkünfte erzielen können, wäre noch weitergehend zu prüfen.⁴¹ Jedenfalls kann ein Testsystem wohl freier agieren und Ressourcen je nach Verfügbarkeit effizienter allozieren, da es Art, Zeitpunkt und Umfang der durchzuführenden Prüfungen im Wesentlichen selbst bestimmt und diesbezüglich nicht von Art und Anzahl eingehender Verleihungsanträge abhängt.

4.6. Was wären vor diesem Hintergrund die Vor- und Nachteile eines Datenschutz-Gütesiegels als integraler Bestandteil der Stiftung Datenschutz?

Nach den obigen Erläuterungen ergeben sich die folgenden Vor- und Nachteile:

4.6.1. Vorteile

- Das datenschutzrechtliche Know-how der Stiftung Datenschutz bzw. der für diese tätigen Gutachter könnte im Rahmen von zwei „Modellen“, d.h. doppelt verwertet werden.
- Das Vertrauen, das die Stiftung Datenschutz genießen wird, könnte auch auf den Bereich der Zertifizierung (Gütesiegel) übertragen werden.
- Die Stiftung Datenschutz könnte sich durch ein Gütesiegel weitere Finanzierungsmöglichkeiten erschließen.

³⁹ Die Beanspruchung der Landesaufsichtsbehörden für den Datenschutz mit entsprechenden Kontrollaufgaben war daher einer der zentralen Kritikpunkte des Bundesrates am DSAG-E, vgl. Stellungnahme des Bundesrates v. 13.02.2009, a.a.O. Fn. 37, Anlage 3, S.40.

⁴⁰ Vgl. z.B. die ULD-Benutzungs- und Entgeltsatzung, abrufbar unter www.datenschutzzentrum.de/material/recht/gebuehrensatzung.htm.

⁴¹ Hierzu s. auch oben 1.3 und 2.2 sowie unten 5.2 und 5.3.

- Ein Gütesiegel mit professionellem, unterscheidungskräftigem Logo fördert den Markenauftritt der zertifizierenden Stelle.

4.6.2. Nachteile

- Beide Modelle (Gütesiegel vs. Testvergleich) harmonisieren allerdings in wesentlichen Aspekten nicht. Insbesondere steht die Unabhängigkeit der Bewertung von Tests in Frage, wenn die bewertende Stelle einem der Kandidaten in Bezug auf die zu prüfenden Produkte bereits ein Gütesiegel verliehen hat.
- Gütesiegel im Datenschutz stehen generell vor dem Problem der Entwicklung überzeugender Bewertungsmaßstäben, die über die Gesetzeskonformität hinausgehen. Testverfahren haben den deutlichen Vorteil, dass sie Bewertungsmaßstäbe im konkreten Produktvergleich entwickeln können.
- Die Bezahlung von Gebühren für ein Gütesiegel durch Wirtschaftsunternehmen könnte das Vertrauen in die Objektivität der Tests beeinträchtigen, insbesondere im Hinblick auf marktstarke „Großkunden“, die über die Mittel verfügen, zahlreiche Produkte mit einem Gütesiegel zertifizieren zu lassen.
- Diese mögliche Beeinträchtigung des Vertrauens in die Unabhängigkeit der Testergebnisse erscheint uns das maßgebliche Argument, das im Ergebnis ein paralleles Anbieten beider Modelle nicht als empfehlenswert erscheinen lässt.

4.7. Welche Alternativen gäbe es zu einem Gütesiegel?

Ein reines Testsystem ist unseres Erachtens die ausschließliche Alternative. Zum einen sollte das Vertrauen in die Unabhängigkeit der Stiftung Datenschutz nicht durch ein Gütesiegelsystem aufs Spiel gesetzt oder gefährdet werden. Zum anderen erscheint es gerade in der Etablierungsphase sinnvoll, ein eindeutig umrissenes Modell anzubieten und dieses im Markt klar kommunizieren zu können. Die Erweiterung um ein Gütesiegel würde hier zu Verwässerungseffekten führen.

5. Zur rechtlichen Auskleidung der Stiftung Datenschutz

5.1. Struktur der Stiftung

Zunächst stellt sich das Erfordernis einer Grundentscheidung zwischen einer öffentlich-rechtlichen und einer privatrechtlichen Organisationsform. Im ersteren Falle, insbesondere zur Errichtung einer Stiftung öffentlichen Rechts, bedürfte es eines Errichtungsgesetzes und damit der Durchführung eines förmlichen Gesetzgebungsverfahrens. Vorteilhaft könnte dabei sein, dass die Errichtung der Stiftung durch die Behandlung im Bundestag zusätzliche Aufmerksamkeit in der Öffentlichkeit erfährt. Nachteilig könnte sein, dass die Durchführung eines förmlichen Gesetzgebungsverfahrens mit einem nicht unerheblichen zusätzlichen Zeitaufwand verbunden ist und damit zu einer Verzögerung führen könnte. Allerdings ist zu bedenken, dass auch bei einer Entscheidung für eine privatrechtliche Organisationsform die haushaltsrechtlichen Voraussetzungen geschaffen werden müssen, um die Stiftung mit dem zur Erfüllung ihrer Aufgaben erforderlichen Stiftungskapital ausstatten zu können. Soweit es das Ziel der Einbeziehung privaten Sachverständes in den Beirat und/oder das Kuratorium der Stiftung betrifft, wäre dieses auch bei einer Entscheidung für eine öffentlich-rechtliche Organisationsform zu erreichen. Zu beachten ist, dass auch die Stiftung Warentest eine privatrechtliche Stiftung ist.

Erfolgt eine generelle Entscheidung für eine privatrechtliche Organisationsform, so ist weiter folgendes zu bedenken:

Neben der klassischen Stiftung nach §§ 80 ff. BGB ist auch an andere Rechtsformen zu denken. In jedem Fall sollte der Rechtsträger im steuerlichen Sinne gemeinnützig sein, d. h. im Sinne der §§ 51 ff. AO. Nur dann ist der Rechtsträger von allen wesentlichen Steuern befreit, d. h. er ist insbesondere mit den Erträgen aus den Vermögensverwaltung des eigenen Vermögens nicht steuerpflichtig, kann Zuwendungsbestätigungen (Spendenquittungen) erteilen und es besteht bei Zuwendung von Vermögen an die Stiftung keine Schenkung- oder Erbschaftsteuerpflicht.

Gemeinnützigkeit kann aber nicht nur eine Stiftung nach §§ 80 ff. BGB erlangen, sondern beispielsweise auch ein Verein oder eine Kapitalgesellschaft (GmbH oder AG). So sind zum Beispiel die "Konrad Adenauer Stiftung" oder die "Stiftung Jugend forscht" keine Stiftungen, sondern Vereine. Der Firmierungsteil "Stiftung" darf in diesem Zusammenhang nicht fehlleiten, auch beispielsweise die Robert Bosch Stiftungs GmbH ist gerade keine Stiftung, sondern eine (gemeinnützige) GmbH.

Der Vorteil, den gemeinnützigen Rechtsträger nicht als klassische Stiftung nach §§ 80 ff. BGB auszukleiden, sondern zum Beispiel als GmbH, liegt in der Flexibilität der Organisation: Eine klassische Stiftung nach §§ 80 ff. BGB unterliegt zwingend der staatlichen Rechtsaufsicht. Dies ist bei den anderen Rechtsträgern, insbesondere der Kapitalgesellschaft oder dem Verein, nicht der Fall. Deswegen kann die Satzung dieser Rechtsträger wesentlich leichter an geänderte Bedürfnisse angepasst werden, es besteht bei den Änderungen kein Mitspracherecht einer staatlichen Stiftungsaufsicht. Dies ist gerade zu Beginn der Tätigkeit eines gemeinnützigen Rechtsträgers oft wichtig, weil häufig erst nach einigen Wochen, Monaten oder Jahren der Tätigkeit der genau zu beschreibende Zweck der Stiftung feststeht. Wichtiger ist – für die Außenwirkung –, dass der Rechtsträger Gemeinnützigkeit nach §§ 51 ff. AO erlangt hat, denn nur dann kann er Spendenquittungen erstellen und Zuwendungen an den Rechtsträger sind von der Erbschaft- und Schenkungsteuer befreit. Zu empfehlen ist daher evtl. der Start über eine "Stiftung Datenschutz GmbH", die dann später in eine entsprechende zivilrechtliche Stiftung umgewandelt wird.

5.2. Unabhängigkeit der Stiftung von der Stifterin trotz ihrer eventuellen finanziellen Beteiligung

Die Organmitglieder der Stiftung sollten von der Stifterin unabhängig sein. Es ist also sicherzustellen, dass die Mitglieder aller Stiftungsgremien, insbesondere der Vorstand, nicht mit Personen besetzt wird, die der Stifterin unmittelbar (und ggf. auch mittelbar) nahe stehen. Dies kann durch eine entsprechende Bestimmung in der Stiftungssatzung verbindlich vorgegeben werden, d. h. es ist möglich (und in Stiftungssatzungen auch üblich), Regeln aufzustellen, wer Organ der Stiftung sein kann und wer nicht. Selbstverständlich kann sich die Stifterin (ggf. also die Bundesrepublik Deutschland) sog. Stifterrechte vorbehalten, z. B. ein Vetorecht gegen die Besetzung von Organstellen mit der Stifterin ungeeignet erscheinenden Personen.

5.3. Finanzierung der Stiftung

Die finanzielle Ausstattung der Stiftung Datenschutz sollte auf eine breite Basis gestellt werden, um nicht nur von einem Spender abhängig zu sein. Sofern die Bundesrepublik Deutschland auf Dauer für die Stiftung Datenschutz Leistungen erbringen will und kann, könnte dies in der Satzung verankert werden. So heißt es beispielsweise in der Satzung der Stiftung Wartentest (§ 4 Abs. 2):

"(2) Der Stiftung wird zur Erfüllung ihrer satzungsgemäßen Aufgaben von der Stifterin jährlich ein Festbetrag als Zuwendung nach Maßgabe der Haushaltspläne des Bundes zur Verfügung gestellt."

Wie bei gemeinnützigen Organisationen nicht unüblich könnte dafür geworben werden, Spenden und Zustiftungen unter Lebenden, aber auch von Todes wegen, zu erwerben. Es sollte ein Marketingkonzept erarbeitet werden, wie Privatpersonen für die Idee einer Stiftung Datenschutz zu gewinnen sind. Gegebenenfalls sollte darüber nachgedacht werden, in der Stiftungssatzung zu regeln, dass die Stiftung Zuwendungen Dritter nur annehmen darf, soweit dadurch die Unabhängigkeit ihrer Arbeit nicht gefährdet wird.

5.4. Organe der Stiftung

Eine Stiftung im Sinne der §§ 80 ff. BGB wird durch ihren Vorstand vertreten. Der Vorstand ist das einzige Organ, das rechtlich vorgeschrieben ist. Üblicherweise wird jedoch bei einer Stiftung noch ein Kontrollorgan installiert, das als Beirat, Aufsichtsrat, Stiftungsrat etc. bezeichnet wird. Nicht selten ist auch eine 3er-Struktur der Organe anzutreffen, in der einerseits neben dem Vorstand ein Beirat mit Kontrollfunktion installiert wird, und andererseits ein Kuratorium als wissenschaftliches Beratungsgremium. Für die Stiftung Datenschutz bietet es sich z. B. an, im Kuratorium in der Öffentlichkeit anerkannte Persönlichkeiten zu versammeln, um die Akzeptanz und das fachliche Profil der Stiftung Datenschutz zu stärken. Zudem könnte über das Kuratorium versucht werden, möglichst viele gesellschaftsrechtliche Gruppierungen einzubinden. Denkbar ist auch, die Stifterin zumindest über das Kuratorium einzubinden, falls sie nicht direkt im Vorstand oder im Beirat die Geschicke der Stiftung lenken soll, insoweit ist auf Ziff. 5.2 zu verweisen. Gegebenenfalls ist alternativ auch darüber nachzudenken, der Stifterin lediglich das Recht einzuräumen, zu den Sitzungen der Organe einen nicht stimmberechtigten Vertreter zu entsenden.

Die hier empfohlene Ausgestaltung mit einem zusätzlichen Aufsichtsorgan bzw. die Konstellation mit Aufsichts- und Beratungsorgan kann selbstverständlich auch bei Errichtung der Stiftung Datenschutz in der Rechtsform einer GmbH oder eines Vereins umgesetzt werden.

5.5. Internationale Ausrichtung der Stiftung Datenschutz

Unabhängig von der Form der rechtlichen Ausgestaltung der Stiftung (Stiftung, Verein, Kapitalgesellschaft) können ohne weiteres auch Personen aus dem Ausland in die Organe integriert werden.

5.6. Integration der "offiziellen Datenschützer"

Für die "offiziellen Datenschützer" gilt Gleiches wie für internationale Ausrichtung (5.5): Sie können in jedes der denkbaren Organe integriert werden. Anbieten würde sich insbesondere eine Mitwirkung im Kuratorium, das letztlich als wissenschaftliches Impulsgremium fungieren kann.

6. Schlussteil

6.1 Thesenartige Zusammenfassung der vorstehenden Ausführungen

1. Die Initiative zu einer „Stiftung Datenschutz“ – Arbeitstitel – wird im Prinzip sehr begrüßt.
2. Die Stiftung Warentest kann von ihrer Ausgestaltung her als Modell dienen, auch wenn wesentliche Unterschiede in Zielgruppen und Aufgaben bestehen.
3. Wichtige Aufgabe wäre die Entwicklung und Pflege von Beurteilungskriterien für Produkte, Verfahren und Anwendungen, die auch internationale Akzeptanz finden.
4. Unabhängigkeit und Neutralität der Stiftung sind oberste Ziele. Diese implizieren Restriktionen hinsichtlich Vergütung für Leistungen.
5. Es sollte die Weiterentwicklung des „Datenschutzes“ in der Praxis, aber auch de lege ferenda gefördert werden.
6. Tendenziell wird zumindest zur Startphase eine „Stiftungs-GmbH“ empfohlen, weil sie flexibler ist.
7. Ein Gütesiegel sollte zumindest nicht in der Anfangsphase verliehen werden. Stattdessen stehen die Test-Kriterien, die Tests und die Berichte darüber im Vordergrund.

6.2 Entscheidungsalternativen mit jeweiligen Vor- und Nachteilen

Entscheidungsgegenstand	Vor- und Nachteile		Tz.
Soll die Stiftung nur Waren und Dienstleistungen solcher Anbieter testen, die zur Mitwirkung an einem solchen Test bereit sind?	Dafür spricht, <ul style="list-style-type: none"> - dass die Stiftung Datenschutz über eine derartige Mitwirkung an nähere Informationen zu internen Datenverarbeitungsprozessen der jeweiligen Anbieter gelangen könnte, ohne die aussagekräftige Tests des Datenschutzniveaus der überprüften Dienstleistungen oftmals nur schwer möglich sind. 	Dagegen spricht, <ul style="list-style-type: none"> - dass bei einer solchen Vorgehensweise fraglich, wäre, ob man bei jeder Testreihe hinreichend viele Anbieter betreffender Produkte für eine Teilnahme gewinnen könnte, um einen aussagekräftigen Vergleich für eine bestimmte Produktparte zu erzielen; 	1.5.

Entscheidungsgegenstand	Vor- und Nachteile		Tz.
		<ul style="list-style-type: none"> - dass hierbei die Gefahr bestehen würde, dass gerade "schwarze Schafe" einer Branche oder ggf. sogar gesamte Branchen, die datenschutzrechtliche Belange insgesamt nicht sonderlich ernst nehmen, ihre Mitwirkung verweigern würden, was den gesamten Sinn einer Stiftung Datenschutz in Frage stellen würde. 	
<p>Soll die Stiftung ausschließlich Waren und Dienstleistungen im „B2C“ oder auch im „B2B“-Bereich testen?</p>	<p>Für Beschränkung auf „B2C“-Bereich spricht,</p> <ul style="list-style-type: none"> - dass – vergleichbar dem Modell der Stiftung Warentest – gerade Verbraucher besonders schutzbedürftig erscheinen, während Unternehmer sowohl durch eigene Tests der nachgefragten Produkte als auch durch ihre grundsätzlich stärkere Verhandlungsposition gegenüber den jeweiligen Anbietern weniger auf einen externen Sachwalter ihrer Interessen angewiesen sind; - dass in einem derartigen Fall eine stärkere Anlehnung der Stiftung Datenschutz an die praxisbewährte Struktur der Stiftung Warentest und mithin evtl. eine schnellere 	<p>Für Einbeziehung von „B2B“-Bereich spricht,</p> <ul style="list-style-type: none"> - dass gerade die Beachtung der Tests der Stiftung Datenschutz im nachfragestarken B2B-Bereich eine schnellere und effektivere Umsetzung der Ziele der Stiftung Datenschutz gewährleisten würde; - dass auch die Verbesserung des Datenschutzniveaus im B2B-Bereich mittelbar dem Endkunden und mithin dem B2C-Bereich zugute kommen würde. 	1.5.

Entscheidungsgegenstand	Vor- und Nachteile		Tz.
	Schaffung der Stiftung Datenschutz – ggf. in Form der Eingliederung der Stiftung Datenschutz in die Stiftung Warentest – möglich erscheint.		
Soll die Stiftung über Waren und Dienstleistungen deutscher Anbieter hinaus auch solche ausländischer Anbieter auf dem deutschen Markt testen?	Dafür spricht, <ul style="list-style-type: none"> - dass solche Dienstleistungen von den Bürgern in immer stärkerem Umfang genutzt werden; - dass eine Datenschutzbewertung ausländischer Anbieter durch deutsche Datenschutzkontrollinstanzen nur eingeschränkt oder gar nicht möglich ist; - dass die Datenschutzniveaus international sehr unterschiedlich sind. 	Dagegen spricht, <ul style="list-style-type: none"> - dass solche Kontrollen schwierig und aufwändig sind; - dass Bewertungskriterien bei den international sehr unterschiedlichen Vorstellungen erst erarbeitet werden müssen. 	2.1.2
Soll die Stiftung über Waren und Dienstleistungen privater Anbieter hinaus auch solche öffentlicher Behörden und Unternehmen bewerten?	Dafür spricht, <ul style="list-style-type: none"> - dass auch und gerade öffentliche Behörden und Unternehmen in großem Umfang personenbezogene Daten verarbeiten; - dass auch dort Gefahren für die Betroffenen drohen. 	Dagegen spricht, <ul style="list-style-type: none"> - dass die Regelungsdichte durch Spezialgesetze oft sehr hoch ist; - dass eine wirksame Kontrolle durch Datenschutzkontrollinstanzen, Aufsichtsbehörden, Gerichte und die Öffentlichkeit stattfindet. 	2.1.3

Entscheidungsgegenstand	Vor- und Nachteile		Tz.
<p>Soll die Stiftung über Vergleichsbewertungen hinaus bei Nachweis bestimmter Mindestanforderungen von Waren oder Dienstleistungen Gütesiegel zuerkennen?</p>	<p>Dafür spricht,</p> <ul style="list-style-type: none"> - dass die Stiftung eigenständig Prüfkriterien erarbeitet; - dass die Stiftung sehr sachkundig ist und dies im Rahmen von zwei „Modellen“, d.h. doppelt verwerten könnte; - dass das Vertrauen, das die Stiftung genießen wird, auch auf den Bereich der Zertifizierung (Gütesiegel) übertragen werden könnte; - dass die Stiftung sich hierdurch eine weitere Finanzierungsmöglichkeit erschließen könnte; - dass ein Gütesiegel mit professionellem Logo den Markenauftritt der Stiftung fördern würde. 	<p>Dagegen spricht,</p> <ul style="list-style-type: none"> - dass Gütesiegel üblicherweise von den Geprüften vergütet werden und die Stiftung von solchen Zahlungen nicht abhängig sein darf, um nicht den Anschein der Abhängigkeit zu erzeugen; - dass überzeugende datenschutzrechtliche Bewertungsmaßstäbe, die über die Gesetzeskonformität hinausgehen, noch nicht vorliegen. 	2.2. 4.6.
<p>Bei Verneinung der vorhergehenden Frage: Soll die Stiftung über Vergleichsbewertungen hinaus</p> <p>a) Standards für Gütesiegel vorgeben, und</p> <p>b) Einrichtungen oder Personen akkreditieren, die den Nachweis zur ordnungsgemäßen Zuerkennung von Gütesiegeln nach Maßgabe der von der Stiftung vorgegebenen Standards erbracht haben?</p>	<p>a) Für die Vorgabe von Gütesiegel-Standards spricht,</p> <ul style="list-style-type: none"> - dass die Stiftung sachkundig ist und Bewertungskriterien für ihre eigene Tätigkeit ohnehin entwickelt; - dass die Entwicklung eigener Standards zu einer vertieften, über 	<p>a) Gegen die Vorgabe von Gütesiegel-Standards spricht,</p> <ul style="list-style-type: none"> - dass die Entwicklung eigener Standards einen erheblichen Aufwand erfordern kann, der vorab entsprechende Investitionen erfordert. 	2.2.

Entscheidungsgegenstand	Vor- und Nachteile		Tz.
	<p>den Vergleich vorgefundener Produkte hinausgehenden Auseinandersetzung mit bestehenden Standards in den Bereichen IT-Sicherheit und Datenschutz zwingt.</p> <p>b) Für die Akkreditierung entsprechender Institutionen und Personen spricht,</p> <ul style="list-style-type: none"> - dass die Stiftung sachkundig ist und Bewertungskriterien entwickelt; - dass die Gefahren für die Neutralität bei der bloßen Bewertung von Prüfern gering erscheinen. 	<p>b) Gegen die Akkreditierung entsprechender Institutionen und Personen spricht,</p> <ul style="list-style-type: none"> - dass auch hier Private Vergütungen für die Zertifizierung zahlen. 	
Soll die Stiftung über Vergleichsbewertungen hinaus auch Datenschutz-Audits durchführen?	<p>Dafür spricht,</p> <ul style="list-style-type: none"> - dass die Stiftung eigenständig Prüfkriterien erarbeitet; - dass die Stiftung sehr sachkundig ist. 	<p>Dagegen spricht,</p> <ul style="list-style-type: none"> - dass Audits üblicherweise von den Auditierten vergütet werden und die Stiftung von solchen Zahlungen nicht abhängig sein darf, um nicht den Anschein der Abhängigkeit zu erzeugen. 	
<p>Bei Verneinung der vorhergehenden Frage: Soll die Stiftung über Vergleichsbewertungen hinaus</p> <p>a) Standards für Datenschutz-audits vorgeben, und</p> <p>b) Einrichtungen oder Personen akkreditieren, die den Nachweis zur ordnungsgemäßer Durchführung von Datenschutzaudits nach</p>	<p>a) Für die Vorgabe von DS-Audit-Standards spricht,</p> <ul style="list-style-type: none"> - dass die Stiftung sachkundig ist und Bewertungskriterien für ihre eigene Tätigkeit ohnehin entwickelt. 	<p>a) Gegen die Vorgabe von DS-Audit-Standards spricht,</p> <ul style="list-style-type: none"> - dass die Unabhängigkeit der Stiftung beeinträchtigt wird. 	

Entscheidungsgegenstand	Vor- und Nachteile		Tz.
Maßgabe der von der Stiftung vorgegebenen Standards	b) Für die Akkreditierung entsprechender Institutionen und Personen spricht, <ul style="list-style-type: none"> - dass die Stiftung sachkundig ist und Bewertungskriterien entwickelt; - dass die Gefahren für die Neutralität bei der bloßen Bewertung von Prüfern gering erscheinen. 	b) Gegen die Akkreditierung entsprechender Institutionen und Personen spricht, <ul style="list-style-type: none"> - dass auch hier Private Vergütungen für die Zertifizierung zahlen. 	
Soll die Stiftung im Rahmen der vergleichenden Bewertung als Vergleichskriterium auch berücksichtigen, ob der Anbieter kooperiert und die für eine möglichst umfassende Prüfung erforderlichen Feststellungen ermöglicht hat?	Dafür spricht, <ul style="list-style-type: none"> - dass die Stiftung zur gründlichen Prüfung insbesondere der Durchsetzung von Datenschutzkonzepten auf die Kooperation der Bewerteten angewiesen ist; - dass nur so Druck zur Kooperation erzeugt werden kann. 	Dagegen spricht, <ul style="list-style-type: none"> - dass so Negativbewertungen auch zu Stande kommen können, wenn das Datenschutzniveau des Betroffenen hoch ist. 	2.4.
Soll die Stiftung im Rahmen der Fortentwicklung der Prüfkriterien auch Ansätze und Kriterien aus dem Bereich außerhalb der EU, insbesondere aus den USA und ggf. Fernost einbeziehen?	Dafür spricht, <ul style="list-style-type: none"> - dass Datenschutz global wirken muss; - dass die Adressaten global operieren; - dass die Akzeptanz steigt, wenn Datenschutz kein Markthemmnis mehr ist. 	Dagegen spricht, <ul style="list-style-type: none"> - dass das Gesetz nationale Ausprägung und Wirkung hat; - dass der Gesetzgeber, ggf. EU-RL zur kompatiblen Gesetzgebung berufen ist; - dass das Verhältnis des Einzelnen zum „Datenschutz“ und zur „Privatsphäre“ noch sehr stark von 	

Entscheidungsgegenstand	Vor- und Nachteile		Tz.
		nationalen Eigenheiten geprägt ist.	
Sollte die Stiftung im Namen den Begriff „Datenschutz“ tragen oder einer anderen Terminologie den Vorzug geben?	<p>Dafür spricht,</p> <ul style="list-style-type: none"> - dass zahlreiche Gesetze und Einrichtungen den Begriff tragen; - dass der Begriff seit 40 Jahren benutzt wird; - dass auch die Charta die „personenbezogenen Daten“ schützt. 	<p>Dagegen spricht,</p> <ul style="list-style-type: none"> - dass das falsche Objekt genannt wird; - dass das eigentliche Schutzgut herausgestellt, ggf. entwickelt werden sollte; - dass der Begriff international gute Resonanz und Kompatibilität erreicht, so wie etwa „Persönlichkeitsrecht“ und „Privatsphäre“ als materiell rechtliche Positionen „privacy“ vergleichbar sind. 	
Ist einer Stiftung öffentlichen Rechts Vorzug zu geben gegenüber einer privatrechtlichen Organisationsform?	<p>Dafür spricht,</p> <ul style="list-style-type: none"> - dass durch das notwendige Gesetzgebungsverfahren das Vorhaben besondere Aufmerksamkeit in der Öffentlichkeit erfährt; - dass auch für eine privatrechtliche Organisationsform haushaltsrechtliche Voraussetzungen geschaffen werden müssen. 	<p>Dagegen spricht,</p> <ul style="list-style-type: none"> - dass ein solches Gesetzgebungsverfahren mit einem nicht unerheblichen Zeitaufwand verbunden ist; - dass auch bei vergleichbaren Stiftungen (beispielsweise Stiftung Warentest) privatrechtliche Organisationsformen existieren. 	5.1.