DOI: 10.1007/s10273-012-1397-9

Nicola Jentzsch*

Was können Datenschutz-Gütesiegel leisten?

Die Europäische Kommission unterstützt die Entwicklung und Nutzung von Datenschutz-Gütesiegeln. Diese sollen die Konformität von Produkten und Dienstleistungen mit Datenschutzregeln zertifizieren und Verbrauchern Produktauswahl und -vergleiche erleichtern. In Deutschland plant die Bundesregierung eine Stiftung Datenschutz, die Produkte und Dienstleistungen auf Datenschutzfreundlichkeit prüfen soll. Fraglich ist allerdings, ob Gütesiegel tatsächlich einen Anreizmechanismus für einen erhöhten Datenschutz bieten und somit die Erwartungen der Politik erfüllen.

In der Europäischen Union wird im Augenblick an einer Reform der Europäischen Datenschutzrichtlinie von 1995 gearbeitet.[1] In dem veröffentlichten Vorschlag der Europäischen Kommission wird in Artikel 39 darauf verwiesen, dass die Kommission sowie die Mitgliedstaaten die Entwicklung von Datenschutz-Zertifizierungsmechanismen, Gütesiegeln und ähnlichen IT-Vertrauenszeichen unterstützen sollen. Dies soll Verbrauchern eine einfachere und schnellere Beurteilung des durch IT-Produkte oder IT-Dienstleistungen gewährleisteten Datenschutzes ermöglichen. Schon in vorherigen Dokumenten war auf entsprechende Maßnahmen hingewiesen worden.[2] In Deutschland ist mittlerweile die Bundesregierung aktiv geworden und plant die Einrichtung einer Stiftung Datenschutz. Ziel der Stiftung mit geplantem Sitz in Leipzig ist es, Produkte und Dienstleistungen auf Datenschutzkonformität zu prüfen. Der Ansatz der Gütesiegel-Vergabe birgt allerdings eine ganze Reihe von bislang kaum erforschten Fragen. Beziehen Verbraucher solche Siegel in ihre Kaufentscheidung ein oder sind andere Produktqualitäten (Preis, Funktionalitäten) wichtiger? Welche Wirkung haben Siegel, wenn das Unternehmen bereits ein Datenschutz-Versprechen hat? Welches Design dieser Siegel ist besonders verbraucherfreundlich? Und wie kann man gewährleisten, dass es in zertifizierenden Institutionen nicht zu Interessenkonflikten kommt, ähnlich jenen der Rating-Agenturen im Finanzmarkt? Neben der dünnen empirischen Erkenntnislage können auf Basis der ökonomischen Theorie zum Zertifizierungswettbewerb weitere Bedenken an der Effektivität von Datenschutz-Siegeln geäußert werden. Bevor die Europäische Kommission die Arbeit an einem pan-europäischen System der Datenschutz-Zertifizierung aufnimmt, sollten diese grundlegenden Fragen geklärt sein.

Dieser Artikel gibt daher einen Überblick über Zertifizierung als Geschäftsmodell, wägt die Vor- und Nachteile ab und erläutert ökonomisch grundlegende Probleme im Zertifizierungswettbewerb. Anschließend wird in die empirischen und experimentellen Erkenntnisse zu IT-Gütesiegel eingeführt, um dann im Hinblick auf die Leistungsfähigkeit von Datenschutz-Gütesiegeln Schlüsse zu ziehen.

Datenschutz-Zertifizierung als Geschäftsmodell

Ein Kernziel von Datenschutz-Gütesiegeln ist die Identifizierung von Datenschutz-konformen Prozessen, IT-Produkten und IT-Dienstleistungen. Durch ein Siegel erhalten diese ein sichtbares Zeichen für den gewährleisteten Datenschutz (Datenschutz-Compliance). Zertifikate sollen so Informationsasymmetrien reduzieren und Unternehmen den Aufbau eines guten Rufes am Markt ermöglichen. In einem Zertifizierungssystem vergibt eine zertifizierende Institution ein Zertifikat (Datenschutz-Gütesiegel oder Gütezeichen), welches das zertifizierte Unternehmen zu Marketing-Zwecken verwenden kann. Die zertifizierende Institution wird für diese Dienstleistung vom Unterneh-

* Die Autorin vertritt hier allein ihre persönliche Auffassung und in keiner Weise die des DIW Berlin.

1 Vgl. European Commission: Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25.1.2012.

2 Eine ausführliche Diskussion politischer Maßnahmen zu Datenschutz-Gütesiegeln ist Teil einer erweiterten Studie der Europäischen Agentur für Netz- und Informationssicherheit (ENISA). Teile des Aufsatzes entstanden als Hintergrund-Bericht im Kontext des Arbeitsprogramms 2012 (Arbeitspaket 4.3).

Dr. Nicola Jentzsch ist wissenschaftliche Mitarbeiterin am DIW Berlin.

Tabelle 1
Datenschutz-Gütesiegel

	Name und Anbieter	Umfang der Analyse	Statistik
USA 1997	TRUSTe KonsortiumCommerceNet, EFF, Boston Consulting http://www.truste.com/	Datenschutz von Webseiten Datenschutz-Versprechen, Selbsteinschätzung, Analyse durch Dritte Gebührenbasierend	1300* (2005)
USA 1999	BBBOnline Better Business Bureau www.bbb.org	Datenschutz von Webseiten Anforderungen der Selbstregulierung (der FTC, DOC) Gebührenbasierend	600* (2005)
EU 2008	EuroPriSe Konsortium Mitgliedern in mehreren EU Staaten www.european-privacy-seal.eu/	IT-Produkte und IT-Dienstleistungen, Compliance mit EU-Datenschutzvorschriften Analyse, Audits und Bericht, Akzeptanz des Berichts	25** (2012)
Deutschland 2002	ULD Datenschutz-Gütesiegel Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein www.datenschutzzentrum.de	IT-Produkte und IT-Dienstleistungen, Compliance mit Landesdatenschutzgesetz Analyse, Audits und Bericht, Akzeptanz des Berichts	75** (2012)
Deutschland k. A.	TÜVit Trusted Site Privacy TÜV Nord www.tuvit.de/Trusted_Site_Privacy.asp	IT-Produkte und IT-Dienstleistungen, Compliance mit EU-Richtlinien, BDSG und/oder TÜVit Kriterien Analyse, Audits und Dokumentation	3**
Deutschland 2009	SCHUFA Data Protection Seal SCHUFA Holding AG www.datenschutzsiegel.de/	IT-Produkte und IT-Dienstleistungen, Compliance mit BDSG, SCHUFA Kriterien und D21-Standards	7** (Auswahl)

FTC = Federal Trade Commission, DOC = Dept. Of Commerce. * Zahlen sind aus T. Moores: Do Consumers Understand the Role of Privacy Seals in E-Commerce?, in: Communications of the ACM, 48. Jg. (2005), Nr. 3, S. 86-91. ** Website der einzelnen Institutionen. BDSG ist das Bundesgesetz über den Datenschutz in Deutschland.

Quelle: Eigene Zusammenstellung.

men bezahlt, das so in seinen Ruf investiert. Die Politik sieht Gütesiegel als wichtige marktkonforme Maßnahme zur Erhöhung des Datenschutzes und der Kontrolle über persönliche Informationen. Es gibt verschiedene Mechanismen, auf deren Basis Gütesiegel vergeben werden. Grundsätzlich können zwei Vergabearten unterschieden werden:

- Gütesiegel, die durch öffentliche Stellen vergeben werden und

- Gütesiegel, die von privaten Institutionen vergeben werden, die entweder gemeinnützig oder gewinnorientiert arbeiten.

Darüber hinaus unterscheiden sich Gütesiegel auch in Art und Umfang der Analyse und Bewertung von IT-Produkten und IT-Dienstleistungen. So gibt es Gütesiegel für die generelle positive Bewertung des Käuferschutzes im Online-Shopping. Hier umfasst die Bewertung Informations- und Vertragsphase, Lieferkonditionen und -abwicklung sowie Nachbearbeitung. Beispiele hierfür sind die Siegel der D21-Initiative (Trusted ShopsGuarantee), das Prüfsiegel des TÜV SÜD (Safer Shopping) und das Siegel des EuroHandelsinstitut EHI Retail Institute (EHI geprüfter Online Shop). Andere Gütezeichen basieren dagegen auf technischen Compliance-Standards, wie die Common Criteria für Sicherheit in der Informationstechnik und einige TÜV-Siegel.

Eine dritte Art von Gütesiegel umfasst nur die Datenschutz-relevanten Aspekte der Analyse und Beurteilung. Diese Siegeltypen unterscheiden sich durch die Gesetzesgrundlage, auf welche sich die Zertifikate beziehen: Während die einen auf EU-Datenschutz-Standards basieren (z.B. das EuroPriSe-Siegel), basieren andere auf dem Bundesdatenschutzgesetz (SCHUFA-Datenschutz-Siegel) und dritte auf einem Landesdatenschutzgesetz (z.B. das ULD Datenschutz-Gütesiegel). Einige Anbieter zertifizieren auch die Standards für sichere Online-Transaktionen der erwähnten D21-Initiative. Andere Anbieter von Zertifizierung setzen ihre eigenen Standards, die nicht auf spezifisch nationaler Gesetzgebung basieren. Beispiele hierfür sind die amerikanischen Siegel TRUSTe und BBBOnline.

Die Kosten der Zertifizierungen unterscheiden sich je nach Umfang und Intensität der Beurteilung und reichen von 0 bis 15 000 Euro oder mehr. Tabelle 1 präsentiert einen Überblick über die Siegel, im Folgenden sollen aber nur drei Beispiele diskutiert werden.

- *European Privacy Seal (EuroPriSe)*: Im Juli 2008 wurde das erste EuroPriSe-Gütesiegel von einem Konsortium

unter Führung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) der Internet-Suchmaschine Ixquick gewährt. Im Allgemeinen können sich interessierte Unternehmen um die Zertifizierung von IT-Produkten oder IT-basierten Dienstleistungen bei EuroPriSe bewerben, um so die Einhaltung der EU-Datenschutzvorschriften zertifiziert zu bekommen. Es besteht hierbei ein Katalog von Kriterien, die in der Compliance-Analyse berücksichtigt werden.[3] Unternehmen wählen jeweils einen Rechtsverständigen und einen technischen Sachverständigen aus einer Liste von Experten, die bei dem Konsortium akkreditiert sind. Diese erstellen einen vertraulichen Bericht, der von EuroPriSe bezüglich Methodik, Konsistenz und Vollständigkeit geprüft wird. Er dient als Grundlage für die Entscheidung, ein Gütesiegel für die Dauer von zwei Jahren zu gewähren. Bis Mai 2012 wurden 25 Siegel vergeben oder erneuert.

- *ULD Datenschutz-Gütesiegel*: Seit 2002 vergibt das ULD ein Siegel für Datenschutz im Bereich IT-Hardware, Software und automatisierte Prozesse, die für den Einsatz im öffentlichen Dienst bestimmt sind. Im Mittelpunkt steht die Einhaltung des Landesdatenschutzgesetzes von Schleswig-Holstein. Der Prozess stand Pate für das eben erwähnte EuroPriSe-Siegel. Der Antragsteller kann einen Sachverständigen aus einer Liste der akkreditierten Experten am ULD wählen. Diese nehmen die rechtliche und technische Beurteilung des Produktes oder Verfahrens vor, die in einem Bericht dokumentiert wird. Der Bericht und ein Zertifizierungs-Antrag wird beim ULD eingereicht. Sollten diese genehmigt werden, wird das Siegel für zwei Jahre gewährt. Bis Mai 2012 wurden 75 Verfahren oder Produkte von zumeist deutschen Unternehmen vom ULD zertifiziert oder erneuert.

- *SCHUFA Datenschutz-Siegel*: Dieses Siegel wurde 2009 von der SCHUFA Holding AG, Deutschlands größter Kreditauskunft, ins Leben gerufen. Es wird für die Einhaltung der nationalen Datenschutz-Standards vergeben, aber es können unter anderem auch D21-Standards oder SCHUFA Best Practices zertifiziert werden. Das Siegel ist für drei Jahre gültig. Sein Geltungsbereich umfasst: (1) die Struktur des Datenschutzes in dem sich bewerbenden Unternehmen, (2) Dokumentation, (3) Rechtmäßigkeit der Datenverarbeitung, und (4) eine Risikobewertung. Zuerst wird der Antragsteller über den Kriterien-Katalog informiert, dann darf er eine Selbsteinschätzung vornehmen, nach welcher ein eintägiges Auditing unter der Teilnahme eines unabhängigen Experten und eines SCHUFA-Sachverständigen stattfindet. Diese Prüfung bringt potentielle Schwächen und Möglichkeiten zur Optimierung hervor, nach deren Behebung und Umsetzung das Unternehmen erneut bewertet und schließlich zertifiziert wird. Die SCHUFA führt nur sieben Unternehmen als Referenz ihrer zertifizierten Kunden auf.

Dieser kurze Überblick zeigt, dass sich zwar das Auswahlverfahren der Experten der Siegel-Anbieter unterscheidet, aber in allen Fällen der Antragsteller die zertifizierende Institution bezahlt. In dieser Situation können Interessenskonflikte entstehen. Aus der ökonomischen Theorie sind solche Situationen auch als Principal-Agent-Probleme bekannt. So haben Agenten, die untereinander in Konkurrenz stehen, einen Anreiz, den Auftraggeber durch geringe Preise und niedrigschwellige Standardverfahren zu locken. Der Wettbewerb bei solchen Anbietern kann zu einer gegenseitigen Unterbietung durch die Reduzierung von Standards führen, um Anteile im Markt der Datenschutz-Siegel zu gewinnen. Eine regulierende Intervention könnte diese unerwünschten Entwicklungen durch Festlegung von Mindeststandards für Zertifizierung, Analyse und Experten-Akkreditierung vorbeugen. Eine Regulierungsbehörde sollte außerdem prüfen, ob Zertifikate in diskriminierender Weise einigen Institutionen gewährt werden, die die Bewertungskriterien erfüllen, anderen aber nicht, die dies ebenso tun.

Vor- und Nachteile der Zertifizierung des Datenschutzes

Für Unternehmen und Verbraucher gibt es eine Reihe von Vor- und Nachteilen von Datenschutz-Zertifikaten (vgl. Tabelle 2), sowie eine Reihe von ungelösten Fragen. Die Auswirkung von Gütesiegeln auf das Kaufverhalten ist bisher wenig erforscht. Politik und Forschung müssen mehr investieren, um besser zu verstehen, wie Gütesiegel mit dem allgemeinen Ruf eines Unternehmens interagieren, seinem geleisteten Datenschutzversprechen und möglichen Datenskandalen. Es gibt außerdem kaum unabhängige empirische Erkenntnisse über die Renditen von Investitionen in Datenschutz-Gütesiegel. Auf Basis dieser dürftigen Erkenntnislage sind die hier diskutierten Vor- und Nachteile eher theoretischer Natur.

Für Verbraucher bergen Gütesiegel das Potenzial, Anreize für einen erhöhten Schutz im Umgang mit personenbezogenen Daten in Unternehmen zu schaffen. Allerdings werden Verbraucher sie nur dann als relevanten Aspekt in ihre Entscheidungen mit einbeziehen, wenn sie tatsächlich Differenzierungspotential haben. Nur dann lohnt es sich wiederum für Unternehmen in ein solches Signal zu

3 Vgl. EuroPriSe: EuroPriSe Criteria, Mai 2011, https://www.european-privacy-seal.eu/criteria/EuroPriSeCriteriaMay2011final.pdf (Download: 6.5.2012).

Tabelle 2
Vorteile und Nachteile der Datenschutz-Zertifizierung

Angebotsseite: Unternehmen	Nachfrageseite: Verbraucher
Vorteile	Vorteile
• Möglichkeit der glaubwürdigen Signalisierung von Datenschutz-Compliance • Anreiz zur Erhöhung von Produkt-/Service-Qualität in Bezug auf Datenschutz • Differenzierung im Wettbewerb • Steigerung der Reputation und des Verbrauchervertrauens • Externer Mechanismus, der Schwächen in den Unternehmensprozessen offenlegen könnte • Interne Risikokontrolle und Sicherheits-Optimierung	• Glaubwürdiges Qualitätssignal für höheren Datenschutz (im Vergleich zu nicht zertifizierten Unternehmen) • Potentiell zusätzlicher Aspekt in der Kaufentscheidung • Erhöhung der Vergleichbarkeit von IT-Produkten und IT-Dienstleistungen • Zunahme der Auswahl der Angebote (Angebote mit und ohne Siegel) • Verringern der Informationskosten • Generierung von vermehrtem Datenschutz- und Risikobewusstsein
Nachteile	Nachteile
• Einmalige und laufende Investitionsausgaben für Gütesiegel • Mindeststandard kann als Marktbarriere wirken, wenn es Niedrigqualitätsanbieter gibt, die den Standard nicht erfüllen • Versunkene Investitionen in Gütesiegel, wenn diese keine Rolle in Entscheidungen der Verbraucher spielen	• Zusätzliche Produkteigenschaft kann Entscheidungen/Vergleiche verkomplizieren • Gütesiegel erhöhen die Transparenz nicht, wenn Zertifizierungs-Mechanismen nicht transparent sind • Niedrigqualitäts-Nachfrage wird unter Umständen nicht erfüllt, wenn es Mindeststandards gibt

Quelle: Eigene Zusammenstellung.

investieren. Es ist hierbei zu beachten, dass eine Minderheit von Verbrauchern, die potentiell einen Preisaufschlag für ein solches Siegel zahlen würde, wohl kaum jener kritischen Masse entsprechen dürfte, die notwendig wäre, um die einmaligen sowie laufenden Investitionen in solche Siegel zu rechtfertigen. Während Siegel zwar Vergleiche ermöglichen, gibt es auf der anderen Seite immer mehr davon. Eine solche Vielfalt kann die Vergleichbarkeit reduzieren. Verbraucher müssten die verschiedenen Mechanismen kennen, auf deren Basis die Siegel gewährt werden, um sie vergleichen zu können. Folglich wird das Vertrauen größtenteils heuristisch aus dem Ruf der zertifizierenden Institution abgeleitet. Dies ist auch bei anderen Verbraucher-Gütesiegeln der Fall (z.B. Stiftung Warentest).

Ökonomische Theorie wirft Fragen nach effektivem Wettbewerb auf

Durch Siegel sollen Anreize für Unternehmen geschaffen werden, erhöhte Datenschutz-Standards zu befolgen, aus denen Wettbewerbsvorteile erwachsen.[4] Solche Zertifikate oder Garantien werden zunächst auch von der ökonomischen Theorie positiv untermauert. Verträge unterliegen asymmetrischen Informationen, wenn ein Vertragspartner nicht in der Lage ist, das Verhalten und Handeln des anderen Vertragspartners vollständig zu beobachten. Wie George Akerlof in seinem berühmten Zitronen-Beispiel zeigt, können Käufer von Gebrauchtfahrzeugen die Qualität des einzelnen Gebrauchtwagens nicht vollständig beurteilen.[5] In einem solchen Markt treibt adverse Selektion qualitativ höherwertige Gebrauchtwagen aus dem Markt, in dem schlechte Autos übrig bleiben. Garantien beschreibt Akerlof als eine Möglichkeit, solche Probleme zu reduzieren. Garantien können aber zusätzliche Asymmetrien induzieren. Ein Gütesiegel als Garantie von zertifiziertem Datenschutz ist hierbei eine Signalisierungsstrategie, die ein Unternehmen wählt, um sich aus der Konkurrenz hervorzuheben.

Datenschutz-Compliance als „private Information" soll hiermit glaubwürdig Verbrauchern signalisiert werden. Nur wenn das Signal glaubwürdig ist, wird ein Unternehmen in dieses Signal investieren. Ist ein Datenschutz-Siegel beispielsweise schwer zu erhalten, dann birgt es ein größeres Differenzierungspotential gegenüber Unternehmen, die es nicht erhalten haben, und erhöht somit die Reputation des Trägers.[6]

Für eine privatwirtschaftliche Zertifizierungsstelle ergibt sich daraus allerdings die Abwägung des Verhältnisses von Akzeptanz oder Ablehnung von Unternehmen für Siegel (d.h. Differenzierungspotential) und der eigenen Gewinnmaximierung durch Steigerung der Siegelverga-

4 Vgl. T. Weichert: Datenschutzzertifizierung – Vorteile für Unternehmen, in: ITK-Kompendium 2010, S. 274-279.

5 Vgl. G. A. Akerlof: The Market for „Lemons": Quality Uncertainty and the Market Mechanism, in: The Quarterly Journal of Economics, 84. Jg. (1970), Nr. 3, S. 488-500.

6 Über das Verhältnis von abgelehnten zu zertifizierten Unternehmen sind bisher keine Zahlen vorhanden, auch nicht darüber, wie vielen Unternehmen Siegel wieder entzogen wurden.

be. Werden beispielsweise zu viele Unternehmen für ein Siegel akzeptiert, so verliert dieses Signal seinen Informationswert, da sein Differenzierungspotential sinkt. Des Weiteren könnten Unternehmen den Anreiz haben, erst strategisch in Gütesiegel zu investieren und dann ihre aufgebaute Reputation auszubeuten. Aus diesem Grund ist es angezeigt, Datenschutz-Siegel nur temporär zu vergeben, was bei den meisten hier vorgestellten Systemen der Fall ist.

Bei einer Vielfalt von Zertifikaten hat der Verbraucher typischerweise wenig Mittel, um die Qualitäten der verschiedenen Gütesiegel zu vergleichen. In der Mehrzahl der Fälle ist nur erkennbar, ob ein Gütesiegel existiert oder nicht und nicht welche Stärke des Schutzes es garantiert. Ein „Ampel-System“ würde differenziertere Vergleiche ermöglichen.

Aufgrund der zusätzlich eingeführten Informationsasymmetrie können Zertifizierungsmechanismen also kein effizientes Funktionieren des Marktes garantieren. Allerdings können diese Asymmetrien eine Rechtfertigungsgrundlage für Interventionen darstellen, welche die Glaubwürdigkeit von Signalen erhöhen und die Suchkosten der Verbraucher reduzieren könnten. Des Weiteren könnten regulierende Interventionen Interessenskonflikte reduzieren, die zu einer Ausbeutung des Zertifizierung-Mechanismus durch Unternehmen führen würden.

Mindeststandards sind für vertrauenswürdige Datenschutz-Gütesiegel notwendig

Eine Regulierungsbehörde kann den Informationsgehalt sowie die Vergleichbarkeit von Siegeln verbessern, indem sie qualitative Mindestanforderungen an die Zertifizierung stellt. Die Maßnahmen sollten vor allem darauf abzielen, dass Datenschutz-Siegel für Verbraucher aussagekräftig und vertrauenswürdig sind und bleiben. Siegel, die eine Mehrzahl von Unternehmen für Produkte unterschiedlicher Qualität erwerben können, würden sich möglicherweise in den Augen von Verbrauchern entwerten. Darüber hinaus sollte eine Behörde potentielle Interessenskonflikte in den vertraglichen Beziehungen zwischen der zertifizierenden Institution und Unternehmen reduzieren. Dies kann entweder durch eine direkte Regulierung der Verträge erreicht werden, durch die Forderung der Offenlegung von Interessenskonflikten oder durch die Schaffung von unabhängigen Zertifizierungs-Institutionen. So gilt, dass

- Mindeststandards in der Zertifizierung die Qualität der Datenschutz-Siegel am Markt erhöhen können;
- Mindeststandards sich aber gleichzeitig auch als Markteintrittsbarriere auswirken können, wenn die Zertifizierung Voraussetzung für eine Auftragsvergabe wird, beispielsweise bei öffentlichen Ausschreibungen.

Wie bereits angesprochen, haben Datenschutz-Siegel das Potential, die Differenzierung zwischen den Unternehmen zu erhöhen. Dieser zusätzliche Grad an Differenzierung kann allerdings den Wettbewerb verringern.[7] Das signalisierende Unternehmen gewinnt einen Differenzierungsgrad hinzu und kann andere Preise setzen als der Konkurrent, da es sich beim Marktangebot nun um ein differenziertes Produkt handelt. Die Zweckmäßigkeit der Datenschutz-Siegel hängt ganz wesentlich vom Verbrauchervertrauen ab und ob es keine anderen Signale gibt, die in der Verbraucherentscheidung wichtiger sind und somit die Wirkung des Datenschutz-Gütesiegels reduzieren oder ganz verdrängen.

Empirische Erkenntnisse zu Datenschutz-Gütesiegeln

Es gibt in dem Forschungsgebiet der Ökonomie der Privatsphäre nur wenige experimentelle Arbeiten, die Verbraucherverhalten und Datenschutz-Gütesiegel zum Gegenstand haben. Es gibt zwar Umfrage-basierte Experimente zu diesem Thema, aber diese sind wenig aussagekräftig für reale Handlungen von Verbrauchern. Reine (unbezahlte) Informationsangaben von Verbrauchern unterscheiden sich grundsätzlich von Kauftransaktionen, bei denen persönliche Information ein Beifang ist und Verbraucher neben dem Privatsphärenrisiko zusätzlich ein monetäres Risiko tragen. Tabelle 3 gibt einen Überblick über entsprechende Verhaltensexperimente. Beispielsweise führten Hui et al. in Singapur einen Feldversuch im Internet durch.[8] Zu diesem Zweck arbeiteten sie mit einem lokalen Unternehmen, das das Experiment auf seiner Website unter seinem echten Domain-Namen hostete. Die Teilnehmer wurden nicht über das Experiment informiert. Sie sollten einen Umfragebogen des Unternehmens gegen Bezahlung ausfüllen. Hierbei variierten die Experimentatoren die verschiedenen Situationen, in denen die Probanden den Fragebogen ausfüllten. Ein Hauptergebnis dieser Studie ist, dass die Existenz einer Datenschutzerklärung mehr Teilnehmer dazu verleitete, persönliche Informationen anzugeben. Die Existenz eines

7 Vgl. N. Jentzsch, A. Harasser, S. Preibusch: Monetising Privacy – An Economic Model of the Pricing of Personal Information, ENISA Report, Greece (2012), http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy.

8 K.-L. Hui, H. H. Teo, S.-Y. T. Lee: The Value of Privacy Assurance: An Exploratory Field Experiment, in: MIS Quarterly, Vol. 31 (2007), Nr. 1, S. 19-33.

Tabelle 3
Forschung im Bereich Datenschutz-Gütesiegel

Autoren	Typ Transaktion/Experiment/Probanden	Resultate
Egelman et al. (2009)	• Incentivierte Kauftransaktion • Internet-Suchmaschine im Labor, die Datenschutz-Gütesiegel als Symbole zeigt • 89 Probanden (Studenten)	• Umsetzung von Datenschutz-Versprechen in ein Gütesiegel • Wenn Datenschutz-Versprechen vereinfacht als Gütesiegel dargestellt werden, dann beeinflussen sie die Auswahl des Anbieters bei sensitiven Einkäufen
Gideon et al. (2006)	• Incentivierte Kauftransaktion • Internet-Shopping-Situation im Labor • 24 Probanden (Studenten)	• Umsetzung von Datenschutz-Versprechen in ein Gütesiegel (wie in Egelman et al. 2009) • Wenn Datenschutz-Versprechen als Gütesiegel dargestellt werden, dann beeinflussen sie die Auswahl des Anbieters bei sensitiven Einkäufen
Hui et al. (2007)	• Incentivierte Informationstransaktion • Einladung auf Webseite mit einer auszufüllenden Umfrage • 109 Probanden (Studenten)	• Datenschutz-Versprechen erhöht Informationspreisgabe • Datenschutz-Gütesiegel erhöhen die Informationspreisgabe nicht
Rifon et al. (2006)	• Incentivierte Informationstransaktion • Einladung auf Webseite mit hypothetischer Einkaufssituation • Fragen zur Wahrnehmung der Probanden • 210 Antworten von Probanden (Studenten im Grundstudium)	• Datenschutz-Gütesiegel erhöhen die Erwartung, dass eine Firma transparent ist im Umgang mit Daten • Datenschutz-Gütesiegel induzieren Vertrauen • Datenschutz-Gütesiegel haben keine Auswirkung auf die Intention persönliche Informationen preiszugeben (reale Handlungen wurden hier nicht getestet)

Quelle: S. Egelman, J. Tsai, L. F. Cranor, A. Acquisti: Timing Is Everything? The Effects of Timing and Placement of Online Privacy Indicators, CHI 2009, 3.-9. April 2009, Boston, MA, USA; J. Gideon, L. Cranor, S. Egelman, A. Acquisti: Power Strips, Prophylactics, and Privacy, Oh My!, Institute for Software Research (Paper 24, 2006), http://repository.cmu.edu/isr/24; K.-L. Hui, H. H. Teo, S.-Y. T. Lee: The Value of Privacy Assurance: An Exploratory Field Experiment, in: MIS Quarterly, Vol. 31 (2007), Nr. 1, S. 19-33; N. J. Rifon, R. LaRose, S. M. Choi: Your Privacy is Sealed: Effects of Privacy Seals on Trust and Personal Disclosures, in: Journal of Consumer Affairs, 39. Jg. (2006), Nr. 2, S. 337-360.

Datenschutz-Gütesiegels jedoch nicht. Ein monetärer Anreiz hatte einen positiven Einfluss auf die Preisgabe von Informationen, während vermehrte Nachfragen nach Informationen einen negativen Einfluss hatten. Gemäß dieser Erkenntnisse macht es also für die Wettbewerbsstrategie eines Unternehmens einen Unterschied, ob es in ein Datenschutz-Gütesiegel oder in ein Datenschutzversprechen investiert. Ein Unternehmen, das beabsichtigt, die Extraktion von persönlichen Verbraucherinformationen zu maximieren wird nicht in Gütesiegel investieren.

Rifon et al. luden Studenten ein, eine experimentelle Website zu besuchen, wobei sie die Teilnehmer per Zufallszuordnung einer von zwei Situationen aussetzten (mit Gütesiegel auf der Website und ohne).[9] Danach wurden die Teilnehmer nach ihrer persönlichen Wahrnehmungen der Website befragt. Es ist zu beachten, dass auch hier keine realen Kauftransaktionen durchgeführt wurden. Nach Erkenntnissen dieser Studie erhöhte die Existenz eines Gütesiegels das Vertrauen der Teilnehmer in den Anbieter. Das Gütesiegel erhöhte auch die Erwartung, dass das Unternehmen die Verbraucher in transparenter Weise besser über seine Datenpraktiken informiert. Auf die Intention, persönliche Daten preiszugeben, hatte das Gütesiegel jedoch keinen feststellbaren Einfluss.

In Gideon et al. wurden Bedenken hinsichtlich der Privatsphäre ins Experiment eingeführt, indem die Autoren den Probanden ein mehr und ein weniger sensibles Produkt zum Kauf anboten (ein Überspannschutzgerät und eine Packung Kondome).[10] Die Teilnehmer im Labor konnten eine Suchmaschine für die Auswahl der Anbieter nutzen, bei welchen sie ein Exemplar der beiden Produkte kaufen wollten. Die Teilnehmer wurden gebeten, erst einen Anbieter für das Überspannschutzgerät zu wählen und dann einen für die Packung Kondome. Der sogenannte „Privacy Finder“ setzte hierbei die verschiedenen Datenschutz-Versprechen der Anbieter in ein markantes Ampel-Symbol um. So mussten die Probanden nicht lange Datenschutz-Versprechen lesen. Die Autoren fanden heraus, dass das Datenschutz-Symbol einen signifikanten Einfluss auf die Kondom-Käufe hatte. Die geringe Anzahl an Teilnehmern an diesem Experiment erlaubt allerdings keine detailliertere ökonometrische Analyse und Verallgemeinerung der Ergebnisse. Ein ähnliches Experiment wurde in Egelman

9 Vgl. N. J. Rifon, R. LaRose, S. M. Choi: Your Privacy is Sealed: Effects of Privacy Seals on Trust and Personal Disclosures, in: Journal of Consumer Affairs, 39. Jg. (2006), Nr. 2, S. 337-360.

10 Vgl. J. Gideon, L. Cranor, S. Egelman, A. Acquisti: Power Strips, Prophylactics, and Privacy, Oh My!, Institute for Software Research (Paper 24, 2006), http://repository.cmu.edu/isr/24.

et al. mit 89 Teilnehmern durchgeführt.[11] Diese konnten eine Packung Batterien oder ein Sex-Spielzeug erwerben. Die Anbieter unterschieden sich in ihren Schutz personenbezogener Daten. Das Ergebnis dieser Studie war, dass ein Anzeigen von Datenschutz in Form von Symbolen dazu führt, dass Käufer Datenschutz in ihre Entscheidungen einbeziehen. Sie neigen dann dazu, bei Online-Händlern zu kaufen, die einen höheren Schutz der Privatsphäre garantieren. Zu beachten ist, dass auch hier die Zahl der Teilnehmer eher gering war.

Diese Studien geben zwar einen Einblick in den Zusammenhang zwischen Verbraucherverhalten und Gütesiegel, allerdings haben sie methodische Schwächen und es ist unklar, wie robust ihre Ergebnisse sind. Daher gilt es in Zukunft folgende Fragen zu beantworten:

1. Haben Gütesiegel einen Einfluss auf Kaufentscheidungen und wenn ja, wie?

2. Welche Einflüsse haben verschiedene Gütesiegel auf die Kaufentscheidung? Führt eine Vielzahl zur Abwertung einzelner Siegel?

3. Wie interagieren Gütesiegel in ihrer Wirkung mit Datenschutz-Versprechen?

4. Unter welchen Bedingungen würde ein Unternehmen in Gütesiegel investieren und unter welchen würde es das Siegel wieder verlieren?

5. Sind andere Signale wie Preis und Qualität wichtiger als Datenschutz-Gütesiegel – verdrängen sie die Wirkung des letzteren?

Politikberatung in diesem Bereich sollte evidenzbasiert sein und sich nicht allein auf Umfrage-Erhebungen zum Thema Datenschutz-Gütesiegel stützen. Solche Umfragen zeigen letztlich nicht, wie sich Verbraucher tatsächlich am Markt verhalten.

11 S. Egelman, J. Tsai, L. F. Cranor, A. Acquisti: Timing Is Everything? The Effects of Timing and Placement of Online Privacy Indicators, CHI 2009, 3.-9. April 2009, Boston, MA, USA.

Fazit

Datenschutz-Zertifizierung hat das Potenzial, Informationsasymmetrien zu senken, Produktvergleiche zu erleichtern und Datenschutz zu befördern. Hierzu müssen diese Gütesiegel aber von den Verbrauchern tatsächlich wahrgenommen werden und in ihre Kaufentscheidungen eingehen. Regulierungsbehörden sollten also insbesondere die Qualität von Gütesiegeln in den Fokus nehmen und Mindeststandards für die Zertifizierung, Bewertung von Produkten und Dienstleistungen sowie die Akkreditierung von Experten setzen. Des Weiteren sollte die Zertifizierung transparenter werden. Die Besonderheiten des Wettbewerbs auf Märkten für Zertifizierung rechtfertigen solche Maßnahmen.

Die empirische Grundlage über Erkenntnisse zu Datenschutz-Gütesiegeln und Kaufentscheidungen ist bislang gering. Hier müsste mehr in experimentelle Forschung investiert werden. Eine der Hauptfragen ist, ob und wie Datenschutz-Gütesiegel in Verbraucherentscheidungen eingehen.

Ein weiterer großer Fragenkomplex, der hier nicht diskutiert wurde, betrifft die optimale (öffentliche oder private) Vergabepraxis sowie einheitliche Standards für Gütesiegel. Wahrscheinlich ist, dass die Vielfalt an Siegeln zunehmen wird, da es eine Reihe von unterschiedlichen Datenschutz-Regelungen gibt, auf EU-Ebene, auf nationaler Ebene, sowie regionale und Industrie-Standards. Diese Vielfalt birgt wiederum die Gefahr, dass Zertifikate bedeutungslos für Verbraucher werden, für die sie sich wenig oder gar nicht voneinander unterscheiden. Zunächst sollten die genauen Zusammenhänge zwischen Kaufentscheidungen und der Existenz von Gütesiegeln untersucht werden, bevor große internationale Zertifizierungsprogramme aufgelegt werden. Wenn Gütesiegel keine Rolle in Verbraucherentscheidungen spielen, wird auch die Hoffnung, Datenschutz über Markt-Disziplin zu befördern, enttäuscht werden.

Titel: *How Effective Are Privacy Seals?*

Abstract: *The European Commission supports the development and increased usage of privacy or data protection seals. These seals are intended to certify the compliance of products and services with data protection standards in order to facilitate product comparison and choice for consumers. In Germany, the government is currently planning a foundation for data protection, which is intended to evaluate products and services in terms of their compliance. The main question is, however, whether privacy seals are in fact an effective mechanism for furthering data protection, or whether they will not meet the high expectations of policymakers.*

JEL-Classification: *D82, D83, L15*