Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
16(4)176 G

Dr. Johann Bizer

Modernisierung des Datenschutzes

Stellungnahme zur öffentlichen Anhörung
zur „Modernisierung des Datenschutzes“ am 5. März 2007

1. Eine moderne Datenschutzkonzeption muss eine wirksame Antwort auf die Herausforderungen der Risiken und Gefahren für das informationelle Selbstbestimmungsrecht durch die elektronische, dezentrale und vernetzte Verarbeitung personenbezogener Daten geben. Die Bedeutung der informationellen Selbstbestimmung beschränkt sich dabei nicht alleine auf die Voraussetzungen der Datenverarbeitung, sondern sie ist – wie insbesondere auch in der Online-Kommunikation zu beobachten ist - auch Grundlage für die kommunikative Entfaltung der Bürgerinnen und Bürger. Auf eine Formel gebracht: Datenschutz ist die Voraussetzung für **kommunikative Kompetenz**, ohne die eine moderne Wissens- und Informationsgesellschaft nicht funktionieren kann.
2. Ein deutlicher Zusammenhang besteht zwischen dem Datenschutz und dem Verbraucherschutz: In beiden Fällen geht es um den Schutz der wirtschaftlichen Handlungsfreiheit der Verbraucherinnen und Verbraucher, die durch eine Verarbeitung und Nutzung ihrer Daten beeinträchtigt werden kann. Im Begriff des **Verbraucherdatenschutzrechts** werden diese beiden Aspekte zusammengeführt: Die wirtschaftliche Handlungsfähigkeit der strukturell unterlegenen Verbraucherinnen und Verbraucher muss auch durch einen wirksamen Datenschutz gewährleistet werden. Das ULD hat hierzu eine umfassende Studie im Auftrag des Bundesministeriums für Landwirtschaft, Ernährung und Verbraucherschutz vorgelegt.
3. Die Gewährleistung des Datenschutzes ist ein **unverzichtbarer Akzeptanzfaktor** für die Entwicklung der Informations- und Wissensgesellschaft. Das Vertrauen der Menschen in wirksame Schutzmechanismen im Bereich von Datenschutz und Datensicherheit ist ein tragendes Element für die Entwicklung einer modernen Informations- und Wissensgesellschaft. Ein erhebliches Risikopotenzial für dieses Vertrauen stellen heimliche Erhebungen und Auswertungen personenbezogener Daten dar (bspw. durch Systeme des Data Mining, Customer Relation Ship Management, Ubiquitären Computing, Scoringsysteme etc.). Ein weiteres Risiko für das Vertrauen der Betroffenen ist die explosionsartige Vermehrung an gezielter personalisierter Werbung sowie die Aushebelung der Grundsätze der Datensparsamkeit und Datenvermeidung bspw. durch die Verpflichtung zur Vorratsdatenspeicherung. Signifikant für das Bedrohungspotenzial ist das Beispiel der Online-Durchsuchungen („Bundestrojaner“): Die Legalisierung von Strategien, mit denen der Staat heimlich an sich notwendige technische Schutzmechanismen der Datensicherheit unterläuft, wird zu einem gravierenden Vertrauensverlust in die Sicherheit von Online-Techniken wie bspw. Online-Banking und E-Commerce führen.
4. Der Gesetzgeber steht aufgrund seiner **verfassungsrechtlichen Schutzpflicht** für das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger in der Verantwortung, für eine wirksame und leistungsfähige Schutzkonzeption zu sorgen. Das derzeitige Schutzkonzept wird den Herausforderungen nicht im erforderlichen Umfang gerecht. Die Daten der Betroffenen werden zunehmend ohne ihre Kenntnis und ohne eine ausreichende Rechtsgrundlage verarbeitet.

Im Folgenden beantworte ich die zur Anhörung gestellten Fragen im Zusammenhang mit **vier Säulen** einer modernen Datenschutzkonzeption. Im Übrigen verweise ich auf die Stellungnahmen meiner Kollegen des Bundes, aus Berlin sowie aus Mecklenburg-Vorpommern.

5. **Datenschutz durch Recht**: Das informationelle Selbstbestimmungsrecht ist ein Grundrecht, dessen Schutz und Grenzen der Gesetzgeber durch Regeln zur Datenverarbeitung zu regeln hat. Der durch Rechtsbestimmungen gewährleistete Datenschutz mit seinen Prinzipien der Rechtmäßigkeit, der Zweckbindung, der Erforderlichkeit und der Transparenz sind das zentrale Fundament des Datenschutzes. Das Datenschutzrecht kann aber nur Schutzwirkungen entfalten, wenn seine Regeln klar und präzise sind. Entsprechendes gilt für die für die Datenverarbeitung verantwortlichen Stellen: Sie benötigen vor allem Rechtsklarheit über die Anforderungen des Datenschutzes.

   a) Das geltende Datenschutzrecht ist zu **unübersichtlich**, wie insbesondere an den Datenschutzregeln für Telekommunikation, Telemedien und BDSG zeigen, die ein Anbieter im Internet zu beachten hat. Ein anderes Beispiel ist § 28 BDSG als zentrale Regelung der Datenverarbeitung im Bereich der Wirtschaft, der mit seinen zahlreichen Ausnahmetatbeständen einen Komplexitätsgrad erreicht hat, der jeden Verantwortlichen in die Verzweiflung treiben muss. Ein weiteres Beispiel sind die unzähligen und zudem versteckten Ausnahmetatbestände, die der Gesetzgeber zum Auskunftsrecht des Betroffenen vorgesehen hat(§ 34 Abs. 4 i.V.m. § 33 Abs. 2 BDSG). Eine Modernisierung des Datenschutzes muss mit einer Vereinfachung und Vereinheitlichung des Datenschutzrechts beginnen. Vorschläge hierzu liegen seit Jahren vor.

   b) Das geltende Datenschutzrecht weist **Schutzlücken** auf wie sich insbesondere an den unzureichenden Regelungen für den Datenschutz bei Auskunfteien zeigt (§ 29 BDSG). Ebenso wie der Vertragsschluss eine ausdrückliche Handlung voraussetzt, sollte das Prinzip der *ausdrücklichen Einwilligung* auch im Datenschutzrecht gelten. Das Datenschutzrecht muss der Zunahme an verdeckten Datenerhebungen durch neue Technologien wie bspw. der Verwendung von **Scoringsystemen** wirksam Grenzen setzen. Ein weiteres Defizit sind die fehlenden Regelungen für den Bereich des *Arbeitnehmerdatenschutzes*, den der Gesetzgeber zu regeln sich seit Jahrzehnten nicht in der Lage sieht.

   c) Das geltende Datenschutzrecht muss **effektiv um- und durchgesetzt** werden. Hierzu bedarf es einer flankierenden Stärkung der betrieblichen Selbstverantwortung für eine Rechtmäßigkeit der Datenverarbeitung insbesondere durch einen besseren Schutz der betrieblichen Datenschutzbeauftragten. Erforderlich sind aber auch schlagkräftige und vor allem unabhängige Aufsichtsbehörden, die über ausreichende personelle und technische Ressourcen verfügen. Die unzulässigen Praxen bei Scoringsystemen sind nicht nur auf unklare oder unpräzise Regelungen im Datenschutzgesetz zurückzuführen, sondern vor allem auch ein Problem des Vollzugsdefizits strukturell überlasteter Aufsichtsbehörden.

6. Ein moderner Datenschutz muss präventiv wirken. Hierzu bedarf es der Entwicklung und Förderung eines **Datenschutzes durch Technik.** Mit den Grundsätzen der Datensparsamkeit und Datenvermeidung in § 3 a BDSG hat der Gesetzgeber sich diesen Ansatz zu eigen gemacht: Datenschutz durch Technik bedarf aber auch der gezielten Förderung und Unterstützung, indem Datenschutz und Datensicherheit zu einem integralen Bestandteil einer gezielten staatlichen Förderung von neuen Technologien und Anwendungen werden.

   a) Das ULD hat sich im Rahmen seiner Möglichkeiten bspw. im Auftrag des BMBF an einer Technikfolgenabschätzungsstudie zum Ubiquitären Computing beteiligt und arbeitet unterstützt von der Europäischen Kommission in europäischen Projekten an Konzepten für ein vom Benutzer gesteuertes Identitätsmananagement mit. Im Rahmen eines e-Region Programmes unterstützt das ULD bspw. die Entwicklung eines Spam-Filters für Voice over IP. Die Entwicklung und Be-

reitstellung datensparsamer Technologien (Privacy Enhanced Technologies) bedarf aber einer flankierenden Unterstützung insbesondere durch die Zertifizierung datenschutzfreundlicher Produkte und Verfahren.

b) Regulatorischer Unterstützung bedürfen technisch-organisatorische **Konzepte der Pseudonymisierung**, mit denen zahlreiche Verarbeitungen datenschutzfreundlich gestaltet werden könnten, wenn bspw. die Verantwortlichkeiten, die Zweckbindung der Zuordnungstabellen von Pseudonymen und Identitätsdaten und die Verwendungszwecke gesetzlich abgesichert werden würden.

7. Ein modernes Element des Datenschutzes ist es, die Investitionen in den Datenschutz durch unabhängige Dritte zu zertifizieren, damit sie von den Anbietern gegenüber den Betroffenen kommuniziert und als Wettbewerbsvorteil genutzt werden können. Der Gesetzgeber hat mit § 9 a BDSG einen wichtigen Baustein für einen **Datenschutz als Wettbewerbsvorteil** gelegt, ist aber mit dem Verzicht auf das in dieser Regelung angekündigte Ausführungsgesetz auf der halben Wegstrecke stehen geblieben. Gleichwohl gibt es bereits umfassende Praxiserfahrungen mit der Auditierung von Produkten und Verfahren in Schleswig-Holstein, die die bisherigen Einwände und Zweifel an der Wirksamkeit und Tauglichkeit dieses Konzeptes widerlegen.

   a) In Schleswig-Holstein zertifiziert das ULD aufgrund einer landesrechtlichen Ermächtigung **datenschutzfreundliche Produkte**, die in der Landesverwaltung eingesetzt werden können. Das **Gütesiegel**-Verfahren ist zweistufig: Sach- und fachkundige Gutachter, die über eine entsprechende Zulassung verfügen, begutachten das Produkt auf der Basis eines Privatrechtsverhältnisses mit dem Hersteller oder Anbieter. Eine vergleichbare Struktur hat das Verfahren der Produktzertifizierung des Bundesamtes für die Sicherheit der Informationstechnik (BSI). Das Gutachten wird der Zertifizierungsstelle im ULD vorgelegt und nach einer erfolgreichen Prüfung, ggf. der Klärung von Rückfragen oder Nachbesserungen durch Verleihung des Datenschutz-Gütesiegels zertifiziert. Das ULD hat auf dieser Basis seit 2003 über 35 Gütesiegel an unterschiedliche Produkte vornehmlich mittelständischer Unternehmen aus Deutschland verliehen. Am 16.02.2007 konnte das erste Gütesiegel an einen ausländischen Hersteller verliehen werden. Es handelt sich um das Produkt Windows Update Server der Firma Microsoft, USA.

   b) Mit dem erfolgreichen Abschluss des Gütesiegel-Verfahrens für ein Produkt der Firma Microsoft hat das Gütesiegel-Konzept aus Schleswig-Holstein mittlerweile eine **internationale Ausstrahlungswirkung**. Ausschlaggebend für die Entscheidung von Microsoft für das Zertifizierungsverfahren war der deutsche Standard des Datenschutzes und die Zertifizierung durch das ULD als einer unabhängigen staatlichen Stelle.

   c) Das ULD auditiert darüber hinaus Verfahren der Datenverarbeitung der Behörden in Schleswig-Holstein auf freiwilliger Basis gegen Kostenerstattung (**Datenschutz-Audit**). Mittlerweile hat das ULD über 15 Auditverfahren im Auftrag von Kommunen, Landkreisen, des Landtages sowie der Landesregierung erfolgreich abgeschlossen. Auditiert worden ist bspw. die gesamte Landesnetz-Infrastruktur oder das System der Zutrittsberechtigung im Landtag Schleswig-Holstein. Weitere Auditierungsverfahren sind in der Bearbeitung.

   d) Angesichts der Erfahrungen in Schleswig-Holstein geht es nicht mehr um die Frage, ob eine Zertifizierung auf freiwilliger Basis sinnvoll ist oder nicht, sondern ausschließlich um die Sicherung eines Standortfaktors **„Privacy - made in Germany“** im Europäischen Wettbewerb. Bereits 2004 hatte die Europäische Kommission Schleswig-Holstein einen Europäischen Innovations-

preis für das Konzept verliehen. Noch in diesem Jahr wird das ULD zusammen mit anderen europäischen Partnern im Auftrag der EU-Kommission im Rahmen eines Projektes die Arbeiten an einer Europäisierung des Datenschutz-Gütesiegels aufnehmen. Um die internationale Anerkennung seiner Zertifizierung zu gewährleisten, orientiert sich das ULD zudem in seiner Aufbau- und Ablauforganisation an internationalen Standards, insbesondere der ISO 27001.

e) Eine **Bundesregelung** ist sinnvoll, um die Zulassung der Gutachter zu regeln, den Anwendungsbereich des Gütesiegels erweitern sowie die Auditierung von Verfahren der Datenverarbeitung in der Wirtschaft zu ermöglichen. Dem ULD liegen bereits eine Reihe von Anfragen nach einem Datenschutzaudit vor, die aufgrund der beschränkten Rechtslage in Schleswig-Holstein nicht erfüllt werden können.

8. Der vierte Baustein eines modernen Datenschutzes ist, den Datenschutz durch ein **Prozessmanagement** in den datenverarbeitenden Stellen zu gewährleisten. Der Vorschlag einer **Informationspflicht bei Datenschutzpannen** ist ein Element dieser Datenschutz-Policy. Bereits heute sehen internationale Management-Standards bei Sicherheitsvorfällen in Abhängigkeit von ihrer Bedeutung Informationspflichten vor, damit die Verantwortlichen entsprechende Sofort-Maßnahmen einleiten, aber auch um Schlussfolgerungen für die Zukunft ziehen zu können. Verantwortlich für seine Daten ist der Betroffene als Träger des informationellen Selbstbestimmungsrechts. Es ist also nur konsequent, wenn der Betroffene über Pannen bei der Verarbeitung seiner Daten von der verantwortlichen Stelle unterrichtet wird, damit er bspw. seinen Dienstleistungsanbieter wechseln kann. Gleichzeitig würde eine solche Regelung auch den Wettbewerb um datenschutzkonforme Produkte und Verfahren stärken. Eine entsprechende gesetzliche Regelung sollte gleichzeitig vorsehen, dass die zuständige Aufsichtsbehörde unterrichtet wird, damit der Betroffene bei der Bewertung der Datenschutzpanne sachkundig unterstützt werden kann.

Dr. Johann Bizer

Stellvertretender Landesbeauftragter für den Datenschutz

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Anhang: Kreditscoring

Thesen des Landesbeauftragten für den Datenschutz, Schleswig-Holstein,
Dr. Thilo Weichert vom 27. Juni 2006

1. Als Rechtsgrundlage für das Kredit-Scoring kommt sowohl die Betroffeneneinwilligung (§ 4 a BDSG) wie auch ein Vertrag/vertragsähnliches Verhältnis mit dem Kreditantragsteller (§ 28 Abs. 1 S. 1 Nr. 1 BDSG) in Betracht. Eine Berufung auf ein berechtigtes Interesse des Kreditunternehmens, das den schützwürdigen Betroffeneninteressen überwiegt (§ 28 Abs. 1 S. 1 Nr. 2 BDSG), ist nicht möglich.

2. Externe Scoring-Unternehmen können ihre Datenverarbeitung mit § 29 BDSG begründen. Über die erste Übermittlung ist der Betroffene zu benachrichtigen (§ 33 Abs. 1 S. 2 BDSG). Grundlage für die Anfrage durch ein Kreditinstitut muss eine Einwilligung oder ein Vertrag/vertragsähnliches Verhältnis sein.

3. Im Rahmen der schriftlichen Legitimation ist die betroffene Person zu unterrichten: über den Zweck (Prognose des Kreditrisikos), Art der Datenverarbeitung (Scoring), in generalisierter Form die einfließenden Daten (Antragsdaten, Unternehmensdaten aus ..., soziodemografische Daten), Art der Nutzung (Vertragsschluss, Risikopricing) und beteiligte Stellen. Informationen sollen erfolgen auf die Folgen einer Verweigerung und einer Rücknahme der Zustimmung.

4. Die Rechtmäßigkeit der Scoreberechnung setzt voraus:

   a) die nach einem anerkannten Verfahren festgestellte wissenschaftlich-statistische Relevanz und Gewichtung der einbezogenen Daten,

   b) die Plausibilität der Daten für die Beurteilung der Kreditwürdigkeit und

   c) den Ausschluss von Merkmalen, die einem Nutzungs- oder Diskriminierungsverbot unterliegen.

5. Die wissenschaftlich-statistische Methode soll regelmäßig einer Qualitätskontrolle unterzogen werden, wofür eine Dokumentation des Verfahrens und eine Protokollierung der individuellen Scoregenese und -nutzung erforderlich ist.

6. Die Nutzung von gesperrten Daten sowie von sensitiven Daten nach § 3 Abs. 9 BDSG ist nur mit ausdrücklicher Einwilligung zulässig. Unzulässig ist die Nutzung von Daten über die Wahrnehmung von unabdingbaren Rechten und von einem Diskriminierungsverbot unterliegenden Daten (Alter, Geschlecht, Rasse, sexuelle Orientierung, Behinderung, Religion, Weltanschauung).

7. Das Verbot automatisierter Entscheidungen (§ 6a BDSG) ist umfassend auf Kredit-Scoring anwendbar. Der Betroffene ist über eine möglicherweise negative Entscheidung zu informieren und ihm ist die effektive Möglichkeit zu geben, seine berechtigten Interessen einzubringen.

8. Eine kostenfreie Auskunft nach § 34 BDSG ist zu erteilen über den berechenbaren Score und für die Dauer von 1 Jahr über den beauskunfteten oder genutzten Score. Im Rahmen des § 6 a Abs. 3 BDSG ist Auskunft zu erteilen über die wichtigsten 4 Merkmale in der Reihenfolge ihrer Bedeutung.

9. Korrekturansprüche nach § 35 BDSG bestehen nicht, wenn die durch den Score zum Ausdruck gebrachte Prognose fehlerhaft ist, weil sie bestimmte Merkmale nicht berücksichtigt. Korrekturansprüche bestehen bei einer unzulässigen oder falschen Datenbasis und falschen Berechnungen.

10. Der Widerspruch des Betroffenen führt zur Unzulässigkeit des Kredit-Scoring, wenn keine vertragliche Regelung nach § 28 Abs. 1 S. 1 Nr. 1 BDSG besteht.

11. Im Interesse des Verbraucher- und Datenschutzes bedarf es beim Kredit-Scoring keiner wesentlichen gesetzlichen Änderungen. Wünschenswert wäre eine Verbesserung bzw. Klärung der Aus-

kunftsansprüche sowie die Aufnahme eines Bußgeldtatbestandes für den Fall der Auskunftsverweigerung gegenüber dem Betroffenen.

12. Zum Abbau des vorhandenen Vollzugsdefizits der Datenschutznormen beim Kredit-Scoring bedarf es einer besseren personellen und technischen Ausstattung von unabhängig organisierten Datenschutzaufsichtsbehörden.

13. Durch Verhaltensrichtlinien nach § 38a BDSG, die Auditierung von Scoring-Verfahren nach § 9a BDSG, die Veröffentlichung der Kriterien und Verfahren und die Entwicklung von Best-Practice-Kriterien kann die Kreditwirtschaft das verloren gegangene Vertrauen der Verbraucher beim Kredit-Scoring wiedergewinnen.

Quelle: https://www.datenschutzzentrum.de/vortraege/060627_weichert-scoring.htm