



Gisela Piltz
Mitglied des Deutschen Bundestages

Eckpunktepapier

Errichtung einer **Stiftung Datenschutz**

Seitdem vor 40 Jahren zuerst in einigen Bundesländern, dann durch den Bund selbst Datenschutzgesetze auf den Weg gebracht wurden, haben sich die Rahmenbedingungen für den Datenschutz elementar verändert. Der voranschreitende technologische Fortschritt führt zu einer sich stetig verändernden Nachfrage nach datenschutzrechtlichen Regeln und unterwirft das Recht der Datenverarbeitung einem fortwährenden Wandel. Moderner Datenschutz muss genau diesen Wandel im Blick haben.

Indes entfalten gesetzliche Vorgaben dort, wo personenbezogene Daten die Grenzen einzelner Staaten und damit die Grenzen nationaler Rechtsordnungen überschreiten, nur noch sehr eingeschränkt Wirkung. Die Bestimmung von Ort und Zeit der Datenverarbeitung verliert angesichts lediglich national wirkender Rechtsordnungen nicht nur an Bedeutung, sondern wird durch grenzüberschreitenden Datenverkehr, durch Datenverarbeitung in der „cloud“ und durch mangelnde technische Netzsicherheit zusehends schlicht unmöglich. Auch wenn dies keine Entschuldigung für nationalen gesetzgeberischen Stillstand sein kann, bedarf es im Zeitalter digitaler Datenverarbeitung und Datenübermittlung daneben grundlegend neuer Ansätze zum Schutz personenbezogener Daten. Datenschutz ist und bleibt eine gesamtgesellschaftliche Aufgabe. Staat, Unternehmen und der Bürger selbst sind angehalten, ihren Teil zur Datenschutzkultur des 21. Jahrhunderts beizutragen. Um allen beteiligten Akteuren eine Koordinierungsinstanz an die Seite zu stellen, haben Union und FDP im Koalitionsvertrag die Errichtung einer Stiftung Datenschutz vereinbart, mit dem Ziel, eine bestmögliche Synergie von privater und hoheitlicher Betätigung im Bereich Datenschutz zu erreichen.

Grundprinzipien

- ✓ Der Bund errichtet die Stiftung Datenschutz als **rechtsfähige Stiftung des bürgerlichen Rechts** und gibt ihr eine Satzung, sofern nicht aufgrund der Aufgabenbeschreibung die Errichtung einer öffentlich-rechtlichen Stiftung angezeigt ist. Grundlage für die Errichtung ist Artikel 87 Absatz 3 des Grundgesetzes.
- ✓ Die **Organe der Stiftung** werden paritätisch mit Vertretern aus den Bereichen Datenschutz, Wirtschaft, Verbraucherschutz und der Netzgemeinschaft besetzt. Um eine möglichst effektive Verzahnung mit Gesetzgebung und Politik zu erreichen, werden Vertreter aus Regierung und Parlament in einen zu errichtenden Beirat entsandt. Bei der Kompetenzverteilung zwischen den einzelnen Organen der Stiftung wird eine klare Trennung von beratenden, geschäftsführenden und entscheidenden Stellen angestrebt.
- ✓ Um frei von jeglicher äußeren Einflussnahme agieren zu können, bedarf die Stiftung Datenschutz einer angemessenen **personellen und finanziellen Ausstattung**. Die Finanzierung baut dabei auf einem Mehr-Säulen-Modell auf, welches sich aus dem



Gisela Piltz

Mitglied des Deutschen Bundestages

Stiftungskapital, öffentlichen Mitteln (Festbetrag als Zuweisung), Zuwendungen privater Unternehmen und Kapitalrenditen zusammensetzt. Durch die Vergabe kostenpflichtiger Zertifizierungen sind mittelfristig spürbare Zusatzerlöse zu erwarten. Eine gesetzliche Regelung, wonach künftig die Stiftung Datenschutz vornehmlich Begünstigter bei Bußgeldzahlungen nach dem BDSG sein soll, kann weitere Liquidität sichern und verstärkt darüber hinaus die marktberreinigende Funktion der Stiftung.

- ✓ Die Aufgabenbeschreibung der Stiftung Datenschutz setzt sich aus **vier Säulen** zusammen.

Säule 1 – Vergabe von Audits und Gütesiegeln

Im Zuge der Novellierung des Bundesdatenschutzgesetzes im Jahr 2001 fand neben weiteren Neuerungen § 9a Einzug in das BDSG. Nach dieser Regelung können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen zur Verbesserung des Datenschutzes und der Datensicherheit ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und akkreditierte Gutachter prüfen und bewerten lassen. In Ermangelung des in **§ 9a BDSG** verlangten „besonderen Gesetzes“ zur Regelung der näheren Anforderungen an die Durchführung der Prüfverfahren sowie die Auswahl der Gutachter läuft die Vorschrift auch im zehnten Jahr nach ihrer Verabschiedung ins Leere. Statt dessen drängen im Fahrwasser der Datenskandale der jüngeren Vergangenheit zusehends private Anbieter diverser Zertifizierungen auf den Markt.

Verbraucher, Unternehmen und Aufsichtsbehörden müssen sich jedoch auf **ein einheitliches und deutschlandweit anerkanntes Zertifizierungsinstrument** verlassen können. Eine Vielzahl unterschiedlicher Zertifizierungsmodelle bietet den Beteiligten aufgrund der unterschiedlichen Prüftiefe und der fehlenden Vergleichbarkeit der Ergebnisse keinen Mehrwert. Die Stiftung Datenschutz wird diesen Mangel angehen und als insoweit einzige Institution bundesweit allgemein anerkannte Datenschutzaudits und Datenschutzgütesiegel verleihen.

Der Zertifizierung vorgelagert entwickelt die Stiftung Datenschutz in einem ersten Schritt Konzepte und Strategien zur effektiven und unbürokratischen Durchführung solcher Zertifizierungsverfahren. Der besondere Fokus dieses **think tanks** wird sich dabei auf organisatorische Fragestellungen sowie die Entwicklung valider Zertifizierungsparameter richten. Hierbei kann auf die Erfahrungen einzelner Datenschutzbehörden der Länder zurückgegriffen werden. Die mit dieser Aufgabe befassten Gremien der Stiftung Datenschutz orientieren sich dabei an nachfolgenden Leitlinien:

- ✓ Die Stiftung Datenschutz verleiht **Gütesiegel** für Produkte und Verfahren und vergibt **Audits** für ganze Datenschutzkonzepte.
- ✓ Das eigentliche Prüfverfahren erfolgt durch bei der Stiftung **akkreditierte Sachverständige**. Bundesweit einheitliche und transparente Regelungen zur Bestellung von Sachverständigen werden geschaffen.



Gisela Piltz

Mitglied des Deutschen Bundestages

- ✓ Antragsteller können **europaweit** sowohl **private Unternehmen** als auch solche **öffentliche Stellen** sein, die am Wettbewerb teilnehmen.
- ✓ Einer Prüfung unterzogen werden können **Online- und Offlineprodukte**.
- ✓ Der **Umfang der Zertifizierung** ist festzulegen. Es muss die Entscheidung getroffen werden, ob neben einzelnen Dienstleistungen und Produkten ganze Unternehmen zertifiziert werden sollen. Da für potentielle Auftraggeber (insbesondere im Bereich der Auftragsdatenverarbeitung) letztlich die Vertrauenswürdigkeit der angewandten Verfahren im Mittelpunkt stehen wird, erscheint die Zertifizierung eines gesamten Unternehmens nicht angezeigt. Soll vor dem Hintergrund der Datenskandale um den Missbrauch von Arbeitnehmerdaten die Auditierung auch die datenschutzgerechte Handhabung von Arbeitnehmerdaten erfassen, erscheint die Zertifizierung des gesamten Unternehmens denkbar.
- ✓ Die Zertifizierung erfolgt nicht bereits über den Nachweis der Einhaltung der gesetzlichen Vorschriften. **Honoriert werden sollte nur ein „Mehr“**. Um Benachteiligungen solcher Unternehmen zu verhindern, die lediglich den Nachweis der Einhaltung geltenden Rechts führen wollen, ist eine Zwei-Stufen-Lösung („Gold“ und „Platin“) denkbar. Eine Negativaussage im Sinne einer Abstufung wird hierdurch nicht begründet.
- ✓ Die Entscheidung zur Teilnahme von Zertifizierungsmaßnahmen erfolgt ausschließlich **auf freiwilliger Basis**. Der Prüfungsgegenstand wird durch den Antragsteller bestimmt. Die Stiftung Datenschutz überwacht die hinreichende Nachvollziehbarkeit und Bestimmbarkeit des Prüfungsgegenstandes.
- ✓ Gütesiegel und Audits werden **auf zwei Jahre befristet** verliehen. Die Einhaltung der Voraussetzungen wird stichprobenartig überprüft. Für den Fall der Auffrischung einer bereits erfolgten Zertifizierung sowie für den Bereich Veränderungsmanagement werden Verfahrensvereinfachungen vorgesehen.
- ✓ Die **Parameter des Audits** sind für Verbraucher, Unternehmen und Aufsichtsbehörden gleichermaßen transparent und nachvollziehbar auszugestalten.
- ✓ Die Arbeit des **betrieblichen Datenschutzbeauftragten** kann nicht Prüfungsgegenstand sein. Der betriebliche Datenschutzbeauftragte ist in den Zertifizierungsprozess hinreichend einzubeziehen.
- ✓ Die Stiftung entwirft ein für den Verbraucher verständliches und **visuell eindeutig zu identifizierendes** Auditzeichen/Gütesiegel.
- ✓ Zertifizierungen werden auf Anfrage der Unternehmen erteilt. Sie entfalten gegenüber **Aufsichtsbehörden** nach geltendem Recht keine bindenden Rechtswirkungen und treten grundsätzlich neben die Kontrollinstrumente der Aufsichtsbehörden. Das erfolgreiche Durchlaufen eines Zertifizierungsprozesses kann die aufsichtsbehördliche Prüfung nicht ersetzen. Um gleichwohl gerade auch für Aufsichtsbehörden größtmögliche Synergien zu



Gisela Piltz

Mitglied des Deutschen Bundestages

erreichen, wird die fehlende Rechtswirkung durch Formulierung von in Art und Umfang genau bestimmter Prüfungsgegenstände und –kriterien ersetzt. Zertifizierungen der Stiftung Datenschutz erleichtern den Aufsichtsbehörden auf diese Weise die Vor-Ort- und Einzelfallprüfungen erheblich. Denkbar ist demnach eine vereinfachte aufsichtsbehördliche Prüfung solcher Verfahren, die eine gültige Zertifizierung vorweisen können. Zur Bestimmung belastbarer und praxistauglicher Zertifizierungsparameter werden die Aufsichtsbehörden von Bund und Ländern frühzeitig intensiv in die Entwicklungsprozesse einbezogen.

- ✓ Das Audit/Gütesiegel entfaltet eine deutliche Publizitätswirkung und ist damit für **Unternehmen** ökonomisch sinnvoll. Der Zweckbestimmung von § 9a BDSG entsprechend können erteilte Zertifikate zu Werbezwecken genutzt werden. Regelungen für Unternehmen, die von der Möglichkeit, Zertifizierungen durchzuführen, keinen Gebrauch machen, sind festzulegen. Einem drohenden rechtlicher Zwang zur Teilnahme an Zertifizierungsmaßnahmen ist vorzubeugen.
- ✓ Das **Auditregister** wird durch die Stiftung Datenschutz geführt.
- ✓ Für den Fall unberechtigter Siegelführung sind empfindliche **Bußgeldtatbestände und Strafvorschriften** zu etablieren.
- ✓ Bestrebungen auf **europäischer Ebene** zur Entwicklung eines Audits mit europaweiter Gültigkeit stehen Initiativen einzelner Mitgliedstaaten nicht im Wege. Die Stiftung Datenschutz entfaltet als in dieser Form einzigartige Institution in Europa Ausstrahlungswirkung. Sie trägt durch „**privacy - made in germany**“ zur Rechtsfortbildung in den europäischen Mitgliedsstaaten und zur weiteren Harmonisierung des Datenschutzniveaus im europäischen Raum bei.

Säule 2 – Vergleichende Tests von Produkten und Verfahren

Vergleichende Tests von Produkten und Dienstleistungen haben in Deutschland spätestens seit Gründung der Stiftung Warentest im Jahr 1964 gute und erfolgreiche Tradition. Im Rahmen dieser Tests steht in den ganz überwiegenden Fällen die Leistungs- und Gebrauchsfähigkeit der Testobjekte im Vordergrund. Datenschutzrechtliche Aspekte werden, wenn überhaupt, nur am Rande untersucht und bewertet, obwohl der Verbraucher zusehends gerade in diesem Bereich Aufklärung erwartet.

Neben der Funktion als Zertifizierungsstelle wird die Stiftung Datenschutzes genau an diesem Punkt ansetzen und Produkttests gerade und ausschließlich **unter datenschutzrelevanten Aspekten** durchführen. Richtig ist, dass Produkte mehr als Daten sind. Richtig ist auch, dass datenschutzkritische Produkte oft durch hohe datenschutz- und urheberrechtliche Komplexität gekennzeichnet sind. Um gleichwohl Transparenz auch über Produkte und Verfahren solcher Unternehmen herzustellen, die sich einer freiwilligen Zertifizierung nicht unterwerfen, etabliert die Stiftung Datenschutz den „Datentest“ nach folgenden Maßgaben:



Gisela Piltz

Mitglied des Deutschen Bundestages

- ✓ Bei der Auswahl der Testobjekte bezieht die Stiftung Datenschutz allein bereits **am Markt befindliche Produkte** und Dienstleistungen ein.
- ✓ Die **Durchführung der Tests** erfolgt durch bei der Stiftung Datenschutz akkreditierte Sachverständige.
- ✓ Untersucht werden **Online- und Offlineprodukte** aus einem vorbestimmten Marktsegment.
- ✓ Untersucht werden können **sowohl private Unternehmen als auch öffentliche Stellen** des Bundes. Soweit sich die Untersuchung öffentlicher Stellen der Länder nicht als unzulässige Mischverwaltung darstellt, können auch solche Stellen in die Testreihen einbezogen werden.
- ✓ Jeder Testreihe wird ein an den datenschutzrechtlichen Anforderungen und dem tatsächlichen Anwendungsszenario orientierter **Prüfkatalog** zugrunde gelegt, der den Umfang der Prüfkriterien und Penetrationstests beschreibt. Es werden nur solche Aspekte einer Bewertung unterzogen, die für den Verbraucher tatsächlich von Relevanz sind. Denkbare Kriterien sind z.B. die Menge der erhobenen Daten und die Art der Speicherung, Zugriffs- und Auskunftsrechte, Bewertung der Bearbeitungsdauer von Auskunftersuchen, Umfang von Verfahrensübersichten, Lesbarkeit der Datenschutzerklärung, usw.
- ✓ Die Wahrung von **Geschäfts- und Betriebsgeheimnissen** muss angemessen Berücksichtigung finden.
- ✓ Die **Ergebnisse der Tests** werden durch die Stiftung Datenschutz der Bevölkerung in geeigneter Weise zur Verfügung gestellt.
- ✓ Für den Fall **mangelnder Kooperationsbereitschaft der Hersteller** bedarf es der Entwicklung geeigneter Instrumente zur Negativbewertung. Dabei kann es nicht Anspruch der Testprotokolle sein, mangelnde Transparenz allein mit „0 Punkten“ zu bewerten.
- ✓ Die Stiftung Datenschutz anerkennt den auch im internationalen Kontext herausragenden Stellenwert der **Stiftung Warentest** und arbeitet mit dieser vertrauensvoll zusammen. Die Auswahl der Testobjekte erfolgt in enger Abstimmung mit der Stiftung Warentest. Doppelprüfungen unter denselben Bewertungskriterien sind zu vermeiden.

Säule 3 – Bereitstellen von Bildungsangeboten im Bereich Datenschutz

Datenschutz ist eine Bildungsaufgabe. **Mangelnder Selbstdatenschutz** ist nicht selten Ausdruck mangelnder Kenntnisse und einer fehlenden oder nur unzureichenden Sensibilisierung des Betroffenen. Die Förderung datenschutzrechtlicher Kompetenz erfolgt bislang lediglich punktuell oder projektbezogen und vermag die steigende Nachfrage nach Bildungsangeboten in diesem Bereich nicht zu befriedigen. Doch wo Vorgaben des Gesetzgebers im Internet allenfalls eingeschränkte Wirkung entfalten, wo eine Reglementierung des virtuellen



Gisela Piltz

Mitglied des Deutschen Bundestages

Raumes weder faktisch möglich noch gesellschaftspolitisch wünschenswert ist, rückt der Ursprung des Datenflusses, der Betroffene, unweigerlich in den Mittelpunkt der Betrachtung. Für im Internet zugängliche und damit in der Regel öffentlich vorgehaltene Daten gibt es keinen Kopierschutz. In einer digitalisierten Welt und den sich hierdurch stetig neu eröffnenden Möglichkeiten kann damit ein grundlegendes Mehr an Datenschutz nur durch den Betroffenen selbst erreicht werden.

Nicht nur Schüler und Jugendliche, sondern auch Lehrer und Eltern sind in der Pflicht: Häufig sind gerade Erziehungsberechtigte im Umgang mit neuen Medien nachlässig und überfordert. Bildungsangebote müssen deshalb **für alle Altersstufen** entwickelt und angeboten werden. Erst wenn jeder einzelne Bürger tatsächlich in die Lage versetzt ist, die datenschutzrechtlichen (Neben-)Wirkungen des eigenen Tuns zu erkennen und zu verstehen, ist ein selbstbestimmter und verantwortungsbewusster Umgang mit den eigenen persönlichen Daten gewährleistet. Im Rahmen der dritten Säule macht sich die Stiftung Datenschutz deshalb die Vermittlung von Kompetenz in datenschutzrechtlichen Problemstellungen sowie ein breites Werben für einen verantwortungsvollen Umgang mit den eigenen persönlichen Daten nach Maßgabe der nachfolgenden Erwägungen zur Aufgabe.

- ✓ Die Stiftung Datenschutz entwickelt **Strategien zur Sensibilisierung** der Bürgerinnen und Bürger beim Umgang mit den eigenen persönlichen Daten. Im Fokus sind hierbei nicht nur datenschutzkritische Angebote im Internet, sondern sämtliche Formen moderner Kommunikation.
- ✓ Die Stiftung Datenschutz formuliert **Lernziele** und macht Vorschläge für die Bereitstellung didaktischer Lehrmodelle. Es gilt die Erkenntnis zu vermitteln, dass ein nachlässiger Umgang mit den eigenen persönlichen Daten im Ernstfall erhebliche (Rechts-)Folgen sowie wirtschaftliche und persönliche Nachteile nach sich ziehen kann.
- ✓ Durch **Schulungen** und die Entwicklung und Verbreitung von **Informationsmaterial und Broschüren** informiert die Stiftung Datenschutz über technische und organisatorische Maßnahmen für einen verbesserten Selbstdatenschutz.
- ✓ Die Stiftung Datenschutz informiert frühzeitig über neue **datenschutzkritische Entwicklungen** und formuliert Empfehlungen für einen datenschutzgerechten Umgang.
- ✓ Zur Realisierung dieser Vorgaben bedient sich die Stiftung Datenschutz **externen Sachverständigen** und nutzt Erfahrungen aus bereits bestehenden und bewährten Projekten, wie beispielsweise dem Projekt „Datenschutz geht zur Schule“ des Bundesverbandes der Datenschutzbeauftragten Deutschlands e.V. Eine Kooperation mit der Bundeszentrale für politische Bildung wird angestrebt.
- ✓ Der **föderalen Kompetenzordnung** im Bereich Bildung trägt die Stiftung Datenschutz Rechnung. Eine Zusammenarbeit mit der Kultusministerkonferenz sowie eine enge Kooperation mit der Arbeitsgruppe „Datenschutz und Bildung“ der Datenschutzbeauftragten von Bund und Ländern wird angestrebt.



Gisela Piltz

Mitglied des Deutschen Bundestages

Säule 4 – Forschung und Weiterentwicklung des Datenschutzrechts

Datenschutz muss mit der Zeit gehen. Statische datenschutzrechtliche Rahmenbedingungen verlieren jedoch angesichts eines **galoppierenden technologischen Fortschritts** weiter an Wirkung. Gesellschaftliches wie staatliches Handeln hat bei neuen datenschutzrechtlichen Anforderungen oft nur reaktiven Charakter und ist durch Punktualität und Passivität geprägt. Ein sich ständig veränderndes gesellschaftliches Anforderungsprofil an datenschutzrechtliche Rahmenbedingungen bedarf daher konsistenter Folgenabschätzungen und einer belastbaren Projektion denkbarer Szenarien. Die Stiftung Datenschutz begleitet künftig diese technischen und gesellschaftlichen Entwicklungen unter Zugrundelegung folgender Erwägungen:

- ✓ Die Stiftung Datenschutz **formuliert Forschungsziele** im Bereich Datenschutz und **vergibt Forschungsaufträge**. Denkbar sind dabei Forschungsfelder aus sämtlichen Teilbereichen von Informationstechnologie (z.B. Anonymisierungstechniken, biometrische Anwendungen, ubiquitous computing, Identitätsmanagement, Multimediaforensik), Soziologie, Rechtstheorie, Psychologie, Pädagogik, usw.
- ✓ Mittelfristig wird die **Vergabe von Stipendien** und die **Förderung von Lehrstühlen** angestrebt.
- ✓ Durch die **Ausrichtung von Wissenschaftswettbewerben** können Schüler und Jugendliche für die Lösung datenschutzrechtlicher Fragestellungen begeistert werden.
- ✓ In Wahrnehmung dieser Aufgaben arbeitet die Stiftung Datenschutz intensiv mit wissenschaftlichen **Instituten und Lehrstühlen** zusammen.

Berlin, Mai 2010