

Stellungnahme des SWICO in der Anhörung zum Vorschlag des BAJ für eine Verordnung über die Datenschutzzertifizierungen (VDSZ)

Vorbemerkung

Der Schweizerische Wirtschaftsverband der Informations-, Kommunikations- und Organisationstechnik SWICO als führender Branchenverband der im Bereich der Informations- und Kommunikationstechnologie tätigen schweizerischen Unternehmen hat den vom Vorsteher des Eidg. Justiz- und Polizeidepartements zur Stellungnahme vorgelegten Entwurf vom 1. Februar 2007 betreffend eine „Verordnung über die Datenschutzzertifizierungen“ (VDSZ) durch eine Arbeitsgruppe („SWICO Arbeitsgruppe VDSZ“) prüfen lassen, welcher folgende Mitglieder der von RA Dr. Peter Neuenschwander geleiteten juristischen Kommission des SWICO aktiv mitgewirkt haben: Christiane Ammann, Schindler Management Ltd.; RA Jacques Beglinger; Marcel Huber, Orange Communications; Beat Lehmann, Alcan Holdings Switzerland; Michael Widmer, SAP; Dr. Christoph Stocker, UBS; Dr. Bruno Wildhaber, forte advisors. Die vorliegende Stellungnahme ist das Ergebnis der innerhalb der erwähnten Arbeitsgruppe geführten Konsultationen.

A. Hinweise zur Gesetzgebungsgeschichte

1. Die Möglichkeit der Freistellung privater Datenbearbeiter von der Pflicht zur Registrierung bestimmter qualifizierender Datensammlungen durch Erwerb eines „Datenschutz-Qualitäts-zeichens“ war im **Vernehmlassungsentwurf** zur Revision des Datenschutzgesetzes vom August 2001 nicht vorgesehen, weil in jenem Entwurf die dem Privatrecht unterstehenden Datenbearbeiter von der Registrierung überhaupt ausgenommen werden sollten.

Die Aufhebung der Registrierungspflicht wurde richtigerweise mit der Verstärkung der Pflicht zur Information der betroffenen Personen durch den zusätzlichen Datenschutzgrundsatz von Art. 4 Abs. 4 Rev DSG sowie die Schaffung einer qualifizierten Informationspflicht bei der Beschaffung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen gemäss dem neuen Art. 7a Rev DSG in Erfüllung der vom Parlament überwiesenen Motionen zur Verstärkung der Transparenz im Datenschutz begründet.

Die Registrierungspflicht und deren Aufhebung, bzw. die Instrumente zur Freistellung von der Registrierungspflicht im Bereiche des Privatrechts, wurden daher - u.E. zu Recht - in einen engen funktionellen Zusammenhang mit der Schaffung von Transparenz der Datenbearbeitung für die betroffenen Personen gebracht.

2. In der **Vernehmlassung** wurde die Aufhebung der Pflicht zur Registrierung der von privaten Inhabern gehaltenen Datensammlungen als Gegenstück zu der mit dem Revisionsentwurf vorgeschlagenen Verstärkung der Transparenz überwiegend befürwortet.

Stellungnahme zum Erlass einer Verordnung über die Datenschutzzertifizierungen (VDSZ)

Jene Stimmen, welche sich für die Beibehaltung des Register für bestimmte, qualifizierte Datensammlungen im Bereich des Privatrechts ausgesprochen haben, wollten es bei der bisherigen einfachen, klaren und administrativ mit einem nicht übermässigen Aufwand verbundenen Regelung belassen: Registrierung von Datensammlungen mit besonders schützenswerten Personendaten oder Persönlichkeitsprofilen mit dem vom EDÖB zur Verfügung gestellten Formular, sofern für deren Nutzung keine gesetzliche Pflicht besteht und die betroffenen Personen darüber keine Kenntnis haben.

Mit andern Worten: Die Verschaffung ausreichender Kenntnis der betroffenen Personen hat unter dem bisher geltenden DSG die Pflicht zur Registrierung von Datensammlungen mit besonders schützenswerten Personendaten oder Persönlichkeitsprofilen aufgehoben. Nachdem im Vorentwurf zum Rev DSG die Pflicht zur Verschaffung der Kenntnis der betroffenen Personen über die betreffenden kritischen Datenbearbeitungen erheblich verstärkt werden sollte, konnte die Registrierungspflicht für private Inhaber von qualifizierenden Datensammlungen entweder überhaupt aufgehoben werden, oder die bisherige Anmeldepflicht konnte für jene Fälle unverändert beibehalten werden, wo die Kenntnis der betroffenen Personen über die sie betreffenden kritischen Bearbeitungen aus irgendwelchen Gründen nicht sichergestellt werden konnte.

In den im Mai 2002 publizierten Ergebnissen des Vernehmlassungsverfahrens wird an keiner einzigen Stelle die Forderung der Schaffung eines „Datenschutz-Qualitätszeichens“ bzw. eines Zertifizierungsverfahrens erwähnt. Unter Ziff. 3.2 S. 3 wird lediglich darauf hingewiesen, dass einzelnen Stellen ohne nähere Angaben bemängelt hätten, dass der Revisionsentwurf der technischen Entwicklung zu wenig Rechnung trage.

Dies ist übrigens ein Vorwurf, den man im Zusammenhang mit dem Datenschutz immer wieder hört und nach der hier vertretenen Auffassung eine elementare Verkenning des Datenschutzes darstellt: Es war das erklärte Ziel des Gesetzgebers von 1992, im Sinne einer Rahmengesetzgebung eine Grundlage für die Gewährleistung der Privatsphäre und des informationellen Selbstbestimmungsrechtes bei der automatisierten oder manuellen Bearbeitung von Personendaten zu schaffen, welche für die damals schon erkennbaren vielfältigen technische Entwicklungen offen sein sollte. Für besondere Anforderungen an den Persönlichkeitsschutz bei bestimmten Bearbeitungen sollten bereichsspezifische Regelungen geschaffen werden.

Es entspricht bewährter Rechtsetzungstradition in der Schweiz, dass der Gesetzgeber nicht für jedes neue technische Phänomen eine besondere, in kurzer Zeit schon wieder überholte Regelung schaffen soll. Es hat bisher auch noch niemand schlüssig nachweisen können, welche neuartigen technischen Entwicklungen wie digitale Kommunikation und Internet, Video-Überwachung, relationale Datenbanken und CRM, RFID, Biometrie, GPS usw. durch die bestehenden Datenschutzgrundsätze von Art. 4 – 7

Stellungnahme zum Erlass einer Verordnung über die Datenschutzzertifizierungen (VDSZ)

und die Vorschriften über die Prüfung der Zulässigkeit von Datenbearbeitungen nach Art. 12 und 13 DSG nicht abgedeckt werden.

Die Datenschutzgrundsätze nach Art. 4 - 7 DSG und die Bestimmungen von Art. 12 und 13 DSG betreffend die Abwägung der Interessen der bearbeitenden Stellen und der betroffenen Personen bei Datenbearbeitungen im Bereich des Privatrechts sind daher ohne weiteres auf die nach 1992 eingetretenen technischen Entwicklungen im Informatik- und Telekommunikationsbereich anwendbar, wobei sie von Fall zu Fall in der entsprechenden bereichsspezifischen Gesetzgebung zu präzisieren sind.

3. In der **Botschaft vom 19. Februar 2003** (BBl 2003, S. 2101) wurde dann in Erfüllung des aufgrund der von den Räten am 5.10.2000 überwiesenen Motion 00.3000 „**Erhöhte Transparenz**“ vom 28.1.2000 dem Gesetzgeber erteilten Auftrages sowohl die Transparenz der Datenbeschaffung für die betroffenen Personen durch die bereits erwähnten Art. 4 Abs. 4 und Art. 7a Rev DSG verstärkt, als auch, unter Art. 11a Rev DSG, die **Registrierungspflicht wieder eingeführt**, wobei die Freistellung von der Registrierungspflicht jetzt - in Abweichung von der bisherigen Systematik des Datenschutzgesetzes - nicht mehr auf der Kenntnisverschaffung der betroffenen Personen beruhte, sondern auf einem detaillierten Katalog von Ausnahmen und den dadurch geschaffenen vielfältigen Auslegungs- und Abgrenzungs-Problemen.

In diesem Zusammenhang tauchte dann unter Art. 11 und Art. 11a Abs. 5 Bst. (f) RevE DSG die bisher nie diskutierte, im Vernehmlassungsverfahren nicht behandelte, weder von politischen Parteien noch von den im Bereich des Persönlichkeits- und Konsumentenschutzes aktiven Organisationen, geforderte, und auch im harmonisierten europäischen Datenschutzrecht nicht bekannte Möglichkeit der Freistellung von der Pflicht zur Registrierung durch den Erwerb eines „**Datenschutz-Qualitätszeichens**“ auf.

Der Ursprung dieses neuen Instrumentes zur Verstärkung des Datenschutzes dürfte auf die Zusammensetzung der vom Bundesamt für Justiz gebildeten „informellen Arbeitsgruppe“ zurückgehen, unter deren fünf Mitgliedern **kein einziger Vertreter wirtschaftlich tätiger „Datenschutz-Anwender“** zu finden war, dagegen aber gerade zwei Vertreter von Organisationen welche in der Schweiz als kommerzielle Dienstleistung die Vergabe eines „Datenschutz-Gütesiegels“ betreiben, ihre Anliegen in die Kommissionsarbeit einbringen konnten (vgl. Botschaft vom 19. Februar 2003, BBl vom 18. März 2003, S. 2101 ff, Ziff. 1.2 S. 2107). Das Gütesiegel „Good-Priv@cy®“ ist eines von Dutzenden gegenwärtige in unserem Lande zirkulierenden und übrigens oft mehr zur Verwirrung als zur Information der Konsumenten beitragenden Labels, namentlich in den Bereichen Umweltschutz und Konsumentenschutz.

Die Einführung eines zertifizierten „Datenschutz-Qualitätszeichens“ wurde mit der „Einführung eines Elementes der Selbstregulierung im Datenschutzrecht“ begründet, wodurch die „Selbstverantwortung der Inhaber der Datensammlungen gestärkt und der

Stellungnahme zum Erlass einer Verordnung über die Datenschutzzertifizierungen (VDSZ)

Wettbewerb stimuliert“ werden sollte (wobei diese letztere Aussage als diffuse Erwartung ohne Nachweis zu werten ist). Damit könne bis zu einem gewissen Grade auch der technologischen Entwicklung Rechnung getragen werden (Botschaft zur Revision DSG, a.a.O. Ziff. 2.10, S. 2136).

Wie bereits erwähnt ist aus Kreisen der im SWICO zusammen geschlossenen wirtschaftlich tätigen Anbieter und Anwender von informationsverarbeitenden Systemen nie die Schaffung der Möglichkeit für den Erwerb eines schweizerischen „Datenschutz-Qualitätszeichens“ angeregt oder gar verlangt worden. Insbesondere haben sich die dem Privatrecht unterstellten Anwender und Inhaber von Datensammlungen nie für die Möglichkeit ausgesprochen, den ordnungsgemässen Umgang mit Personendaten nach den Anforderungen des Datenschutzgesetzes durch ein Zertifizierungsverfahren nachzuweisen.

4. In den **Verhandlungen der Eidg. Räte** waren das neue Institut des Datenschutz-Qualitätskennzeichens und des Zertifizierungsverfahrens und die damit verbundenen Probleme nicht Gegenstand irgendwelcher Diskussionen: Der Entwurf des Bundesrates wurde in diesem Punkt von beiden Räten kommentarlos genehmigt (vom Ständerat in der Sitzung vom 3. Juni 2004, vom Nationalrat in der Sitzung vom 6. Oktober 2005).

B. Beurteilung des Datenschutz-Zertifizierungsverfahrens nach Art. 11 Rev DSG

Die im Rahmen der Revision des DSG entwickelte Idee, im Rahmen eines Zertifizierungsverfahrens ein Datenschutz-Qualitätskennzeichen erwerben und sich dadurch über die Einhaltung des Datenschutzes ausweisen zu können, ist grundsätzlich begrüssenswert, weil sie die Umsetzung des Datenschutzes in der Anwendungspraxis mit Hilfe der auf anderen Gebieten der Wirtschaft entwickelten und bewährten Instrumente zu realisieren versucht (Musterbeispiele: Qualitätsmanagementsysteme nach der Normenfamilie ISO 9001-2000 oder Umweltmanagementsysteme nach der ISO Norm 14000:2004).

Die Förderung von berufsständischen Verhaltensregeln zur Umsetzung der Vorschriften über den Datenschutz im Sinne der sog. „Deontologie“ (was allerdings nicht das gleiche ist wie die Zertifizierung von datenschutzgerechten Verfahren und Produkte) ist auch ein erklärtes Ziel der europäischen Datenschutzrichtlinie (Artikel 27 (1) Richtlinie 95/46/EG).

Es ist aus der Sicht der in der SWICO Arbeitsgruppe VDSZ vertretenen Unternehmen allerdings zu befürchten, dass dieser gut gemeinte Ansatz in der Wirklichkeit die Erwartungen, welche der Gesetzgeber an die Zertifizierung des Datenschutzes stellt, aus folgenden Gründen nicht oder nicht im erhofften Umfange erfüllen kann:

1. Datenschutz durch organisatorische und technische Mittel und Verfahren

Stellungnahme zum Erlass einer Verordnung über die Datenschutzzertifizierungen (VDSZ)

- 1.1 „**Zertifizieren**“ ist der Nachweis der Übereinstimmung („Konformität“) von Tatbeständen oder Verfahren mit definierter Vorgabe in Form eines nationalen oder internationalen Standards, z.B. einer ISO/DIN/SNV Norm im Sinne von Art. 3 der Buchstaben (g) bis (l) des Bundesgesetzes über die technischen Handelshemmnisse (THG) vom 6. Oktober 1995 (SR 946.51).

Als „**Datenschutz**“ wird hier der verantwortungsbewusste Umgang mit Personendaten zum Schutze der Persönlichkeit und der Grundrechte (Art. 1 DSG), d.h. des Schutzes der Privatsphäre und des „informationellen Freiheitsrechtes“ der betroffenen Personen im Sinne der Gewährleistung der „informationellen Selbstbestimmung“ betrachtet.

Bei der Bearbeitung von Personendaten wird der Schutz der Privatsphäre und des informationellen Selbstbestimmungsrechts verwirklicht durch die Beachtung der Datenschutzgrundsätze gemäss Art. 4 DSG (namentlich Treu und Glauben, Verhältnismässigkeit, Zweckbindungsgebot), durch die Erfüllung der vielfältigen weiteren sich aus dem Rev DSG ergebenden Handlungspflichten wie Information der betroffenen Personen nach Art. 4 Abs. 4 und Art. 7a Rev DSG, die Erteilung von Auskünften und die Prüfung der Möglichkeiten zu deren Einschränkung (Art. 8 und 9 Rev DSG), die Beurteilung der Zulässigkeit bestimmter Bearbeitungsvorgänge wie grenzüberschreitende Bekanntgabe (Art. 6 Rev DSG) oder Datenbearbeitung durch Dritte (Art. 10a Rev DSG), sowie durch die Interessenabwägung und Beurteilung von Rechtfertigungsgründen durch bearbeitende Stellen des Privatrechts nach Art. 12 und 13 Rev DSG.

Die Umsetzung des Datenschutzes verlangt vom Anwender somit **kritische, wertende Entscheidungen im Einzelfall**. Dieses datenschutzgerechte Soll-Verhalten lässt sich nicht ohne weiteres zum vornherein feststellen und festhalten, wie die teilweise kontroverse Lehre, die publizierten Resultate der Abklärungen des EDÖB, sowie die von der Eidg. Datenschutzkommission (Art. 33 DSG) und vom Bundesgericht in Datenschutz-Angelegenheiten gefällten Entscheidungen zum Ausdruck bringen.

- 1.2 Die Einhaltung des Datenschutzes durch den Anwender entzieht sich nach der in der SWICO Arbeitsgruppe VDSZ vorherrschenden Auffassung weitgehend der Möglichkeit einer Zertifizierung, weil sich „rechtskonformes künftiges Verhalten“ als solches gar nicht zertifizieren lässt.

Zertifizieren lassen sich, wie in Art. 4 VE VDSZ umschrieben, das **Vorhandensein eines Datenschutz-Managementsystems** sowie bestimmte **organisatorische und technische Massnahmen** und die zu deren Umsetzung **verwendeten technischen Hilfsmittel, namentlich für die Datensicherung**.

Die in diesem Zusammenhang angesprochenen Normen OHSAS 18001:1999 „Arbeitssicherheit und Gesundheitsschutz“ sowie die in Art. 4 Abs. 3 VE VDSZ erwähnte Norm ISO/IEC 27001: 2005 (ex BS 7799-2:2002) „Informationssicherheits-

Stellungnahme zum Erlass einer Verordnung über die Datenschutzzertifizierungen (VDSZ)

Managementsysteme“ beziehen sich allerdings kaum oder nur ganz am Rande auf den Kernbereich des Datenschutzes als Schutz der Privatsphäre und Gewährleistung der informationellen Selbstbestimmung im Sinne der Überlegungen unter der vorstehenden Ziff. B/1.1 sondern sie behandeln ausschliesslich oder ganz überwiegend die Gewährleistung der Datensicherheit im Sinne von Art. 7 DSGVO / Art. 8 ff VDSG.

- 1.3 Dabei ist nicht in Zweifel zu ziehen, dass geeignete **IT-Produkte, Organisationsstrukturen, Abläufe und Verfahren** den Anwender in der Wahrung der Persönlichkeitsrechte der betroffenen Personen bei der Bearbeitung der sie betreffenden Daten **unterstützen** und insbesondere die **Datensicherheit** bei der Bearbeitung von Personendaten **fördern** können.

Die Gewährleistung der Datensicherheit nach Art. 7 Rev DSGVO ist jedoch nur einer, und nach der in der SWICO Arbeitsgruppe VDSZ vorherrschenden Auffassung gerade von Informatikern und Datenschutz-Aufsichtsbehörden in seiner Bedeutung und Tragweite für die Umsetzung des „Datenschutzes“ im Sinne der Definition unter Ziff. B/1.1 gerne überschätzter Teilbereich des sorgfältigen Umganges mit Personendaten unter Achtung und Wahrung der Persönlichkeit der betroffenen Personen und des informationellen Selbstbestimmungsrechtes.

Die Erwartung, „Datenschutz“ als Persönlichkeitsschutz und Gewährleistung der informationellen Selbstbestimmung im Sinne der Definition unter vorstehender Ziff. B/1.1 lasse sich ausschliesslich oder vorwiegend durch organisatorisch und technische Mittel und Verfahren herstellen, beruht nach Meinung der vom SWICO eingesetzten Arbeitsgruppe VDSZ auf einem falschen Verständnis von „Datenschutz“ und lässt sich nicht rechtfertigen.

- 1.4 Es überrascht daher nicht, dass sich **Normen oder Standards zur Wahrung des „Datenschutzes“** im Sinne der Definition unter vorstehender Ziff. B/1.1 zur Zeit **weder auf nationaler noch auf internationaler Ebene** finden lassen, und es uns sind diesbezüglich auch keine diesbezüglichen Projekte oder Vorarbeiten bekannt (auf das „Modell“ Schleswig-Holstein wird unter nachstehender Ziff. B/1.6 eingegangen).

Diese Situation ist u.E. darauf zurückzuführen, dass die Gesetzgebung über den Datenschutz auch unter dem durch die Richtlinie 95/46/EG harmonisierten europäischen Datenschutzrecht - und erst recht in den Ländern ausserhalb des Europäischen Wirtschaftsraumes - dem nationalen Gesetzgeber übertragen ist und daher zum vornherein wenig Raum für verbindliche internationale Normen über den Datenschutz im Sinne der Begriffsdefinition von Ziff. B/1.1 besteht.

- 1.5 Die auf dem Gebiet der **Entwicklung datenschutzfreundlicher Normen und Standards** eingeleiteten Initiativen in Kanada „Model Code for the Protection of Personal Information, a National Standard of Canada“, bzw. die Arbeiten der internationalen

Stellungnahme zum Erlass einer Verordnung über die Datenschutzzertifizierungen (VDSZ)

Normenvereinigung CEN / ISS „Initiative on Privacy Standardisation in Europe“, Final Report 13 February 2002, sind von der unter Art. 29 Richtlinie 95/46/EG geschaffenen EU Datenschutzfachgruppe in der Opinion 1/97, WP XV/5023/97-Final und Opinion 1/2002, WP 57, 10761/02/EN/Final zwar in allgemeiner Form begrüsst worden, ohne dass sie bisher zu europäischen oder internationalen Datenschutz-Standards geführt hätten.

Aufgrund einer von der SWICO Arbeitsgruppe VDSZ vorgenommenen Analyse von Gegenstand, Inhalt und Zielsetzung berühren die vorstehenden Initiativen die Kern-Anforderungen des Datenschutzes gemäss der Definition unter Ziff. B/1.1 „Schutz der Privatsphäre und Gewährleistung des informationellen Selbstbestimmungsrechtes“ nur am Rande: Sie beziehen sich mit Schwergewicht auf Technologien, Verfahren und Produkte, beispielsweise auf dem Gebiet des Konsumentenschutzes beim elektronischen Geschäftsverkehr, welche die Umsetzung der Anforderungen aus dem Datenschutz, insbesondere die Datensicherheit im Sinne von Art. 7 DSG / Art. 8 - 12 VDSG, erleichtern und unterstützen, das datenschutzgerechte Verhalten der bearbeitenden Stellen als solches jedoch nicht gewährleisten können.

- 1.6 Das im Zusammenhang mit Datenschutz-Zertifizierung häufig angeführte und durch einen EU Förderungsbeitrag unterstützte **Zertifizierungsmodell des „Unabhängigen Landesentrums für Datenschutz Schleswig-Holstein“** („ULDS“) kann nach Auffassung der SWICO Arbeitsgruppe VDSZ aus folgenden Überlegungen nur sehr eingeschränkt zur Unterstützung der in Art. 11 und Art. 11a Abs. 5 Bst. (f) Rev DSG und im VE VDSZ enthaltenen Regelungen herangezogen werden:

/1 **Datenschutz-Audit**

Das „Landesdatenschutzgesetz Schleswig-Holstein vom 9. Februar 2000 („LDSG-SH“) kann zum vornherein **nur Geltung für öffentliche Stellen** des Bundeslandes beanspruchen (§ 3 (1) LDSG-SH) und ist somit für die in Art. 11a Abs. 3 und 4 angesprochenen Daten bearbeitenden Stellen des Privatrechtsverkehrs gerade nicht anwendbar.

Gemäss § 43 Abs. 3 LDSG-SH können die öffentlichen Stellen des Bundeslandes ihr „Datenschutzkonzept“ durch das ULDS „prüfen und beurteilen“ lassen: sog. „**Datenschutz-Audit**“, ohne dass jedoch für die Durchführung eines solchen „Audit“ ein Datenschutz-Qualitätskennzeichen vergeben wird.

/2 **Zertifizierung von IT-Produkten**

In Schleswig-Holstein ist die Zertifizierung ausschliesslich auf die „**Zertifizierung von IT-Produkten**“ mit dem Schwergewicht „Datensicherheit“ ausgerichtet.

„IT-Produkte“ sind „Hardware, Software und automatisierte Verfahren, die zur Nutzung durch öffentliche Stellen (des Landes Schleswig-Holstein) geeignet

Stellungnahme zum Erlass einer Verordnung über die Datenschutzzertifizierungen (VDSZ)

sind“ (§ 1 Abs. 2 der Landesverordnung über ein Datenschutz-Audit vom 3. April 2001 („DSAVO“).

Es handelt sich um „Produkte, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde“. Solche Produkte „sollen (durch die dem Gesetz unterstellten öffentlichen Stellen) vorrangig eingesetzt werden“ (§ 4 Abs. 2 LDSG-SH).

Nach § 1 Abs. 1 DSAVO nimmt das „Unabhängige Landeszentrum für Datenschutz einen „Datenschutz-Audit“ vor und erteilt einem IT-Produkt, welches den Rechtsvorschriften über den Datenschutz und die Datensicherheit entspricht, ein Zertifikat in Form eines „**Datenschutz-Gütesiegels**“.

- 1.7 In Abweichung zum „Modellgesetz“ LDSG-SH sehen Art. 11 Rev. DSG und Art. 1 Abs. 2 Bst. (a) sowie Art. 4 VE VDSZ, dass die Gesamtheit der Datenbearbeitungsvorgänge einer „Organisation“, bzw. „einzelne, abgrenzbare Datenbearbeitungsverfahren“ zertifiziert werden können.

Wie vorstehend unter Ziff. B/1.1 ausgeführt, bestehen allerdings erhebliche Bedenken und Vorbehalte betreffend die Möglichkeit, den von einer Organisation als ganzes oder in Bezug auf eine kritische Anwendung befolgten Datenschutz zertifizieren zu lassen, insbesondere weil entgegen den Angaben unter Art. 4 Abs. 3 VE VDSZ keine anerkannten internationalen Normen und Standards für die Umsetzung des Datenschutzes vorhanden sind.

Die in Art. 4 Abs. 3 VE VDSZ erwähnten ISO Norm 27001:2005 (ex BS 7799-2:2002) „Information technology – Security techniques – Information security management systems – Requirements“ bezieht sich auf die „Anforderungen an die Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems“ und erwähnt die Einhaltung der Anforderungen aus den Rechtsvorschriften über den Datenschutz nur am Rande und ohne dafür spezifische Anforderungen aufzustellen.

Es ist schwer vorstellbar, wie aufgrund eines sehr allgemein gehaltenen Nebensatzes in der Norm ISO 27001:2005 eine Organisation und die von ihr angewendeten Datenbearbeitungsverfahren hinsichtlich der Einhaltung des Datenschutzes nach den vielfältigen rechtlichen Anforderungen des schweizerischen Datenschutzgesetzes zertifiziert werden sollen.

- 1.8 Im Gegensatz zu dem Konzept von Art. 11 und Art. 11a Abs. 5 Bst. (f) Rev DSG ist in Schleswig-Holstein mit der Durchführung eines „Datenschutz-Audit“ sowie der Vergabe eines „Gütezeichens“ gemäss dem ULDS Zertifizierungsverfahren auch weder eine Freistellung von der allgemeinen Registrierungspflicht gemäss § 7 LDSG SH jener öffentlichen Stellen verbunden, welche zertifizierte IT Produkte einsetzen, noch ist ir-

Stellungnahme zum Erlass einer Verordnung über die Datenschutzzertifizierungen (VDSZ)

gend eine Vermutung ausgesprochen, dass die Anwender durch den Einsatz von zertifizierten IT-Produkten zur Bearbeitung von Personendaten die Anforderungen des deutschen Bundesdatenschutzgesetzes oder des Landesdatenschutzgesetzes Schleswig-Holstein erfüllen.

Die bearbeitenden Stellen der öffentlichen Verwaltung des Bundeslandes Schleswig-Holstein werden durch § 4 (2) LDSG-SH lediglich dazu angehalten, bei IT Anwendungen vorrangig Produkte mit einem von der ULDS verliehenen Gütesiegel einzusetzen. Mehr oder andere Rechtswirkungen enthält das von der ULDS nach Durchführung eines Datenschutz-Audits abgegebene „Datenschutz-Gütesiegel“ nicht.

- 1.9 Sachgerecht erscheint nach Auffassung der SWICO Arbeitsgruppe VDSZ andererseits, dass die Vergebung von „Datenschutz-Qualitätszeichen“, welche die Anforderungen von Art. 11 Rev DSG und der Zertifizierungsverordnung erfüllen und die dort vorgesehenen Rechtswirkungen entfalten, gemäss Art. 1 Abs. 1 VE VDSZ **akkreditierten Zertifizierungs-Dienstleistern** übertragen werden soll.

Das schliesst u.E. die Weiterführung der Vergebung von „Datenschutz-Gütesiegeln“ nach dem Muster von „GoodPriv@cy“ durch private Organisationen nicht aus, nur sollten die Anbieter solcher „Datenschutz-Labels“ zur Vermeidung der Irreführung des Publikums (Art. 3 UWG) deutlich machen, dass sie nicht zur Vergebung von Datenschutz-Qualitätszeichen im Sinne von Art. 11 Rev DSG berechtigt sind.

2. Überlegungen zum Erwerb eines Datenschutz-Qualitätszeichens durch IT-Anwender

- 2.1 In Bezug auf die Erfüllung der vielfältigen Anforderungen aus dem DSG zum Schutz der Privatsphäre und zur Gewährleistung der „informationellen Selbstbestimmung“ der betroffenen Personen bei der Bearbeitung der sie betreffenden Daten kann ein „Datenschutz-Qualitätskennzeichen“ nach der hier vertretenen Auffassung lediglich aussagen, dass ein bestimmter Anwender über eine Organisation verfügt (z.B. durch die Bezeichnung eines „Datenschutzverantwortlichen“ nach Art. 11 Abs. 5 Bst. (e) Rev DSG), dass er eine revisionsfähige Protokollierung und Dokumentation datenschutzkritischer Anwendungen unterhält (wozu er schon heute nach Art. 10 und 11 VDSG verpflichtet ist), und dass der betreffende Anwender bestimmte Verfahren entwickelt hat (z.B. über die Prüfung von neuen Applikationen, Auskunftserteilung, Datenschutzgarantien durch Vertrag) welche den Datenschutz befördern (vgl. die Angaben zu einem zertifizierten „Datenschutzmanagementsystem“ nach Art. 4 Abs. 2 VE VDSZ).
- 2.2 Dagegen wird das in einem aufwendigen, gemäss Art. 11 Rev DSG und VE VDSZ zertifizierten Verfahren erworbene Datenschutz-Qualitätszeichens - vergleichbar der Zertifizierung eines Qualitäts-Managementsystems nach ISO/DIN 9001- den mit der Bearbeitung von Personendaten betrauten und in das Verfahren zum Erwerb des Da-

Stellungnahme zum Erlass einer Verordnung über die Datenschutzzertifizierungen (VDSZ)

tenschutz-Qualitätszeichens einbezogenen Hilfspersonen des betreffenden Anwenders zweifellos die Bedeutung des Datenschutzes klar machen und das Bewusstsein für den Datenschutz heben.

Der Erwerb eines Datenschutz-Qualitätszeichens schafft somit mindestens eine - widerlegbare - Vermutung, dass sich der betreffende Anwender ernsthaft mit den Anforderungen aus dem Datenschutz befasst hat; ein Zertifikat kann somit den Anwender, solange er die dem Zertifikat zu Grunde liegenden Verfahren einhält, vom Vorwurf der absichtlichen Verletzung der Datenschutzbestimmungen gemäss Art. 34 Rev DSG entlasten.

- 2.3 Hingegen kann der Erwerb eines Datenschutz-Qualitätszeichens nach der hier vertretenen Auffassung niemals gewährleisten, dass der Inhaber eines Zertifikates und seine mit der Bearbeitung personenbezogener Daten betrauten Mitarbeitenden sich zu jeder Zeit, in jeder Beziehung und unter allen Umständen datenschutzgerecht verhalten (vgl. als Beispiel den Schlussbericht des EDÖB vom 23. Mai 2005 mit Anhang vom 28. September 2007 über das Ergebnis der Datenschutzkontrolle des - durch das „Datenschutz-Gütesiegel“ GoodPriv@cy[®] ausgezeichneten - Kundenbindungsprogrammes „M-CUMULUS“: Der erwähnte Bericht enthält eine Reihe von Empfehlungen des EDÖB gemäss Art. 29 Abs. 3 DSG zur Verbesserung des Datenschutzes der durch ein „Datenschutz-Gütesiegel“ ausgezeichneten Anwendung „M-CUMULUS“, weil diese Anwendung nicht in allen Punkten den Anforderungen des Datenschutzes entsprochen hat. Bekanntlich ist der Migros-Genossenschafts-Bund MGB wegen der Nutzung der mit der zertifizierten Anwendung „M-CUMULUS“ elektronisch erfassten und genutzten Personendaten trotz Erwerbs des Gütesiegels „Good Priv@cy[®]“ mehrmals für den „Big Brother Award“ nominiert worden, der Organisationen verliehen wird, welche durch ihre Anwendungen nach Auffassung der Vergebungsstelle die Persönlichkeit betroffener Personen besonders massiv verletzen).
- 2.4 Nachdem, wie eingangs gezeigt wurde, weder das harmonisierte europäische Datenschutzrecht noch ausländische Datenschutzgesetze die Zertifizierung des Datenschutzes vorsehen, und - mit Ausnahme der sich auf die Datensicherheit beziehenden Normen - heute und in voraussehbarer Zukunft auch keine internationalen Normen oder Standards zur Umsetzung des Persönlichkeitsschutzes bei der Datenbearbeitung vorhanden sind, leidet ein in der Schweiz ausgegebenes Datenschutz-Qualitätszeichen für das Datenschutzmanagementsystem eines auf den globalen Märkten tätigen Unternehmens zum vornherein unter einem **unheilbaren Mangel: *Es fehlt die internationale Anerkennung***. Denn es ist schlechthin nicht einzusehen, welche Bedeutung die deutsche, englische oder französische Aufsichtsbehörde über den Datenschutz einem in der Schweiz von einer privaten Organisation verliehenen Datenschutz-Gütesiegel betreffend die korrekte Anwendung der deutschen, englischen oder französischen Vor-

Stellungnahme zum Erlass einer Verordnung über die Datenschutzzertifizierungen (VDSZ)

schriften über den Datenschutz beimessen könnte, selbst wenn das Datenschutz-Qualitätszeichen in Zukunft durch eine nach den Bestimmungen der VDSZ akkreditierte Organisation vergeben wird.

- 2.5 Im weiteren **fehlt** - jedenfalls für die privatwirtschaftlich tätigen Anwender (es sei diesbezüglich daran erinnert, dass das Gütesiegel in Schleswig-Holstein auf Anwendungen durch die öffentliche Verwaltung zugeschnitten ist) - **ein ins Gewicht fallender wirtschaftlicher Anreiz**, in einem aufwendigen und kostspieligen Verfahren ein „Datenschutz-Qualitätszeichen“ von einem akkreditierten Anbieter zu erwerben, und damit gemäss Art. 11a Abs. 5 Bst. (f) Rev DSG von der Registrierungspflicht freigestellt zu werden. Denn die meisten Anwender werden es nach Auffassung der SWICO Arbeitsgruppe VDSZ vorziehen, für die in der Regel geringe Zahl der unter die Registrierungspflicht fallenden Datensammlungen das vom EDÖB, in Zukunft möglicherweise im Download zur Verfügung gestellte Anmeldeformular auszufüllen, oder gemäss Art. 11a Abs. 5 Rev DSG für alle Datenbearbeitungen in ihrem Unternehmen eine umfassende Freistellung von der Registrierungspflicht durch die Bezeichnung eines Datenschutz-Verantwortlichen („Datenschutz-Berater“) zu erwirken.
- 2.6 Nach der von der SWICO Arbeitsgruppe VDSZ vertretenen Auffassung kann durch den Erwerb eines Datenschutz-Qualitätszeichens grundsätzlich nur eine bestimmte, konkrete Anwendung, also eine gemäss Art. 11 Abs. 3 Rev VDSG der Registrierungspflicht unterliegende Datensammlung (wie z.B. das bereits erwähnte Kundenbindungsprogramm „M-CUMULUS“) im Hinblick auf die Einhaltung des Datenschutzes geprüft und zertifiziert werden, oder ein Unternehmen, dessen wirtschaftliche Tätigkeit sich auf ganz bestimmte, eng umschriebene Datenbearbeitungen beschränkt (z.B. Sammlung, Auswertung und Verkauf von Adressen) - kaum aber ein Unternehmen oder ein Konzern wie eine Grossbank oder eine weltweit tätige Versicherung mit Dutzenden oder hunderten von Datensammlungen und Informatik-Anwendungen, welche darüber hinaus einem ständigen dynamischen organisatorischen und technischen Wandel unterliegen.
- 2.7 In Bezug auf ein Unternehmen kann ein Datenschutz-Qualitätszeichen gemäss der Formulierung von Art. 11 Abs. 1 Rev DSG nur nachweisen, dass das zertifizierte Unternehmen über eine mit kompetenten, sachkundigen Personen besetzte **Organisation** verfügt, welche mit der Umsetzung des Datenschutzes im Unternehmen betraut ist (vgl. Art. 1 Abs. 2 Bst. (a) und Art. 4 VDSZ). Eine solche Organisation entspricht nach ihrer Funktion und Zweckbestimmung jedoch weitgehend der Bezeichnung eines im Sinne von Art. 12a und 12b RevE VDSG fachlich ausgewiesenen, in Bezug auf die Erfüllung seines Auftrages nicht an Weisungen gebundenen **Datenschutzberaters**, welcher Tag für Tag die Geschäftsleitung und die Fachabteilung über die korrekte Anwendung des Datenschutzes berät und unterstützt. In der Regel wird ein Unternehmen

Stellungnahme zum Erlass einer Verordnung über die Datenschutzzertifizierungen (VDSZ)

somit den Weg wähle, die Freistellung von der Pflicht zur Anmeldung sämtlicher innerbetrieblicher Datensammlung gestützt auf Art. 11a Abs. 5 Bst. (e) Rev DSG durch die Bezeichnung eines Datenschutzverantwortlichen (Datenschutzberater) zu erwirken, anstatt seine Organisation und das Datenschutzmanagementsystem gegen Entgelt durch eine betriebsfremde Organisation überprüfen zu lassen.

- 2.8 Die nach der Einführung eines von privaten Organisationen in der Schweiz angebotenen „Datenschutz-Gütesiegels“ in der Schweiz gemachten praktischen Erfahrungen haben nach der Beurteilung der SWICO Arbeitsgruppe VDSZ gezeigt, dass der **Erwerb eines Datenschutz-Gütesiegels keinen messbaren Vorsprung im wirtschaftlichen Wettbewerb schafft**. So haben die Geschäftsleitungen der beiden Grossverteiler Migros und Coop in Bezug auf den Erwerb eines „Datenschutz-Gütesiegels“ gerade einander entgegen gesetzte Entscheidungen getroffen, und die in der Folge vom E-DÖB nach Art. 29 DSG durchgeführten Abklärungen der beiden Kundenbindungsprogramme „M-CUMULUS“ und Coop „Supercard“ haben gezeigt, dass der Erwerb eines „Datenschutz-Gütesiegels“ (System „M-CUMULUS“) offenbar nicht mit einem höheren Grad des betrieblichen Datenschutzes verbunden ist als die Wahrnehmung der Pflichten aus dem DSG durch eine nicht zertifizierte Organisation (Coop „Supercard“-System). Auf jeden Fall sind die privaten Organisationen, welche in der Schweiz „Datenschutz-Gütesiegel“ anbieten, bisher den Beweis dafür schuldig geblieben, dass sich der erhebliche Aufwand für den Erwerb und die periodische Erneuerung eines Zertifikates hinsichtlich des Grades des erreichten betrieblichen Datenschutzes und der dadurch bewirkten Vorteile im Wettbewerb lohnt.

Zusammenfassung

Aus den vorstehenden nur beispielhaft aufgeführten Gründen stehen nach dem Kenntnisstand der SWICO Arbeitsgruppe VDSZ die privatwirtschaftlichen Anbieter und Anwender von Informations- und Kommunikationssystemen in der Schweiz dem durch Art. 11 Rev DSG ohne ihre vorgängige Anhörung und Möglichkeit zur Stellungnahme geschaffenen Angebot des Erwerbs eines „Datenschutz-Qualitätszeichens“ für das „Datenschutz-Managementsystem“ in ihrer Mehrheit distanziert, kritisch oder ablehnend gegenüber.

3. Überlegungen zur Zertifizierung von IT-Produkten

- 3.1 Wie sich aus der Analyse der Problematik von sog. „Datenschutz-Zertifizierungen“ ergibt, sind durch Art. 11 Rev DSG hat **zwei grundlegend unterschiedliche Kategorien von „Datenschutz-Qualitätszeichen“** geschaffen worden, nämlich
- /1 **Zertifizierung der „Organisation und Verfahren“**, d.h. der Aufbau- und Ablauforganisation eines IT-Anwenders im Hinblick auf die Beachtung der Anforderun-

Stellungnahme zum Erlass einer Verordnung über die Datenschutzzertifizierungen (VDSZ)

gen aus dem Datenschutz („Datenschutzmanagementsystem“), entsprechend dem durch das ULD-SH durchgeführten „Datenschutz-Audit“; und

- /2 **Zertifizierung von bestimmte Produkten (Programme und Systeme)**, welche die Beachtung des Datenschutzes durch technische und organisatorische Mittel fördern und unterstützen z.B. durch Zugriffskontrolle und Zugriffsschutz, Daten-selektion, geschützte Archivierung, Datensicherung, automatisierte Sicherheitsprüfung, Verschlüsselung, bis zur kontrollierten Aktenvernichtung (vgl. die Übersicht der vom ULD-SH verliehenen „Datenschutz-Gütesiegel“).

Art. 1 Abs. 2 sowie Art. 4 und 5 VE VDSZ unterscheiden richtigerweise zwischen diesen beiden grundlegend unterschiedlichen Formen einer Datenschutz-Zertifizierung.

- 3.2 Wie bereits erwähnt beschränkt sich die Vergebung eines Datenschutz-Qualitätszeichens („Datenschutz-Gütesiegel“) nach dem in dieser Beziehung gewissermassen als „Modellgesetz“ dienenden Landesdatenschutzgesetz Schleswig-Holstein in § 4 Abs. 2 LDSG-SH und § 1 DSAVO auf die Prüfung von **informationstechnischen Produkten** („IT-Produkte“), „umfassend Hardware, Software und automatisierte Verfahren“ zur Bearbeitung von Personendaten im Hinblick auf die „Erfüllung der Rechtsvorschriften über den Datenschutz und die Datensicherheit“, namentlich „Datenvermeidung und Datensparsamkeit, Datensicherheit und Revisionsfähigkeit der Datenverarbeitung; Gewährleistung der Rechte der betroffenen Personen“.

Nach Auffassung der SWICO Arbeitsgruppe VDSZ ist der vom „Modellgesetz“ LDSG-SAH gewählte Zertifizierungs-Ansatz grundsätzlich richtig und zweckmässig: Es gibt zweifellos technische Eigenschaften von IT-Produkten (wie hierarchische Zugangsverfahren und Zugriffsregeln, Passwortverwaltung, automatisierte Protokollierung von Verarbeitungsvorgängen, Zugriffsschutz, Kontrolle der Datenbekanntgabe, Kopierschutz, Verschlüsselung, geschützte Datenarchivierung und kontrollierte Datenlöschung / Vernichtung), welche die Daten verarbeitenden Stellen bei der Einhaltung der gesetzlichen Anforderungen an den Datenschutz und insbesondere an die Datensicherheit wirksam unterstützen.

- 3.3 Die Erwartung ist wohl nicht ganz unberechtigt, dass der vom Gesetzgeber durch Schaffung der Datenschutz-Zertifizierung geförderte Einsatz von „datenschutzgerechten IT-Produkten“ bei den für die Einhaltung der Rechtsvorschriften über den Datenschutz verantwortlichen Anwendern in Wirtschaft und Verwaltung längerfristig eine allgemeine Hebung des Niveau des Datenschutzes bewirken kann.

Insbesondere ist denkbar, dass die Inhaber von Datensammlungen in den für den Datenschutz kritischen öffentlichen und privaten Bereichen wie innere und äussere Sicherheit, Medizin, Banken, Versicherung, Sozialfürsorge, dazu übergehen werden, bei neuen IT-Projekten der Beschaffung von zertifizierten IT-Produkten den Vorzug zu ge-

Stellungnahme zum Erlass einer Verordnung über die Datenschutzzertifizierungen (VDSZ)

ben. Dieser Grundsatz ist auch in § 4 Abs. 2 LDSG-SH verankert, wo die öffentlichen Stellen des Landes Schleswig-Holstein angehalten werden, „bei der Beschaffung von Informatikmitteln zertifizierten IT-Produkten den Vorrang einzuräumen“.

- 3.4 Die Schaffung der Möglichkeit für die Zertifizierung von IT-Produkten darf aus der Sicht der durch den SWICO vertretenen Anbieter und Anwender von IT-Produkten in der Schweiz allerdings **nicht zu einer Verzerrung des Wettbewerbs** führen, denn ein Grossteil der in der Schweiz angebotenen IT-Produkte wird im Ausland hergestellt und in die Schweiz eingeführt: Es versteht sich, dass die Zertifizierung auf international anerkannten technischen Normen beruhen sollte (Art. 11 Abs. 2 Rev DSG).

Die von ausländischen, in einem mit der VDSZ vergleichbaren Verfahren zugelassenen Zertifizierungsstellen ausgegebenen „Datenschutz-Gütesiegel“ sollten auch in der Schweiz anerkannt werden (wie das Art. 7 VE VDSZ zu recht vorsieht).

So wie der Erwerb eines Zertifikates für ein IT-Produkt durch einen Anbieter auf **Freiwilligkeit** beruht, so sollten auch Wirtschaft und Verwaltung nicht durch Rechtsvorschriften zum Einsatz zertifizierter IT-Produkte verpflichtet werden: Die Beschaffung von zertifizierten oder nicht zertifizierten IT-Produkten muss dem Ermessen der betreffenden Anwender überlassen bleiben.

- 3.5 Im Weiteren kann nur die Zertifizierung einer Organisation oder eines Verfahrens nach Art. 1 Abs. 2 Bst. (a) und Art. 4 RevE VDSZ zu einer Freistellung des betreffenden Anwenders von der Pflicht zur Anmeldung der Gesamtheit oder einzelner, abgrenzbaren Datenbearbeitungsverfahren (Art. 11a Abs. 5 Bst. (f) Rev DSG) zur Registrierung der betreffenden Datensammlungen bei dem oder der Beauftragten führen. Es ist aus der Sicht der SWICO Arbeitsgruppe nicht denkbar, dass z.B. eine Organisation wie ein Spital, das einen zertifizierten „Reisswolf-Aktenvernichter“ zur Vernichtung von medizinischen Aufzeichnungen einsetzt (vgl. die von der ULD SH vergebenen Zertifikate 4-6/2004 und 1-1/2006), infolge des Einsatzes eines solchen zertifizierten Aktenvernichters von der Anmeldung des Patienten-Informationssystems zur Registrierung beim Beauftragten entbunden wird. Eine entsprechende, u.E. zutreffende Konsequenz ergibt sich - allerdings nicht mit letzter Klarheit - aus Art. 4 Abs. 4 VE VDSZ.

Zusammenfassung

Zusammenfassend ist die SWICO Arbeitsgruppe VSZ, in welcher verschiedene Anbieter und Anwender von IT-Produkten vertreten sind, der Meinung, dass die Vergebung von Datenschutz-Qualitätszeichen für IT-Produkte längerfristig zu einer Verbesserung namentlich der sicherheitsbezogenen Aspekte der Bearbeitung von Personendaten führen kann. Wichtig ist in diesem Zusammenhang, dass der Erwerb eines Datenschutz-Qualitätszeichens und der Einsatz von zertifizierten IT-Produkten auf dem **Grundsatz der Freiwilligkeit** beruht, dass zur Prüfung der Konformität auf **internatio-**

nale Normen und Standards abgestellt wird, und dass ein im Ausland in einem gleichwertigen Verfahren erworbene Zertifikat in der Schweiz anerkannt wird.

4. Stellungnahme zur Zertifizierung nach dem VE VDSZ

4.1 Zertifizierung von Organisation und Verfahren nach Art. 4 VE VDSZ

Die eingangs aufgedeckte Problematik der Zertifizierung des „datenschutzgerechten Verhaltens“ findet ihre Bestätigung im Gegenstand der Begutachtung des von einem Anwender unterhaltenen „**Datenschutzmanagementsystems**“ nach Art. 4 Abs. 2 VE VDSZ: Die hier aufgeführten Anforderungen beziehen sich praktisch ausschliesslich auf die Errichtung, den Betrieb, die Überwachung und die Verbesserung von Sicherheits- und Risiko-Managementsystemen.

Insbesondere enthält die in Art. 4 Abs. 3 VE VDSZ als Grundlage der Konformitätsprüfung erwähnte Norm ISO 27001: 2005, wie bereits unter Ziff. B/1.7 erwähnt, keine konkreten Anforderungen für die Einhaltung der Vorschriften zum datenschutzgerechten Verhalten nach dem in Ziff. B/1.1 umschriebenen Verständnisses des Datenschutzes als Schutz der Privatsphäre und Gewährleistung der informationellen Selbstbestimmung.

Auch der Gegenstand der Konformitätsprüfung nach Art. 4 Abs. 2 VE VDSZ, d.h. eine formulierte „Datenschutzpolitik“, eine „Dokumentation von Zielen und Massnahmen“ zur Gewährleistung des Datenschutzes und der Datensicherheit, sowie die „organisatorischen und technischen Vorkehrungen zur Verwirklichung der festgelegte Ziele und Massnahmen und zur Behebung festgestellter Mängel“ beziehen sich mit Schwergewicht auf die organisatorisch-technischen Massnahmen zur Gewährleistung der Datensicherheit, wie sie in Art. 7 DSG und Art. 8 - 12 der geltenden VDSG umschrieben sind.

Daraus folgt, dass ein IT-Anwender aufgrund der dargestellten Kriterien relativ einfach ein „Datenschutz-Qualitätszeichen“ erwerben kann, eine Gewährleistung des datenschutzgerechten Verhaltens im Sinne der Begriffsbestimmung unter Ziff. B/1.1 dadurch jedoch nicht gewährleistet werden kann.

Das Defizit in der Umsetzung Datenschutzes nach der Zielsetzung des DSG: „Schutz der Privatsphäre und Gewährleistung der informationellen Selbstbestimmung“ liegt ganz eindeutig - das beweisen viele publizierte Berichte und Empfehlungen des EDÖB über die von ihm gemäss Art. 29 DSG durchgeführten Abklärungen - weniger in den organisatorischen und technischen Massnahmen zur Gewährleistung der Datensicherheit: Solche Massnahmen ergreift der IT-Anwender schon im eigenen Interessen - sondern in der korrekten Umsetzung der Datenschutzgrundsätze, und dazu trägt ein Datenschutz-Qualitätszeichen, das sich auf die Prüfung der unter Art. 4 Abs. 2 VE

Stellungnahme zum Erlass einer Verordnung über die Datenschutzzertifizierungen (VDSZ)

VDSZ aufgeführten Voraussetzungen für ein sog. „Datenschutzmanagementsystem“ beschränkt, nur sehr wenig bei.

4.2 Zur Zertifizierung von IT Produkten nach Art. 5 VE VDSZ

Zunächst ist nicht einzusehen, weshalb sich die Zertifizierung der IT-Produkte gemäss Art. 5 Abs. 1 VE VDSZ auf „Softwareprodukte oder deren Kombination mit bestimmten Hardwareprodukten“ beschränken soll. Dieser Anwendungsbereich ist erheblich enger als die Definition der IT Produkte nach § 1 Abs. 2 DSAVO: „IT-Produkte im Sinne dieser Verordnung sind Hardware, Software und automatisierte Verfahren ...“.

Auch die Zertifizierung von IT-Produkten nach Art. 5 nimmt auf die eigentlichen Forderungen des Datenschutzes welche durch ein zertifiziertes IT-Produkt zu erfüllen wären, kaum Bezug, sondern beschränkt sich auf die altbekannten Anforderungen (vgl. die Aufzählung in Art. 8 Abs. 1 VDSG) an Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der bearbeiteten Personendaten. Über derartige Eigenschaften dürfte die grosse Mehrheit der heute eingesetzten Softwareprodukte und Hardwarekomponenten verfügen. Diese Funktionen tragen jedoch nur in sehr beschränktem Umfang zur Umsetzung der Anforderungen aus dem Datenschutz im Sinne der Umschreibung nach Ziff. B/1.1 bei.

Wirklich datenschutzfördernd wäre dagegen die durch das zertifizierte IT-System unterstützte Wahrung des Zweckbindungsgebotes, z.B. mittels einer systemgestützten hierarchischen Zugriffs-Autorisierung; die automatisierte Kontrolle bzw. Beschränkung der Verknüpfung von verschiedenen Elementen einer Datenbank; die systemgestützte Kontrolle der Bekanntgabe von Personendaten an Dritte; die Unterstützung des IT-Anwenders bei der Erfüllung seiner Auskunftspflicht; Funktionen zur Umsetzung von Lösungs- und Berichtigungsansprüchen der betroffenen Personen, für das Einbringen eines Bestreitungsvermerks, oder die Benachrichtigung von Dritt-Empfängern über eine Berichtigung, Löschung oder Sperrung der Personendaten.

4.3 Erteilung und Gültigkeit der Datenschutzzertifizierung nach Art. 6 VE VDSZ

Der **erste Absatz** von Artikel 6 VE VDSZ umschreibt möglicherweise die Voraussetzungen für die Erteilung der Datenschutzzertifizierung nicht ganz vollständig. Allenfalls sollte der Satz wie folgt lauten:

“ ... dass die datenschutzrechtlichen Anforderungen sowie die weiteren Anforderungen, die sich aus den Artikeln 4 und 5 und aus den Anhängen 1 und 2 ergeben, erfüllt werden.“

Der dritte Absatz von Artikel 6 VE VDSZ könnte in der Praxis zu erheblichen Problemen führen: Ein nicht triviales Softwarepaket, welches gemäss der u.E. zu engen Umschreibung ja einziger oder überwiegender Gegenstand der „Datenschutz-

Stellungnahme zum Erlass einer Verordnung über die Datenschutzzertifizierungen (VDSZ)

Zertifizierung“ ist, unterliegt bekanntlich in der Praxis sehr häufigen Veränderungen. Wenn nun bei jedem neuen Release eines zertifizierten Softwarepaketes die Zertifizierung nach dem Wortlaut von Art. 5 Absatz 3 Satz 2 VE VDSZ wiederholt werden müsste, wäre dies sowohl für den Anbieter des betreffenden IT-Produktes wie auch für die Zertifizierungsdienste-Anbieter mit einem sehr grossen Aufwand verbunden. Dieses Beispiel zeigt, dass die ganze Problematik der Datenschutz-Zertifizierung ein neues, auch international nicht erforschtes und erprobtes Gebiet ist und in der Praxis wohl viele zu lösende Probleme bieten wird.

4.4 Zur Mitteilung der Ergebnisse des Zertifizierungsverfahrens (Art. 8 VE VDSZ)

Art. 2 und Art. 8 VE VDSZ enthalten wichtige Bestimmungen über das Zusammenspiel von Akkreditierungsstelle, Zertifizierungsdiensteanbieter und EDÖB: Die Akkreditierungsstelle hat darüber zu wachen, dass die Bestimmungen der Akkreditierungs- und Bezeichnungsverordnung vom 17. Juni 1966 (SR 946.512) eingehalten werden - der EDÖB hat dafür zu sorgen, dass bei der Zertifizierung und der Vergebung von Datenschutz-Qualitätszeichen sowie bei den Nachkontrollen die Anforderungen des Datenschutzes berücksichtigt und umgesetzt werden.

Zu Absatz 1: Im Sinne der wirkungsvollen Umsetzung wäre zu fordern, dass nicht die zertifizierte Stelle, sondern die gemäss Art. 1 VE VDSZ akkreditierte **Zertifizierungsstelle** dem oder der Beauftragten bei Erteilung eines Datenschutz-Gütezeichens die Ergebnisse der Prüfung mitteilen. Nach dem jetzt vorliegenden Entwurf der VDSZ liegt es allein im Ermessen der zertifizierten Stelle, ob sie ein Datenschutz-Qualitätszeichen lediglich zu Marketing- und Werbezwecken oder zur Freistellung von der Pflicht zur Anmeldung registrierungspflichtiger Datensammlungen nach Art. 11a Absatz 5 Bst. (f) Rev DSG verwenden will.

Es könnte daher ein Anreiz für die Zertifizierungsstellen und gewisse IT-Anwender entstehen, ein Datenschutz-Qualitätszeichen in recht grosszügiger Art und Weise auch für nicht registrierungspflichtige Datensammlungen und Anwendungen zu vergeben bzw. zu erwerben, oder ein Qualitätszeichen zu erwerben, ohne dieses für die Freistellung von der Pflicht zur Anmeldung registrierungspflichtiger Datensammlungen zu nutzen, um sich unabhängig von jeder Kontrolle durch den oder die Beauftragte mit einem „Datenschutz-Gütesiegel“ zu schmücken.

Stellungnahme zum Erlass einer Verordnung über die Datenschutzzertifizierungen (VDSZ)

Wenn mit der Zertifizierung von Datenschutzmanagementsystemen wirklich eine allgemeine Anhebung des Datenschutzniveaus in der Schweiz angestrebt werden soll, dann muss u.E. der oder die Beauftragte von den Zertifizierungsstellen über sämtliche von ihnen vergebenen Datenschutz-Qualitätszeichen unterrichtet werden, unter Beilage des Bewertungsberichtes und der Zertifizierungsdokumente, denn sonst droht der Wildwuchs bei der Vergebung von Datenschutz -Qualitätszeichen, und diese könnten auf die Stufe unverbindlicher, von kommerziellen Anbieter vergebenen „Datenschutz-Labels“ herabsinken.

Zum bisherigen Absatz 2 (neu Absatz 5): Die vom SWICO eingesetzte Arbeitsgruppe erachten die im VE VDSZ vorgeschlagene Regelung aus folgenden Gründen als nicht zielführend und sogar geradezu lebensfremd: Wenn die Zertifizierungsstelle bei ihrer Kontrolltätigkeit nach Artikel 6 Abs. 2 VE VDSZ feststellt, dass die Zertifizierungsvoraussetzungen sich geändert haben, dann hat auf jeden Fall die Zertifizierungsstelle, und nicht die zertifizierte Stelle, den Beauftragten darüber zu informieren, sonst hängen die in Art. 2 und Art. 6 Abs. 2 VE VDSZ vorgesehenen Nachkontrollen in der Luft, und die Umsetzung der Ergebnisse dieser Nachkontrolle ist dem Ermessen der zertifizierten Stellen anheim gestellt.

Zu einem neuen 2. Absatz - Prüfung durch den EDÖB: Nach Auffassung der SWICO VDSZ Arbeitsgruppe sollte der oder dem Beauftragten durch die VDSZ die Möglichkeit eingeräumt werden, die ihm oder ihr gemeldeten **Bewertungsberichte und Zertifizierungsdokumente zu prüfen** und dazu gegebenenfalls gestützt auf Art. 27 Abs. 4, 29 Abs. 3 und Art. 31 Abs. 1 Bst. (f) eine **Empfehlung abzugeben**. Dieses Verfahren ist in Art. 31 Abs. 1 Bst. (f) Rev DSG ja ausdrücklich vorgesehen und sollte in der VDSZ entsprechend umgesetzt werden.

Denn in der Praxis dürfen die akkreditierten Zertifizierungsstellen (bei welchen es sich im Unterschied zum „Modell-Land Schleswig-Holstein“ eben nicht um das „Unabhängige Landeszentrum für Datenschutz“, d.h. um eine öffentliche Anstalt handelt, sondern um private, dem Gewinnstreben verpflichtete Unternehmen) verständlicherweise das Bestreben haben, gegen Verrechnung ihres Honorars und unter Optimierung des Zeit- und Ressourcen-Aufwandes möglichst viele Zertifikate zu vergeben.

Dieser voraussehbaren Tendenz ist durch das Prüfungsrecht des oder der Beauftragten entgegenzuwirken, weil sonst die von den Zertifizierungsstellen vergebenen „Datenschutz-Qualitätszeichen“ rasch zu wenig aussagekräftigen „Datenschutz-Labels“ herabsinken könnten. Datenschutz-Qualitätszeichen sollten von den Zertifizierungsstellen erst ausgegeben werden dürfen, wenn die Bewertungsberichte und die Zertifizierungsunterlagen durch den EDÖB im Hinblick auf die Einhaltung der Datenschutzvorschriften geprüft worden sind. Da in voraussehbarer Zukunft nicht damit zu rechnen ist,

Stellungnahme zum Erlass einer Verordnung über die Datenschutzzertifizierungen (VDSZ)

dass Datenschutz-Qualitätszeichen in grosser Zahl ausgegeben werden, ist eine solche Prüfung dem EDÖB und seinem Stab zumutbar.

Zu Absatz 3 - Veröffentlichung der Zertifizierungen: Darüber hinaus sollten die Zertifizierungsberichte und der Bewertungsbericht nicht lediglich dem oder der Beauftragten mitgeteilt und dort archiviert werden, sondern sie sind wie im europäischen „Modell-Land“ Schleswig-Holstein in vollständiger oder zusammengefasster Form (vgl. die auf der Webseite des ULD-SH publizierten „Kurzberichte“ oder „Kurzgutachten“ über durchgeführte Datenschutz-Audits und erteilte „Datenschutz-Gütesiegel“) online allgemein zugänglich zu machen. Im Weiteren sollte jede interessierte Person die Möglichkeit haben, vom EDÖB eine Kopie eines Bewertungsberichtes und/oder der Zertifizierungsunterlagen zu erhalten.

Die mit der Vergebung eines Datenschutz-Qualitätszeichens angestrebte Anhebung des Datenschutz-Niveaus wird vor allem dann erfüllt, wenn die betroffenen Personen in geeigneter Weise Kenntnis nehmen können, was hinter dem von einer zertifizierten Stelle bei ihrem öffentlichen Auftreten verwendeten Datenschutz-Qualitätszeichen wirklich steckt. Darüber hinaus bilden die vom ULD-SH publizierten Gutachten und Berichte über durchgeführte Datenschutz-Audits und Produkteprüfungen - vergleichbar den vom EDÖB auf seiner Webseite publizierten Ergebnisse seiner Abklärungen und Empfehlungen - eine äusserst wertvolle Quelle für die IT-Anwender und die Anbieter von IT-Produkten über Prüfungskriterien, Feststellungen und Empfehlungen zur Verbesserung des Datenschutzes bei den überprüften Anwendungen, Verfahren und IT-Produkten.

Im Sinne der vorstehenden Überlegungen wird folgende Formulierung von Art. 8 VDSZ vorgeschlagen:

Art. 8 Mitteilung und Prüfung der Ergebnisse des Zertifizierungsverfahrens

¹ Vor der Vergebung eines Datenschutz-Qualitätszeichens an die zertifizierten Stellen reichen die Zertifizierungsstellen der oder dem Beauftragten folgende Unterlagen zur Prüfung ein:

- a. Bewertungsbericht;
- b. Zertifizierungsdokumente

² Der oder die Beauftragte prüft aufgrund der mitgeteilten Unterlagen die Einhaltung der Vorschriften über den Datenschutz bei der Vergebung der Datenschutz-Qualitätszeichen und kann dazu innert 30 Tagen nach Einreichung der Unterlagen gemäss Artikel 27 Absatz 3 und 29 Absatz 2 DSG zusätzliche Auskünfte einholen oder Empfehlungen nach Artikel 27 Absatz 4 oder 29 Absatz 3 DSG abgeben. Nach Ablauf dieser Frist, oder nach schriftlicher Bestätigung des oder der Beauftragten über den

Stellungnahme zum Erlass einer Verordnung über die Datenschutzzertifizierungen (VDSZ)

Erhalt zusätzlicher Auskünfte oder die Erfüllung der Empfehlungen kann das Datenschutz-Qualitätszeichen erteilt werden.

³ Die oder der Beauftragte veröffentlicht eine Liste der zertifizierten Stellen sowie die Bewertungsberichte und Zertifizierungsdokumente in abgekürzter Form und macht diese online zugänglich. Die oder der Beauftragte erstellt auf Gesuch hin kostenlos Auszüge aus den Bewertungsberichten und Zertifizierungsdokumenten.

⁴ Wenn eine zertifizierte Stelle aufgrund der erfolgreich absolvierten Zertifizierung nach Artikel 4 von der Pflicht zur Anmeldung von Datensammlungen nach Art. 11a Absatz 5 Buchstabe f DSGVO befreit werden möchte, teilt sie dies der oder dem Beauftragten unter Verweis auf die Eintragung in der Liste der zertifizierten Stellen mit.

⁵ Stellt die Zertifizierungsstelle im Rahmen ihrer Kontrolltätigkeit nach Artikel 6 Absatz 2 wesentliche Änderungen der Zertifizierungsvoraussetzungen fest, beispielsweise betreffend die Erfüllung von Bedingungen oder Auflagen, so hat sie die oder den Beauftragten darüber zu informieren.

4.5 Zu Sistierung und Entzug der Zertifizierung (Art. 9 VE VDSZ)

Im ersten Absatz wäre gemäss der von der SWICO Arbeitsgruppe VDSZ vorgeschlagenen Verstärkung der Zusammenarbeit zwischen den Zertifizierungsstellen und dem EDÖB beizufügen, dass die Zertifizierungsstelle vor Entzug oder Sistierung einer Zertifizierung im Sinne von Art. 2 VE VDSZ eine Stellungnahme der oder des Beauftragten einholt.

Im dritten Absatz sollte der Schlussteil „... wenn ihm oder ihr die Zertifizierung nach Artikel 8 Absatz 1 mitgeteilt wurde.“ ersatzlos gestrichen werden, da nach der hier vorgeschlagenen Regelung sämtliche von den Zertifizierungsdiensteanbietern ausgegebenen Datenschutz-Qualitätszeichen dem EDÖB gemeldet werden müssen.

5.5 Zum Verfahren bei Aufsichtsmaßnahmen - Art. 2 und Art. 10 VE VDSZ

Die Aufsichtskompetenzen des EDÖB beschränken sich nach dem vorliegenden Entwurf für die VDSZ primär auf die nach Feststellung von Mängeln bei der zertifizierten Stelle zu treffenden Massnahmen. Es ist jedoch durchaus möglich, dass der EDÖB bei der Ausübung seiner Aufsichtstätigkeit nach Art. 27 oder 29 Rev. DSGVO auch **Mängel bei der Zertifizierungsstelle** feststellt. Diesbezüglich sollte die Kompetenzen des EDÖB in dem Sinne **verstärkt und erweitert** werden, dass der letzte Satz von Absatz 4 gestrichen und die Aufsichtskompetenzen des EDÖB in Bezug auf die Zertifizierungsstellen neu in einem **Absatz 5 von Art. 10 VDSZ** umschrieben werden:

⁵ Stellt der oder die Beauftragte bei der Aufsichtstätigkeit fest, dass eine Zertifizierungsstelle die ihr übertragenen Aufgaben nicht richtig erfüllt oder die ihr von der

Stellungnahme zum Erlass einer Verordnung über die Datenschutzzertifizierungen
(VDSZ)

oder dem Beauftragten erteilten Empfehlungen nicht befolgt, so informiert er oder sie die Schweizerische Akkreditierungsstelle darüber.

Im gleichen Sinne wäre **Art. 2 VE VDSZ** wie folgt zu ergänzen:

Die Schweizerische Akkreditierungsstelle zieht für das Akkreditierungsverfahren, die Nachkontrolle sowie die Suspendierung oder den Widerruf den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten oder die Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (den Beauftragten oder die Beauftragte) bei.
