



Deutsche Vereinigung
für Datenschutz e.V.

Gesetzentwürfe für ein Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen

**der Sächsischen Staatsregierung vom 02.04.2002 (LT-Drs. 3/6181),
künftig zitiert als RegE**

**und der PDS-Fraktion vom 08.05.2002 (LT-Drs. 3/6448),
künftig zitiert als PDSE**

Stellungnahme der DVD

Kiel, den 09.09.2001

Die Stellungnahme ist **thematisch gegliedert** und stellt die Vorschläge der Staatsregierung (RegE) und der PDS-Fraktion (PDSE) zu einzelnen Fragestellungen nebeneinander auf den Prüfstand.

Die Europäische Datenschutzrichtlinie (EU-DSRL vom 24.10.1995, Richtlinie 95/46/EG des Europäischen Parlaments und des Rates, ABl. EG Nr. L 281/31 v. 23.11.95) hätte nach deren Art. 32 Abs. 1 S. 1 bis Oktober 1998 umgesetzt werden müssen. Es zeugt nicht von besonderem Respekt vor dem Europarecht, vor dem Ziel der Verwirklichung eines einheitlichen Binnenmarktes und vor dem in Art. 33 SächsVerf garantierten und vom Bundesverfassungsgericht konkretisierten Grundrecht auf informationelle Selbstbestimmung (v.a. BVerfGE 65, 1 ff. = NJW 1984, 419 ff.), dass sich der Sächsische Gesetzgeber erst mehr als **drei Jahre nach Fristablauf** anschickt, die nötigen gesetzgeberischen Änderungen vorzunehmen.

Zielsetzung einer aktuellen Neuregelung des allgemeinen Datenschutzrechtes darf es nicht nur sein, die zwingenden europäischen Vorgaben umzusetzen. Weiteres Ziel sollte, ja muss es sein, den neuen rechtstatsächlichen Gegebenheiten bei der Umsetzung des Rechts auf informationelle Selbstbestimmung gerecht zu werden. Im Vordergrund steht dabei insbesondere eine Abwendung von der ausschließlichen ordnungsrechtlichen Orientierung hin zur Nutzung marktwirtschaftlicher Instrumente und zur Stärkung der Selbstregulierung durch die Daten verarbeitenden Stellen bzw. des Selbstschutzes durch die Betroffenen. Weiterhin muss den neuen technischen Gegebenheiten der Miniaturisierung der Datenverarbeitung, der globalen Vernetzung sowie der "intelligenten" Auswertbarkeit Rechnung getragen werden sowie den absehbaren weiteren technischen Entwicklungen. Ohne eine solche Anpassung wird nicht die Akzeptanz bei den Bürgern und ein moderner Regelungsrahmen entstehen können, der für eine erfolgreiche Nutzung des Internet für E-Government und E-Commerce nötig ist. Es ist inzwischen unter Wissenschaftlern und Praktikern unbestritten, dass **Datenschutzgesetze der Dritten Generation** zugleich eine starke Verbesserung hinsichtlich der Verständlichkeit und einer Vereinfachung (Reduzierung komplexer Regelung) bedürfen, um von Betroffenen, Anwendern wie von der Öffentlichkeit verstanden und umgesetzt werden zu können (dazu Bäumler/v. Mutius, Datenschutzgesetze der Dritten Generation, 1999).

Zu den einzelnen Regelungen:

Änderung der Verfassung des Freistaates Sachsen

Der PDSE sieht eine Änderung des Art. 57 der Verfassung des Freistaates Sachsen vor, in der das Recht auf informationelle Selbstbestimmung sowie detailliert die Unabhängigkeit einer **“Landeskrollstelle für den Datenschutz”** (LfD) normiert werden. Die präzise verfassungsrechtliche Absicherung der LfD ist auf Grund der aktuellen Bestrebungen im Landes, deren Unabhängigkeit und deren Handlungsmöglichkeiten einzuschränken, nachzuvollziehen. Sie erscheint aber angesichts der Erfahrungen in den anderen Bundesländern nicht erforderlich, wo für eine ausreichende Absicherung der Funktionsfähigkeit der Landesbeauftragten für den Datenschutz eine einfachgesetzliche Ausgestaltung genügt. Sowohl die derzeitige Regelung, wonach der SächsDSB beim Landtag berufen wird, wie auch die geplante Regelung des Art. 57 Abs. 6 des PDS-Entwurfes, wonach die Dienstaufsicht beim Landtagspräsidenten angesiedelt wird, stellen vielleicht nicht zwingend, aber doch tendenziell die Wahrnehmung der hoheitlichen Aufgaben nach § 38 BDSG (Datenschutzaufsicht im nicht-öffentlichen Bereich) in Frage.

Änderung des Sächsischen Datenschutzgesetzes (SächsDSG)

Bei einer umfassenden Neugestaltung des Datenschutzrechtes nach der o.g. Konzeption eines Datenschutzgesetzes der Dritten Generation wäre eine vollständige Neuregelung, wie sie der RegE, nicht aber der PDSE enthält, vorzuziehen.

Zweck des Gesetzes

Es wäre wünschenswert, ohne dass dies dringend nötig wäre, wenn neben der Erwähnung des Rechts auf informationelle Selbstbestimmung ein genereller Bezug auf die **Grundrechte** als Gesetzeszweck erfolgen würde, da eine Vielzahl dieser Grundrechte einen informationellen Bezug haben und daher im Rahmen des Schutzes informationeller Selbstbestimmung mit berücksichtigt und mit geschützt werden müssen (z.B. Telekommunikationsgeheimnis, Schutz der Wohnung, politische Freiheitsrechte, Pressefreiheit, Religionsfreiheit; zu allem Weichert in Kilian/Heussen, Computerrechts-Handbuch, 1993, 130 Rdn. 45 ff.).

Die bisher in § 1 SächsDSG erfolgende Bezugnahme auf das **Persönlichkeitsrecht** ist möglich, sie ist aber nicht so umfassend wie eine Verweisung auf den gesamten Grundrechtsbestand.

Anwendungsbereich

Die in § 2 Abs. 3 RegE vorgesehene vollständige Ausnahme von öffentlich-rechtlichen **Wettbewerbsunternehmen** aus dem Geltungsbereich des SächsDSG ist nicht sinnvoll, da dadurch die Grenzlinie der Datenschutzaufsicht zwischen öffentlichem und privatem Bereich unklar wird, insbesondere wenn Unternehmen sowohl im Wettbewerb tätig sind als auch Verwaltungsaufgaben wahrnehmen. Die bisher geltende Regelung des § 2 Abs. 3 SächsDSG ist vorzugswürdig, die eine Geltung des BDSG nur vorsieht, “soweit” eine Teilnahme am Wettbewerb erfolgt (ebenso die meisten sonstigen Länder). Dies hat zudem zur Folge, dass die Mitarbeiter-Datenverarbeitung nach dem SächsDSG erfolgt.

Vorzugswürdig wäre zudem eine Beschränkung der Anwendbarkeit lediglich auf die materiell-rechtlichen Regelungen des BDSG und die Belassung der Kontrollzuständigkeit beim Sächsischen Datenschutzbeauftragten (SächsDSB), da anderenfalls für eine Stelle u.U. zwei Datenschutzkontrollinstanzen (SächsDSB und Aufsichtsbehörde nach § 38 BDSG) zuständig sein könnten.

Die in § 2 Abs. 2 PDSE vorgesehene Klarstellung zur **Vereinigungen des Privatrechtes** mit einer absoluten Anteilsmehrheit öffentlicher Stellen entspricht den Regelungen anderer Länder und ist zu begrüßen.

Begriffsbestimmungen

Der in § 3 Abs. 6 RegE wie in § 3 Abs. 6 SächsDSG enthaltene **Verweis auf Bild- und Tonträger** ist angesichts der heutigen Möglichkeiten der digitalen Datenauswertung von Bildern und Tonaufzeichnungen eher verwirrend als klarstellend und sollte gestrichen werden.

Systemwidrig und widersprüchlich ist es in § 3 Abs. 6 RegE, Datenträger, "soweit sie nicht im Sinne von Absatz 5 automatisiert verarbeitet werden" als Akten zu definieren, wenn dann auch noch in § 3 Abs. 7 Nr. 2 RegE **nicht-automatisierte Verarbeitungsformen** als Datei definiert werden. Die in der Begründung hierfür gegebene Erklärung, man wolle den Dateibegriff zurückdrängen, ist nicht plausibel, so lange auf den Aktenbegriff - im SächsDSG wie im RegE - materiellrechtliche Regelungen Bezug nehmen. Völlig unlogisch ist es, dem Aktenbegriff den Begriff der "automatisierten Verarbeitung" entgegenzusetzen. Dies hat zur Folge, dass das Datenschutzniveau bei konventionellen Dateien auf das von Aktenverarbeitung gesenkt wird. Völlig falsch ist der Verweis auf das europäische Recht, wo in Art. 2 c) EU-DSRL der Dateibegriff gerade extensiv definiert wird und weit in die bisherige Aktenverarbeitung hineinwirkt, während der hier genutzte Begriff der "automatisierten Verarbeitung" eine europarechtsunverträgliche Ausweitung des Aktenbegriffs zur Folge hat.

Es wäre sehr zu begrüßen, wenn Regelungen zur "**Verschlüsselung**", zur "**Pseudonymisierung**" personenbezogener Daten sowie zu "**mobilen personenbezogenen Datenspeicher- und Verarbeitungsmedien**" aufgenommen würden, so wie dies in § 3 PDSE vorgesehen ist. Dabei handelt es sich um drei regelungsbedürftige technische Erscheinungen mit hoher datenschutzrechtlicher und -praktischer Relevanz. Die in § 3 PDSE vorgeschlagenen Begriffsbestimmungen entsprechen denen anderer moderner Datenschutzgesetze. Dies gilt für das Verschlüsseln (§ 2 Abs. 2 Nr. 8 LDSG SH), das Pseudonymisieren (§ 2 Abs. 2 Nr. 7 LDSG SH, ungeschickt dagegen § 3 Abs. 6a BDSG) und mobile Verarbeitungsmedien (§ 3 Abs. 10 BDSG, § 18 Abs. 1 LDSG SH).

Datenvermeidung und Datensparsamkeit, Datenschutzaudit

Die in § 3a PDSE vorgesehene Regelung zu **Datenvermeidung und Datensparsamkeit** sowie zum Datenschutzaudit entspricht dem aktuellen Stand der wissenschaftlichen Diskussion wie auch praktischen Bedürfnissen. Sie folgt den Regelungen des Bundes (§§ 3a, 9a BDSG) und anderer Länder (§§ 4, 43 Abs. 2 LDSG SH). In § 3a Abs. 2 S. 2 sollte das Wort "dabei" gestrichen werden, da es überflüssig ist und unklar bleibt, worauf es sich bezieht.

Nachhaltig unterstützt wird der Vorschlag, das **Datenschutzaudit durch Satzung** zu regeln, da eine solche Regelungskonzeption mehr Flexibilität zulässt als ein besonderes Auditgesetz. Die in Schleswig-Holstein damit gesammelten Erfahrungen sind bisher durchgängig positiv und belegen (§§ 4 Abs. 2, 43 Abs. 2 LDSG), dass Datenschutz als positiver Wettbewerbsfaktor genutzt werden kann.

Verarbeitung sensibler Daten

Es sollte erwogen werden, in die Erlaubnis zur Verarbeitung sensibler Daten (§ 4 Abs. 2 RegE, § 4 Abs. 4 PDSE) zugleich eine Offenbarungsbefugnis nach § 203 StGB zu integrieren, so wie dies z.B. in § 11 Abs. 3 LDSG SH erfolgt ist. Dadurch wird die Zwei-Schranken-Prüfung bei Daten, die einem **besonderen Berufs- oder Amtsgeheimnis** unterliegen, vereinfacht.

Einwilligung

Es ist ausdrücklich zu begrüßen, dass die Einwilligung auch in **elektronischer Form** zugelassen werden soll (§ 4 Abs. 5 RegE). Systemwidrig ist das Verbot der Einwilligung mit einem Pseudonym (§ 4 Abs. 5 S. 2 RegE). Da der RegE keine Regelung zur pseudonymen Datenverarbeitung enthält, bleibt ungeklärt, ob diese überhaupt unter den Anwendungsbereich des SächsDSG fallen soll. Würde dies verneint, so machte das Verbot der pseudonymen Einwilligung überhaupt keinen Sinn. Bejahte man jedoch die Anwendbarkeit des SächsDSG bei pseudonymer Datenverarbeitung, so schlosse der Regelungsvorschlag die im Interesse der Datensparsamkeit wünschenswerte pseudonyme Datenverarbeitung durch die restriktive Einwilligungsregelung teilweise aus bzw. zwänge - lediglich zur materiellen Zulassung der Datenverarbeitung durch Einholung der Einwilligung - zur (rechtstatsächlich wie technisch) unnötigen Aufdeckung des Pseudonyms.

Erforderlichkeit der Datenverarbeitung- Aktentrennung

Die in § 4a PDSE enthaltene Regelung zur Erforderlichkeit der Datenverarbeitung ist als ausdrückliche Bestätigung des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes eigentlich überflüssig. Sie kann aber als klarstellende Regelung für die Bediensteten öffentlicher Stellen eine relevante Erinnerungsfunktion erfüllen. Sehr zu begrüßen ist die Regelung zur Organisation der Datenverarbeitung, **getrennt nach Zwecken und Betroffenen** (§ 4a Abs. 2 PDSE), da diese technisch-organisatorische Pflicht in der Praxis oft nicht beachtet wird.

Datenverarbeitung im Auftrag, Wartungsarbeiten

Die in § 7 Abs. 5 PDSE geplante Regelung zu **beratenden und begutachtenden Tätigkeiten** füllt eine rechtliche Lücke. Bei einer Beauftragung, die sich nicht auf Hilfstätigkeiten bei der Datenverarbeitung beschränkt, ist nach bisher geltendem Recht eine hierfür nötige Datenweitergabe (= Übermittlung) nicht zulässig. So erfolgt z.B. bisher die Übermittlung von Daten nach Einschaltung eines beratenden Rechtsanwaltes oder eines externen Organisationsgutachters ohne erkennbare Rechtsgrundlage. Die praktische

Notwendigkeit solcher Aufträge als moderne und kostensparende Outsourcing-Maßnahmen liegt auf der Hand. Der dem § 17 Abs. 5 LDSG SH nachempfundene Regelungsvorschlag sieht die bei dieser Form der Beauftragung nötigen Sicherheitsvorkehrungen vor.

Die Einbeziehung von **Wartungsarbeiten** und von vergleichbaren Unterstützungstätigkeiten bei der Datenverarbeitung (§ 7 Abs. 5 RegE, § 7 Abs. 6 PDSE) entspricht dem inzwischen auch im Bundesrecht und in sonstigem Landesrecht eingeführten Standard. Verzichtet man auf eine Regelung zur Datensparsamkeit (so nicht § 3a PDSE), so bietet es sich im Interesse einer Erhöhung der Datensicherheit an, den Datenzugriff für Wartungszwecke darauf zu beschränken, "dass ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann" (so ausdrücklich § 11 Abs. 5 BDSG), etwa durch Verschlüsselung der gespeicherten Personendaten.

Die in § 7 Abs. 1 S. 2 RegE geplante gleichrangige datenschutzrechtliche **Verantwortlichkeit des Auftragnehmers** neben dem Auftraggeber trägt nicht zur Rechtsklarheit bei. So ist unklar, ob und inwieweit der Auftragnehmer verantwortlich ist für die materiell-rechtliche Zulässigkeit der Datenverarbeitung oder bei der Wahrnehmung von Betroffenenrechten. Unklar ist die Rechtslage auch, wenn angesichts der gemeinsamen Verantwortlichkeit von Auftragnehmer und Auftraggeber sich widersprechende Handlungen vorgenommen werden. Einzuräumen ist zu Gunsten der unüblichen Regelung, dass sie die oft bestehende Dominanz des Auftragnehmers und dessen sich darauf ergebende faktische Verantwortlichkeit reflektiert.

Automatisiertes Abrufverfahren, Unterrichtungspflicht

Vor einer pauschalen, fast **voraussetzungslosen Zulassung von automatisierten Abrufverfahren**, wie sie § 8 Abs. 1 u. 2 RegE vorsieht, ist dringend abzuraten. Sie hätte zwangsläufig zur Folge, dass im Interesse angeblicher Synergieeffekte und Rationalisierungsgewinne gegenseitige Datenzugriffe eingeräumt würden, ohne dass hierüber ein Überblick oder auch nur eine Kontrolle bestünde. Es könnte nicht mehr festgestellt werden, welches die jeweils für ein Datum verantwortliche Stelle ist. Es mag angebracht sein, die bisher in § 8 Abs. 1 SächsDSG enthaltenen hohen formellen Anforderungen an die Einrichtung automatisierter Abrufverfahren (Gesetzesvorbehalt) zu lockern. Dies kann aber nicht zur vollständigen Regelfreiheit führen. Die geplante Norm dürfte wegen Unbestimmtheit bzw. wegen des Fehlens organisatorischer und verfahrensrechtlicher Vorkehrungen verfassungswidrig sein (vgl. BVerfG NJW 1984, 419, 422 ff., 425).

So bedarf es neben einer möglichen materiellen Präzisierung der Angemessenheit (z.B. Vielzahl der Übermittlungersuchen, Eilbedürftigkeit, Schutz besonders sensibler Daten) vor allem **verfahrensrechtlicher Sicherungen**. Diese können in der Präzisierung des Normcharakters der Zulassung (Rechtsverordnung, Anordnung durch oberste Landesbehörde, schriftliche Festlegung - so § 8 Abs. 2 S. 2 SächsDSG), in besonderen Beteiligungserfordernissen, z.B. Unterrichtung des SächsDSB (so § 8 Abs. 3 SächsDSG, § 8b Abs. 1 S. 1 PDSE) sowie in spezifischen Revisionsregelungen bestehen. Ungenügend ist die gesetzliche Forderung, "dass die Zulässigkeit der Übermittlung ... zumindest stichprobenweise überprüft werden kann". Abgesehen von wenigen Ausnahmen (z.B. polizeiliche Abrufe anlässlich von Personenkontrollen) kann nur eine Vollprotokollierung sämtlicher Abrufe im Interesse der Revisionsfestigkeit der Datenverarbeitung ausreichend sein. Eine Stichprobenprotokollierung genügt nicht. Außerdem genügt nicht die Möglichkeit

eine nachträglichen Überprüfung der Zulässigkeit; vielmehr muss eine tatsächliche Kontrolle gewährleistet werden.

Vorabkontrolle

Der Regelungsvorschlag in § 10 Abs. 5 RegE i.V.m. § 11 Abs. 3 Nr. 4 RegE genügt gerade den Mindestanforderungen des Art. 20 EU-DSRL an eine Vorabkontrolle. Unklar ist der Regelungsvorschlag in § 8b Abs. 3 PDSE bzgl. der **Zuständigkeit für die Vorabkontrolle**. Diese kann danach, muss aber nicht von der LfD vorgenommen werden. Ob eine Freigabe zwingend ist, ergibt sich nicht eindeutig, ebenso wenig, wer diese vorzunehmen hat, wenn die LfD innerhalb der Frist nicht tätig wird. Aus § 11a Abs. 5 Nr. 1 PDSE ist zu schließen (“hinzuwirken”), dass die Freigabe (= Vorabkontrolle) - entgegen Art. 20 Abs. 2 EU-DSRL - nicht vom behördlichen Datenschutzbeauftragten durchgeführt werden soll.

Gewährleistung des Datenschutzes (technisch-organisatorische Maßnahmen)

Die in § 9 SächsDSG geregelten und von § 9 RegE weitestgehend übernommenen Vorschriften zur allgemeinen **Datensicherheit** entsprechen nicht mehr dem aktuellen Stand der Technik und der wissenschaftlichen Diskussion. Zwar wird in § 9 Abs. 2 Nr. 10 RegE als weitere Maßnahme die Verfügbarkeitskontrolle aufgenommen. Es bleiben aber z.B. Fragen der Revisionssicherheit (vgl. § 9 Abs. 2 Nr. 6 RegE) völlig unzureichend geregelt. Statt des umfangreichen und unsystematischen Maßnahmenkatalogs hat es sich in modernen Datenschutzgesetzen durchgesetzt, lediglich die Ziele der Datensicherung zu definieren (vorbildlich § 10 DSGVO NRW, vgl. § 5 Abs. 1 LDSG SH). Überhaupt nicht nachvollziehbar ist, welche Funktion weiterhin die gesonderte Aktenregelung des § 9 Abs. 4 SächsDSG (= § 9 Abs. 4 RegE) erfüllen soll.

Besondere Maßnahmen zur Gewährleistung des Datenschutzes beim Einsatz automatisierter Verfahren

Sehr zu begrüßen sind die in § 9a PDSE geregelten **zusätzlichen Sicherungsmaßnahmen** bei besonders riskanten automatisierten Verarbeitungsverfahren. Diese von § 6 LDSG SH übernommene Regelung hat sich in Schleswig-Holstein als präzisierende Vorgabe für die Verwaltung bestens bewährt.

Datei-, Verfahrens- und Geräteverzeichnis

Der aus § 10 SächsDSG in § 10 Abs. 2 Nr. 2 PDSE und in der Überschrift des § 10 PDSE übernommene Begriff des **Dateiverzeichnisses** sollte zugunsten des umfassenderen Begriffs des Verfahrenszeichnisses ersatzlos wegfallen. Es hat sich als zu bürokratisch und technisch nicht umsetzbar erwiesen, sämtliche eigenständigen Dateien den bisherigen hohen Dokumentationsanforderungen auszusetzen. Deren Zusammenfassung zu nach Stelle, Zweck und Rechtsgrundlage definierten “Verfahren” genügt den datenschutzrechtlichen Dokumentationsanforderungen. Zwar leidet der Verfahrensbegriff an einer gewissen Unbestimmtheit. In der Praxis anderer Länder hat sich aber anhand dieses Begriffs eine befriedigende Praxis herausgeschält.

Eine hohe bürokratische Hürde ohne erkennbaren datenschutzrechtlichen Gewinn liegt auch im **Geräteverzeichnis** nach § 10 Abs. 2 Nr. 12 PDSE. Das Führen solcher Verzeichnisse im Interesse einer wirtschaftlichen Haushaltsführung ist hiervon unberührt.

Behördliche Datenschutzbeauftragte

Die **fakultative Regelung** zu behördlichen Datenschutzbeauftragten (bDSB, § 11 Abs. 1 RegE, § 11a PDSE) macht für kleine Stellen Sinn. Auf Grund der Erfahrungen in Schleswig-Holstein, wo selbst bei sehr großen Einrichtungen auf eine Bestellung verzichtet wird, sollte dort eine Pflicht zur Bestellung vorgesehen werden (so § 11a Abs. 1 S. 2 PDSE).

Dringend abzuraten ist von der Regelung, dass der Datenschutzbeauftragte nicht Beschäftigter einer öffentlichen Stelle sein muss (§ 11 Abs. 1 S. 3 RegE). Das Instrument des **externen Datenschutzbeauftragten** gibt es bisher vor allem im nicht-öffentlichen Bereich. Dort macht diese Konstruktion Probleme, wenn der externe bDSB Datenverarbeitung kontrollieren soll, die einem besonderen Berufsgeheimnis unterliegt. Hierzu wäre er als Externer nach § 203 Abs. 1 StGB nicht befugt, wohl aber als interne Hilfsperson (§ 203 Abs. 3 StGB). Es ist daher auch anzuraten, entgegen § 11a Abs. 4 S. 2 PDSE dem bDSB **Einblick in besondere Amts- und Berufsgeheimnisse** zu geben. Eine sanktionierbare Pflicht zur Geheimhaltung (vgl. § 11a Abs. 2 S. 3 PDSE, § 11 Abs. 4 RegE) besteht auch für Hilfspersonen i.S.v. § 203 Abs. 3 StGB. Gegen die Beschäftigung externer bDSB spricht zudem, dass Externe zumeist nicht die notwendige Verwaltungskennntnis haben, um in der Verwaltung wirksam Datenschutz zu realisieren.

Erhebung bei Dritten, Zweckänderung

Der bisher bestehende (§ 11 Abs. 4 SächsDSG) Katalog, der mögliche Erhebungen und Zweckänderungen (§ 12 Abs. 2 Nr. 1) erlaubt, wird in § 12 Abs. 4 RegE (bzw. § 13 Abs. 2 Nr. 1 RegE) inhaltlich unverändert übernommen. Engere Regelungen anderer Länder haben sich auch als praktikabel erwiesen (z.B. § 13 Abs. 3 LDSG SH). In jedem Fall sollte auf die Regelung verzichtet werden, nach der eine Zweckänderung bzw. eine Erhebung nicht beim Betroffenen wegen **unverhältnismäßigem Aufwand** erlaubt wird (§ 12 Abs. 4 Nr. 8 RegE). Eine solche Regelung eröffnet der Verwaltung Tür und Tor, vom Grundsatz der Erhebung beim Betroffenen abzuweichen.

Die Zulassung einer Zweckänderung “zu **historischen oder statistischen Zwecken**” in § 13 Abs. 2 Nr. 4. RegE ist sprachlich verunglückt. Es ist nicht erkennbar, weshalb sonstige Nutzungen “zur Durchführung wissenschaftlicher Forschung” (so bisher § 12 Abs. 2 Nr. 4 SächsDSG) künftig nicht mehr erlaubt sein sollen.

Verbot automatisierter Einzelentscheidungen

Weiter als in § 12a PDSE werden in § 34 RegE Ausnahmen vom Verbot automatisierter Einzelentscheidungen zugelassen. Ich halte es für nicht wünschenswert, dass schon auf Grund einer **einfachen Rechtsvorschrift** (z.B. Rechtsverordnung, Satzung) von diesem Verbot abgewichen werden können soll.

Übermittlung an öffentlich-rechtliche Religionsgesellschaften

Auf die aus § 14 SächsDSG in § 15 RegE übernommene Regelung zur Datenübermittlung an Religionsgesellschaften kann - wie unter Nr. 19 vom PDSE vorgeschlagen - **ersatzlos verzichtet** werden. Soweit spezifische Übermittlungen, z.B. aus dem Melderegister, erfolgen sollen, müssen diese bereichsspezifisch geregelt werden. Derartige Bereichsregelungen bestehen. Für eine allgemeine Regelung besteht weder eine praktische Notwendigkeit noch eine normative Rechtfertigung.

Übermittlung an nicht-öffentliche Stellen

Nach der von § 15 Abs. 1 Nr. 2 SächsDSG in § 16 Abs. 1 Nr. 2 RegE übernommenen Regelung soll schon ein **berechtigtes Interesse** eine Datenübermittlung an Private rechtfertigen. Dabei kann es sich um jedes von der Rechtsordnung gebilligte ideelle, soziale, kulturelle oder wirtschaftliche Interesse handeln (Dammann in Simitis u.a., BDSG, § 16 Rdn. 17; Schaffland/Wiltfang, BDSG, § 16 Rdn. 13, § 28 Rdn. 85). Ein "rechtliches Interesse", also ein Bezug auf die Rechtsstellung des Datenempfängers, wird nicht gefordert (Ancot, SächsDSG 1993, § 15 Rdn. 3). Eine solche Nutzungsmöglichkeit macht öffentliche Stellen zu Informationsquellen für Private, ohne dass die Betroffenen einen genügenden Schutz genießen würden. Der Verweis auf die schutzwürdigen Interessen des Betroffenen ist wenig hilfreich, solange nicht sichergestellt ist, dass der Betroffene vorab über die geplante Übermittlung benachrichtigt wird. Daher wird dringend empfohlen, entsprechend den Regelungen in anderen Ländern (z.B. § 15 Abs. 1 Nr. 1 LDSG SH) für ein fremdnützige Übermittlung an Dritte ein "rechtliches Interesse" zu verlangen.

Übermittlung ins Ausland

§ 16 PDSE genügt nicht den differenzierten Anforderungen an die Datenübermittlung ins Ausland der Art. 25, 26 EU-DSRL, insbesondere da die Regelung keine Differenzierung zwischen einer **Übermittlung innerhalb der Europäischen Union** (vgl. Art. 1 Abs. 2 EU-DSRL) und so gen. Drittländern vornimmt. Die relativ schlanke Regelung des § 17 RegE genügt dagegen den europarechtlichen Anforderungen.

Auskunft

In § 18 Abs. 5 Nr. 3 RegE wird die **Auskunftsverweigerung** erlaubt, wenn die personenbezogenen Daten des Betroffenen "ihrem Wesen nach ... geheim gehalten werden müssen". Diese Regelung ist zu unbestimmt. Es sind keine Sachverhalte vorstellbar, die eine Auskunftsverweigerung rechtfertigen und nicht durch die anderen Tatbestandsalternativen (öffentliche Sicherheit, Straf- oder OWiG-Verfolgung, Rechtsvorschrift, überwiegende berechnigte Interessen Dritter) abgedeckt wären. Andere Gesetze kommen ohne diesen Rechtsbegriff aus (z.B. § 27 Abs. 3 LDSG SH).

Berichtigung

Im Fall der Berichtigung ist eine unverzügliche Mitteilung bei den Datenempfängern vorgesehen. Während § 18 Abs. 2 PDSE nur dann eine Ausnahme von dieser Benachrichtigungspflicht zulässt, “wenn sie nachweislich einen unverhältnismäßigen Aufwand erfordern würde und durch das Unterlassen der Mitteilung schutzwürdige Belange der Betroffenen nicht berührt werden”, soll es nach § 19 Abs. 2 RegE genügen, dass sich die Benachrichtigung als unmöglich erweist oder einen unverhältnismäßig hohen Aufwand erfordert. Der Verweis auf den Aufwand allein kann nicht den Verzicht auf die Benachrichtigung rechtfertigen. Zusätzlich muss in jedem Fall festgestellt werden, dass durch diesen Verzicht “**schutzwürdige Belange des Betroffenen** nicht beeinträchtigt werden” (so z.B. § 28 Abs. 5 S. 2 LDSG SH).

Löschung

§ 20 Abs. 2 RegE sieht bei der Löschungsverpflichtung eine **Sonderregelung für Akten** vor. Diese Pflicht soll erst entstehen, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist. Diese Regelung macht nur Sinn, wenn die Akten nicht trennbar sind. Anderenfalls müssen die allgemeinen Löschungsregelungen anwendbar bleiben (vgl. § 28 Abs. 2 S. 2 LDSG SH).

Schadensersatzpflicht

Während § 23 Abs. 1 RegE eine spezifische Schadensersatzpflicht nur bei unrichtiger und unzulässiger **automatisierter Datenverarbeitung** auslösen möchte, sieht § 21 Abs. 1 PDSE eine solche Pflicht vor, ohne dass eine automatisierte Verarbeitung erfolgt sein müsste. Aus Sicht des Betroffenen kann es nicht darauf ankommen, ob der Schaden auf einer automatisierten oder einer konventionellen Datenverarbeitung basiert. Daher ist der PDSE-Vorschlag vorzugswürdig.

Anrufung der Unabhängigen Landeskontrollstelle bzw. des Datenschutzbeauftragten

§ 22 Abs. 1 S. 2 PDSE stellt klar, dass auch **Beschäftigte öffentlicher Stellen** das Recht der Anrufung haben, “ohne dass der Dienstweg einzuhalten ist”. Angesichts der bei öffentlich Bediensteten insofern sehr weit verbreiteten Unsicherheit ist eine solche Klarstellung wünschenswert.

Es sollte darüber hinausgehend erwogen werden, ob ein diskriminierungsfreier Anrufungsrecht auch dann zugestanden werden soll, wenn jemand annimmt, “dass bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen datenschutzrechtliche Vorschriften verletzt wurden”, **ohne** dass der Petent **selbst** hiervon **betroffen** sein müsste (so z.B. § 40 S. 1 LDSG SH).

Sächsischer Datenschutzbeauftragter (SächsDSB) - Unabhängige Landeskontrollstelle für den Datenschutz (LfD)

Der **wichtigste Unterschied** zwischen dem RegE und dem PDSE liegt in der Regelung der Datenschutzaufsicht. Während sich der RegE am klassischen Beauftragtenmodell orientiert und hierbei gravierende Zuständigkeits- und Befugniseingrenzungen vornimmt, sieht der PDSE eine Ausweitung dieser Zuständigkeiten und Kompetenzen vor und schlägt als Organisationsform das Anstalts-Modell vor, das sich in Schleswig-Holstein seit einigen Jahren gut bewährt hat. Angesichts der sowohl quantitativen wie der qualitativen Bedeutung der Regelungsvorschläge des RegE irritiert dessen Begründung, wo auf S. 2 f der "wesentliche Inhalt des Entwurfs" zusammengefasst wird, ohne dass dabei auch nur eine Regelung zum Status des SächsDSB auch nur erwähnt würde.

Der **Name** "Unabhängige Landeskontrollstelle für den Datenschutz" ist insofern zu begrüßen, als er die Unabhängigkeit nach Art. 28 Abs. 2 EU-DSRL betont und die Terminologie "Kontrollstelle" der EU-DSRL übernimmt. Dennoch gibt dieser Begriff nur unzureichend die Funktion dieser Stelle wieder, die sich nicht in der repressiven Kontrolltätigkeit beschränkt, sondern ihren Schwerpunkt im Interesse eines vorgezogenen Datenschutzes in der Prävention setzen soll (§ 28a PDSE).

Hinsichtlich der **Organisationsform** wird unterschieden zwischen dem Hilfsorgan des Sächsischen Landtags (§ 25 Abs. 1 S. 1 RegE) und einer rechtsfähigen Anstalt des öffentlichen Rechts mit eigener Dienstherrenfähigkeit (§ 23 PDSE). Dem zweitgenannten Organisationsmodell ist der Vorzug zu geben, da nur auf diese Weise dem Datenschutzbeauftragten die exekutiven Aufgaben einer Datenschutzaufsichtsbehörde im nicht-öffentlichen Bereich nach § 38 BDSG zugewiesen werden können, so wie dies nach § 23 Abs. 2 PDSE möglich sein soll und in § 25 Abs. 3 PDSE ausdrücklich vorgesehen ist. Eine Konzentration des Datenschutzes von öffentlichem und nicht-öffentlichem Bereich in einer Hand ist im Interesse der Bürgerfreundlichkeit, erreichbarer Synergieeffekte, eines effektiven Mitteleinsatzes und wegen Zuständigkeitsüberschneidungen dringend geboten (ausführlich dazu Dronsch, DuD 1994, 612). Die in den Ländern Berlin, Bremen, Hamburg, Niedersachsen, Nordrhein-Westfalen und Schleswig-Holstein insofern gesammelten positiven Erfahrungen sind unbestritten und eindeutig.

Es erscheint aber rechtssystematisch problematisch, die **Dienst- und Rechtsaufsicht**, soweit hoheitliche Aufsichtstätigkeit gegenüber privater Datenverarbeitung erfolgt, dem Präsidenten des Landtages zu übertragen (§ 23 Abs. 1, 2 PDSE). Hoheitliche eingreifende Tätigkeit ist exekutives Handeln, das verfassungsrechtlich der Landesregierung zugewiesen ist. Die Zuweisung von Eingriffskompetenzen zu einer der Legislative zugewiesenen Anstalt des öffentlichen Rechts stellt eine Durchbrechung des Gewaltenteilungsgrundsatzes dar. Rechtssystematisch wie praktisch komplikationsfrei wäre dagegen eine Dienstaufsicht der Person des SächsDSB und eine Rechtsaufsicht gegenüber der hoheitlichen Datenschutzaufsicht im privaten Bereich durch den Ministerpräsidenten oder bzgl. der Rechtsaufsicht durch ein Ressortministerium, so wie dies in den § 35 Abs. 5, 38 LDSG SH geregelt ist.

Die Regelungen zur **Rechtsstellung** des SächsDSB im RegE sind, wird die organisatorische Zuordnung beim Landtag beibehalten, vom Wesen her vertretbar. Überflüssig erscheint die Befugnis zur Anzeigeerstattung bei datenschutzrechtlichen Ordnungswidrigkeiten und Straftaten (so auch § 25 Abs. 6 PDSE) sowie die Regelung, dass die durch das SächsDSG begründeten Rechte und Pflichten des SächsDSB nicht durch Abreden geändert werden können (§ 25 Abs. 8, 9 RegE). Derartiges ist in anderen Ländern eine ungeregelt bleibende Selbstverständlichkeit.

Die Regelung der **Kontrollkompetenzen** in § 27 RegE ist teilweise widersprüchlich, teilweise nicht praktikabel und teilweise verfassungswidrig. So sehr die Beschränkung der Kontrollkompetenzen durch den Konflikt zwischen dem derzeitigen SächsDSB und der Sächsischen Staatsregierung erklärt werden kann; gerechtfertigt ist sie deshalb nicht (vgl. DVD, DANA 1/2001, 36). Aus Regierungssicht sollte man froh sein, mit einer u.U. sehr misstrauischen Kontrollinstanz ein behördliches Frühwarnsystem zu haben, welches vor größerem politischen Schaden, als er durch öffentliche Kritik des SächsDSB entstehen kann, bewahren kann. Zu mehr als solcher Kritik ist ein Datenschutzbeauftragter nicht befugt. Die Souveränität einer Exekutive erweist sich nicht in der Einschränkung von Kontrollkompetenz, sondern in der öffentlichen Auseinandersetzung mit einer als unbegründet empfundenen Kritik. Auch wenn die Erfahrungen mit der in Einzelfällen etwas unkonventionellen Datenschutzkontrolle in Sachsen von Manchem als unerfreulich erlebt wird, so muss man zugestehen, dass sich die Kritik des SächsDSB zumeist als nicht unbegründet erwiesen hat. Es darf zudem nicht aus dem Auge verloren werden, dass dem SächsDSB keine Weisungs- oder Anordnungs-kompetenzen, sondern lediglich Kontroll- und Beanstandungskompetenzen zustehen.

Es ist widersprüchlich und zugleich nicht praktikabel, wenn dem SächsDSB eine Kontrollkompetenz bzgl. **Patientengeheimnissen** (ärztliche Schweigepflicht) in Dateien zugesprochen wird, wenn die Daten nicht zugleich in Akten gespeichert werden ("elektronische Patientenakte", § 27 Abs. 2 S. 2 RegE), nicht aber, wenn die Daten in Akten und in automatisierten Dateien mit Aktenrückhalt gespeichert sind. Geradezu absurd ist, dass wiederum eine Kontrolle nach § 27 Abs. 1 RegE möglich sein soll, wenn die Daten in konventionellen Dateien gespeichert sind, auch wenn diese Daten zugleich auch in Akten enthalten sind. Da diese Regelung wesentlich Gleiches ungleich behandelt, liegt hierin auch ein Verstoß gegen das Gleichheitsgebot des Art. 3 Abs. 1 GG bzw. des Art. 18 Abs. 1 SächsVerf.

Die Pflicht zur **Einholung einer Einwilligung** im Fall der Prüfung von Daten, "die dem Arztgeheimnis unterliegen, Personalakten einschließlich Disziplinarakten sowie Sicherheitsakten und Sicherheitsüberprüfungsakten" würde de facto in diesen Bereichen zu einem datenschutzkontrollfreien Raum führen, da der damit verbundene Verwaltungsaufwand gescheut würde und z.B. bei älteren Akten die Datenbeschaffung zur Kontaktierung und Einholung der Einwilligungen bei den Betroffenen oft unmöglich wäre. Im Ergebnis würde die geplante Regelung dazu führen, dass gerade in den Fällen eine informierte Einwilligung einzuholen praktisch unmöglich ist, in denen die Betroffenen besonders schutzbedürftig sind (geistig Kranke, Behinderte, alte Menschen), mit der Folge, dass keine Kontrollen möglich wären. Die Erfahrungen zeigen, dass gerade in diesen Bereichen ein besonders hoher Kontrollbedarf besteht, da derart Abhängige eher wenig behördliche oder sonstige Fürsprache finden.

Schon die Widerspruchsregelung in § 24 Abs. 2 BDSG gegen eine Datenschutzkontrolle, die sich auch auf Eingriffe in das Fernmeldegeheimnis, auf Personalakten und Sicherheitsüberprüfungsakten bezieht, hat sich als mit kaum überwindlichen **praktischen Schwierigkeiten** verbunden erwiesen (dazu ausführlich Weichert, CR 1994, 174). Dies hat zur Folge, dass der Widerspruchsregelung im Prüfgeschäft heute kaum eine praktische Relevanz zukommt. Die geplante Regelung als Einwilligungsregelung wird darüber hinausgehend Konflikte schaffen. Dem wird kein erkennbarer Nutzen, schon gar nicht für das Recht auf informationelle Selbstbestimmung, gegenüberstehen. Die erste nicht zu beantwortete Frage wird sein: Muss der SächsDSB oder die geprüfte Stelle die Einwilligung einholen? Wenn es der Erstere sein sollte, stellt sich die Frage, wie der SächsDSB Name und Adresse von Betroffenen erfahren soll, deren Akten er erst nach Erlangung der

Einwilligung prüfen können soll. Und wenn es die Letztere sein sollte: Welchen Aufwand erwartet man von einer zu prüfenden Stelle beim Bemühen um die Erlangung von Einwilligungen, die erst die Voraussetzung schaffen für die eigene Kontrolle? Noch viel heikler ist die Frage, wie bei einer Prüfung von Akten verfahren werden soll, wenn der SächsDSB im Rahmen einer Prüfung einer Akte plötzlich unerwarteterweise auf Patientengeheimnisse stößt. Nimmt er diese Daten dann tatsächlich zur Kenntnis, was kaum zu vermeiden ist, so ist nicht er sanktionierbar. Wohl aber wäre der Verantwortliche der geprüften Stelle nach § 203 Abs. 1 StGB strafbar, weil er eine unbefugte Geheimnisoffenbarung zugelassen hat. Die Konsequenz würde sein, dass Stellen Akten der Kontrolle entziehen mit der bloßen Behauptung, darin könnten sich Patientengeheimnisse befinden. Die gesetzliche Aufgabe des SächsDSB ist die eines Ombudsmanns für die Bürgerrechte der Betroffenen. Es wäre ein Konstruktionsfehler, gerade diesem zu unterstellen, er würde bei seiner Aufgabenwahrnehmung zum Schaden des Betroffenen tätig werden und er bedürfe daher nicht nur einer gesetzlichen (kollektiven), sondern einer individuellen Legitimation für seine Tätigkeit.

Dem gegenüber ist der Regelungsvorschlag des § 26 S. 3 PDSE zu unterstützen, wonach die LfD im Rahmen ihrer Kontrollen personenbezogene Daten auch **ohne Kenntnis der Betroffenen** erheben darf. Diese Rechtslage ist außerhalb von Sachsen eine solche Selbstverständlichkeit, dass sie keiner ausdrücklichen Erwähnung bedarf.

Geradezu wie eine Satire liest sich die Norm, dass niemand **benachteiligt oder gemaßregelt** werden dürfe, der in eine Kontrolle durch den SächsDSB einwilligt (§ 27 Abs. 2 S. 3 RegE). Eine solche Benachteiligung oder Maßregelung könnte allenfalls vom SächsDSB erfolgen, der hierfür auch nicht im Ansatz einen Anlass oder eine Gelegenheit haben kann.

Soweit bekannt weltweit einzigartig wäre die Regelung, dass der SächsDSB keine Kontrollkompetenz hat, "soweit der **Kernbereich exekutiver Eigenverantwortung** berührt ist" (§ 27 Abs. 3 RegE). Der Jurist muss erst noch gefunden werden, der mit nachvollziehbarer Begründung die Grenze zwischen kontrollfreiem Kernbereich und zu kontrollierendem Randbereich definiert. Die Regelung ist ein untauglicher Versuch am untauglichen Objekt: Wer meint, ein Aktenvermerk eines Staatsministers in einer zunächst politisch relativ irrelevanten Justizakte gehöre zum exekutiven Kernbereich, der möge erläutern, was dann nicht zum Kernbereich gehört (zum konkreten Fall vgl. DANA 4/2001, 26, 1/2001, 25). In einer demokratischen Republik nicht akzeptabel wäre eine "royalistische" Regelung, wonach der Ministerpräsident, dessen Ehefrau und die Minister von einer Datenschutzkontrolle frei gestellt würden. Das in der Begründung zum RegE (S. 23) erwähnte Zitat aus dem "Flick-Urteil" des BVerfG (BVerfGE 67, 139) legitimiert in keinem Fall die Annahme von demokratie- und kontrollfreiem Handeln, wenn damit Grundrechtseingriffe verbunden sind, so wie dies bei Eingriffen in das Grundrecht auf Datenschutz der Fall ist.

Wegen der praktischen großen Bedeutung und der insofern schon bestehenden "Vorbild"-Wirkung einer bayerischen Regelung (Art. 30 Abs. 4 BayDSG) soll vor einem Ausschluss der Datenschutzkontrolle in laufenden Strafverfahren gewarnt werden. Nach § 27 Abs. 6 RegE soll die Kontrolle der Datenverarbeitung bei der Verfolgung von Straftaten "erst **nach Abschluss des Strafverfahrens**" unterliegen. Das Strafverfahren mit den Eingriffsbefugnissen der Strafprozessordnung ist wohl das staatliche Instrument, mit welchem am weitesten in zivilisierten Staaten wie der Bundesrepublik Deutschland in Grundrechte und insbesondere in das Recht auf informationelle Selbstbestimmung eingegriffen werden kann. Einer gerichtlichen Kontrolle unterliegen diese Eingriffe nicht; nur in Einzelfällen (z.B. Telefonüberwachung, § 100b StPO) ist eine gerichtliche Anordnung vorgesehen. Eine gerichtliche Würdigung von Ermittlungseingriffen erfolgt allenfalls im Rahmen der Wertung des Beweisergebnisses und durch die Prüfung von

Verwertungsverboten in einem Endurteil. Angesichts dieser im Interesse der Funktionstüchtigkeit und Effektivität des Strafverfahrens bestehenden Rechtslage ist es um so dringender, dass eine unabhängige verwaltungsinterne Rechtskontrolle stattfinden kann. Um eine solche handelt es sich bei der Datenschutzkontrolle. Auch der Zeitpunkt des endgültigen Abschlusses des Strafverfahrens macht wenig Sinn, wenn es um den Schutz von Ermittlungsmaßnahmen gehen soll, da die relevanten Ermittlungsmaßnahmen vor der Erhebung der Anklage beendet sein müssen.

Als kontraproduktive reine Schikane muss die in § 28 Abs. 2 RegE vorgesehene Pflicht des SächsDSB angesehen werden, "den Leiter der betroffenen Stelle **vor Beginn einer Kontrolle** in deren Diensträumen zu **informieren**". Dies ist dann nicht möglich, wenn eine Prüfung dringend ist, aber der Leiter nicht erreichbar ist. Will man insofern - entgegen dem eigentlich eindeutigen Wortlaut der Regelung - auch die Information des Stellvertreters des Leiters genügen lassen, so ändert dies nichts daran, dass eine Stelle sich dadurch einer Prüfung entziehen könnte, dass sich deren Leitung als nicht ansprechbar erweist. Moderne Prüfansätze wie z.B. unangekündigte Kontrollen oder reine Nachschauen (z.B. in Aktenabfallcontainern) würden durch die Regelung verboten. Völlig unklar wäre, wie bei technischen Online-Prüfungen oder bei Prüfungen bei Auftragsdatenverarbeitern verfahren werden muss bzw. soll.

Die umfassende und effektive Kontrollkompetenz der unabhängigen Datenschutzkontrollinstanz ist nach Art. 28 EU-DSRL zwingendes **europäisches Recht**. Die im RegE vorgesehenen Einschränkungen sind in der EU-DSRL nicht vorgesehen und daher europarechtswidrig. Das in der Begründung zum RegE auf S. 23 vorgebrachte Gegenargument, Art. 28 Abs. 3 EU-DSRL gewähre nur ein Recht auf Zugang zu Daten, nicht aber "ein Recht auf unbeschränkten Zugang zu allen Daten", grenzt an Rabulistik. Weder in der Entstehungsgeschichte noch im Wortlaut der EU-DSRL war bzw. ist erkennbar, dass die Kontrollbefugnis auf bestimmte Daten ausgenommen werden könnte, und gar auf solche Daten, denen wegen ihrer Sensibilität ein besonderes Gefährdungspotenzial für das Recht auf informationelle Selbstbestimmung zukommt.

Die Beschränkungen verstoßen aber auch gegen **deutsches Verfassungsrecht**: "Wahrscheinlich lässt sich nur über das Verfahrensrecht verhindern, dass der Bereich zwischen Recht und Technik zum juristischen Niemandsland wird" (Simon, Heußner in BVerfGE 53, 76). Derartige "schützende Formen" hat das BVerfG als grundrechtssicherndes Verfahrensrecht zwingend aus dem Grundgesetz abgeleitet. Der Schutz des Persönlichkeitsrechtes bedarf organisatorischer und verfahrensrechtlicher Vorkehrungen (BVerfGE 65, 49 = NJW 1984, 425): "Wegen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen der automatisierten Datenverarbeitung und auch im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen ist die **Beteiligung unabhängiger Datenschutzbeauftragter** von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung" (BVerfGE 65, 46 = NJW 1984, 422 f.; dazu Simitis NJW 1984, 403). Insbesondere bei abgeschotteten Verfahren (wie z.B. der "strategischen Kontrolle" des Post- und Fernmeldeverkehrs durch den BND oder Sicherheitsüberprüfungen durch den Verfassungsschutz) sind verfahrensrechtliche Sicherungen, zu denen z.B. die Kontrollkompetenz des Bundesbeauftragten für den Datenschutz (BfD) gehört, verfassungsrechtlich geboten (BVerfGE 67, 185).

Eher als irrationale Reaktion auf unerquickliche Erfahrungen und weniger als eine vernünftig begründete Verfahrenssicherung muss der § 29 Abs. 4 RegE angesehen werden, wonach der SächsDSB, wenn er beabsichtigt sich "im Rahmen seiner gesetzlichen Zuständigkeiten **zu dem Verhalten einer öffentlichen Stelle zu äußern**, ohne dass es sich hierbei um eine

Beanstandung .. handelt", verpflichtet wird, "die betroffene öffentliche Stelle zu hören, bevor er die Äußerung einem anderen zugänglich macht". Dabei soll der SächsDSB sich "inhaltlich mit dem Vorbringen der öffentlichen Stelle auseinander"setzen müssen (Verweis auf § 29 Abs. 1 S. 3 RegE). Den öffentlichen Datenschutzbeauftragten in ihrer Funktion steht zwar ebenso wie sonstigen Beamten nicht das Grundrecht auf freie Meinungsäußerung zu. Aber man stelle sich vor, eine Regierung müsse erst die Stellungnahme der Opposition einholen, bevor sie eine öffentliche Äußerung von sich gibt, oder die Staatsanwaltschaft bei ihrer Pressearbeit bedürfe erst der Stellungnahme des Beschuldigten. Soll das deutsche System der öffentlichen Datenschutzkontrolle ohne jegliche finanzielle oder rechtlich wirkende Sanktion beibehalten werden, so kann dem Kontrolleur nicht sein stärkstes Schwert aus der Hand genommen werden: die öffentlich geäußerte Kritik. Es sollte eine Selbstverständlichkeit sein, dass ein SächsDSB versucht, vor einer öffentlichen Äußerung um einen Sachverhalt die "andere Seite" zu hören. Oft ist dies aber gar nicht möglich, etwa, weil im Rahmen eines Interviews ein Journalist eine Frage stellt, die der SächsDSB zwar beantworten könnte, die er aber zuvor der öffentlichen Stelle nicht zur Stellungnahme vorgelegt hat. Bei akuten datenschutzrechtlichen Gefahren, etwa, wenn bei der Nutzung eines öffentlichen Internet-Angebots für Tausende von Nutzenden ein Schaden entstehen kann, müsste der SächsDSB sehenden Auges diesen Schaden hinnehmen, bis der "betroffenen" öffentlichen Stelle angemessene Zeit und Möglichkeit zur Stellungnahme gegeben worden ist. Bei komplizierten Sachverhalten mag man gerade von einer besonders langen Reaktionszeit ausgehen? So wenig staatliche Funktionsträger für sich das Grundrecht auf Meinungsäußerungsfreiheit in Anspruch nehmen können, so wenig haben öffentliche Stellen einen persönlichkeitsrechtlichen Abwehranspruch. Die Möglichkeit der allgemeinen öffentlichen Gegenwehr mit entsprechenden Rechten steht der kritisierten Stelle jederzeit offen. Verblüffenderweise enthält der RegE keine Regelung, wonach öffentliche Stellen, die den SächsDSB in der Öffentlichkeit kritisieren wollen, zuvor dessen Stellungnahme einholen müssen. Es hat nichts mit "dem rechtsstaatlichen Gebot eines fairen Verfahrens" (so Begründung RegE S. 26) zu tun, wenn Datenschutzbeauftragten der Mund verboten wird.

Hinsichtlich der zusätzlich zu der klassischen Datenschutzkontrolle im öffentlichen Bereich dem SächsDSB obliegenden Aufgaben bewegt sich die Regelung des § 30 RegE im Rahmen des Üblichen.

Die darüber hinaus gehende Übertragung der Zuständigkeit für die **Datenschutzkontrolle im nicht-öffentlichen Bereich** (§ 25 Abs. 3, 4 PDSE) ist sehr zu unterstützen. Es muss jedoch beachtet werden, dass diese Tätigkeit aus Gründen der Gewaltenteilung nicht der Legislative zugeschlagen wird (dazu s.o. zur "Organisationsform").

Der Vorschlag in § 27 Abs. 2 PDSE, wonach die LfD das Recht hat, "gegenüber der Daten verarbeitenden Stelle das **vorläufige oder endgültige Verbot der Verarbeitung von Daten**", die unter Verstoß gegen Datenschutzrecht erfolgt, anzuordnen, wäre für das deutsche Datenschutzrecht im öffentlichen Bereich eine absolute Neuigkeit. Sie greift Art. 28 Abs. 3 3. Sp. EU-DSRL auf, die der Kontrollstelle "wirksame Einwirkungsbefugnisse, wie beispielsweise ... die Befugnis, die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen", zuspricht. Dessen ungeachtet ist von einer solchen Anordnungsbefugnis dringend abzuraten. Im öffentlichen Bereich hat sich die Beschränkung auf die öffentliche Beanstandungsmöglichkeit als wirksamer erwiesen, als es jede zwingende verwaltungsrechtliche Zwangsmaßnahme sein könnte. Insbesondere veranlasst sie die Beteiligten zu einem Diskurs mit dem Versuch der gegenseitigen Überzeugung und letztendlich mit dem Ziel einer gemeinsamen Lösungssuche. Dem gegenüber würden Anordnungen, verwaltungsgerichtliche Klagen hiergegen bzw. solche Klagen der Kontrollinstanz bei Missachtung einer Beanstandung (§ 28

PDSE) zwangsläufig den Konflikt zwischen verarbeitenden Stellen und Kontrollinstanz verschärfen. Regelmäßig genügt schon die theoretische Möglichkeit einer öffentlichen Darstellung eines Datenschutzverstoßes, um diesen für die Zukunft abzustellen. Es obliegt der Rechtsaufsicht der verarbeitenden Stelle sowie den politisch-parlamentarischen Kontrollinstanzen, insbesondere dem Landtag, gegenüber der verarbeitenden Stelle bei deren Widerspenstigkeit die Beachtung des Datenschutzrechtes durchzusetzen.

Sehr zu begrüßen sind die in § 28a PDSE vorgeschlagenen zusätzlichen **Serviceaufgaben** der LfD. Die Beratung und Information der Bürger erhöht deren Kompetenz zur Wahrnehmung ihres Rechtes auf informationelle Selbstbestimmung und zur Ergreifung von Selbstschutzmaßnahmen (§ 28a Abs. 1 PDSE). Dies gilt auch für die Durchführung von Fortbildungsveranstaltungen, die zugleich bei einer Adressierung an die Mitarbeiter der Verwaltung deren Bereitschaft zur Beachtung des Datenschutzrechtes erhöht (§ 28a Abs. 3 S. 1 PDSE). Die Möglichkeit für öffentliche Stellen, ihr Datenschutzkonzept prüfen und beurteilen zu lassen, die erstmals in Schleswig-Holstein mit § 43 Abs. 2 LDSG SH eingeführt wurde ("Behörden-Audit"), erfreut sich dort schon großer Zusprache (§ 28a Abs. 2 PDSE). Zu begrüßen ist weiterhin, dass die LfK die Möglichkeit eingeräumt bekommen soll, ihre Servicetätigkeit (auch Beratung von nicht-öffentlichen Stellen, § 28a Abs. 3 S. 2 PDSE) durch Entgelte zumindest teilweise zu refinanzieren. Dies stärkt das Verständnis, dass es sich bei Datenschutz nicht nur um Ordnungsrecht handelt, sondern auch um einen Akzeptanzfaktor beim Bürger bzw. um einen Wettbewerbsfaktor beim Kunden.

Videoüberwachung

Die Vorschläge zur Videoüberwachung entsprechen insofern dem üblichen Regelkonzept, als sie eine Hinweispflicht vorsehen (§ 33 Abs. 2 RegE, § 29a Abs. 1 S. 1 PDSE). Soll Videoüberwachung generell erlaubt werden, ist eine Regelung wenig ergiebig, die hinsichtlich der materiellen Zulässigkeit auf **ein weiteres Gesetz** verweist (so § 29a Abs. 1, 3 PDSE). Während § 29a Abs. 5 PDSE eine vertretbare **maximale Speicherfrist** von 7 Tagen vorsieht, sind die in § 33 Abs. 4 RegE genannten zwei Monate unverhältnismäßig lang.

Wissenschaftliche Forschung

Die Regelung des § 30 PDSE ist insofern äußerst forschungsfreundlich, als sie eine Privilegierung pseudonymisierter Datenverarbeitung (Abs. 1) und die Datenerhebung zum Zweck der Pseudonymisierung bzw. Anonymisierung durch die Forschenden selbst ("Personalüberlassung" Abs. 3) zulässt. Derartige Erleichterungen sieht § 36 RegE nicht vor. Diese Regelung ist insofern kritikwürdig, als hier die Entscheidung der teilweise äußerst schwierigen Frage nach der Erforderlichkeit für wissenschaftliche Zwecke und die **Abwägung** der schutzwürdigen Interessen der völlig fachfremden Daten übermittelnden Stelle übertragen wird. Vorzugswürdig ist hier das Konzept des § 30 Abs. 4 Nr. 3 PDSE, das bei einer personenbezogenen Forschung ohne Einholen der Einwilligung der Betroffenen eine Entscheidung der Aufsichtsbehörde vorsieht.



Deutsche Vereinigung
für Datenschutz e.V.

Arbeitnehmer-Datenverarbeitung

Das in § 31 Abs. 5 S. 2 PDSE vorgesehene Verbot der Nutzung von **Daten aus technisch-organisatorischen Datensicherungsmaßnahmen** für Zwecke der Verhaltens- und Leistungskontrolle entspricht im Ergebnis der Regelung des § 13 Abs. 4 RegE, wonach solche Daten ausschließlich für "Maßnahmen gegenüber Bediensteten genutzt werden" dürfen. Sinnvoll ist zweifellos, die automatisierte Datenverarbeitung von Beschäftigten einem Freigabeverfahren zu unterwerfen (§ 31 Abs. 7 S. 1 PDSE). Die in der gleichen Vorschrift zwingend vorgesehene Unterrichtungspflicht der LfD ist angesichts der Vielzahl solcher Verfahren dagegen kaum eine wirksame Schutzvorschrift.

Altdatenbestände

Die im RegE vorgesehene **ersatzlose Streichung** der Altdatenregelung aus dem Datenschutzgesetz mit der problematischen Anzeigepflicht und einer ebenso problematischen Fiktionsregelung von Gewahrsamsinhabern von DDR-Altdatenbeständen ist nach dem Verlust praktischer Relevanz sehr zu unterstützen.

Dr. Thilo Weichert

Vorsitzender der Deutschen Vereinigung für Datenschutz e.V. (DVD)

Bonner Talweg 33-35
53173 Bonn

weichert@datenschutzverein.de