Baden-Württemberg
DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

PRESSEMITTEILUNG **18. März 2010**

Ergebnisse der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17. / 18. März 2010 in Stuttgart

Datenschutz am Scheideweg - Datenschützer fordern Neuorientierung für einen besseren Datenschutz

Zum Abschluss der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in Stuttgart hat der diesjährige Konferenzvorsitzende, der baden-württembergische Datenschutzbeauftragte Jörg Klingbeil, gemeinsam mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Peter Schaar, und dem Berliner Beauftragten für Datenschutz und Informationfreiheit, Dr. Alexander Dix, die Konferenzergebnisse vorgestellt. Beide vertreten den deutschen Datenschutz auch auf europäischer Ebene.

Die Datenschutzbeauftragten des Bundes und der Länder sehen sich durch das Urteil des **Europäischen Gerichtshofs** vom 09. März 2010 bestätigt, nach dem auch die deutschen Datenschutzaufsichtsbehörden von jeder Weisung durch Regierungsstellen völlig frei sein müssen, soweit sie private Datenverarbeiter kontrollieren. Sie halten daher eine grundsätzliche Neuordnung der Datenschutzaufsicht in Deutschland für geboten und fordern von den Gesetzgebern in Bund und Ländern eine europarechtlich einwandfreie Regelung, die für die Tätigkeit der unabhängigen Datenschutzbeauftragten im öffentlichen Bereich ebenfalls Folgen haben dürfte. Die in den Ländern und beim Bund bisher bestehenden Regelungen und Strukturen müssen im Einzelnen daraufhin überprüft werden, wie die **Unabhängigkeit** im Sinne des Urteils realisiert und im Interesse der Bürgerinnen und Bürger auch wirksam ausgestaltet werden kann. Eine Fach- und Rechtsaufsicht darf es nicht geben (siehe hierzu **Anlage 1**).

Die Konferenz hat sich erneut mit der **Modernisierung des Datenschutzrechts** befasst. „Unser Recht passt nicht mehr ins Internetzeitalter“, so Jörg Klingbeil. Oft sei es schwer zu klären, wer in den Welten des Internets jeweils für den Datenschutz zuständig ist. Als Grundlage für eine Diskussion über eine grundlegende Reform des Datenschutzrechts haben die Datenschutzbeauftragten ein Eckpunktepapier

Urbanstraße 32 · 70182 Stuttgart · Telefon 0711 615541-0 · Telefax 0711 615541-15 · poststelle@lfd.bwl.de
www.baden-wuerttemberg.datenschutz.de · PGP Fingerprint: A5A5 6EC4 47B2 6287 E36C 5D5A 43B7 29B6 4411
E1E4

vorgelegt; u.a. werden darin ein technikneutraler Ansatz, die Stärkung der Betroffenenrechte und wirksamere Sanktionen gefordert (siehe hierzu **Anlage 2**).

Das Bundesverfassungsgericht hat durch Urteil vom 02. März 2010 die **Vorratsdatenspeicherung** in der aktuellen Form für verfassungswidrig erklärt. Die Datenschutzbeauftragten sehen sich durch die Entscheidung des höchsten deutschen Gerichts in ihrer Auffassung bestärkt. Jörg Klingbeil: „Der Gesetzgeber hätte sich die erneute Blamage ersparen können. Bereits 2007 hatte die Konferenz der Datenschutzbeauftragten auf die Unverhältnismäßigkeit dieses Eingriffs in die Kommunikationsfreiheit hingewiesen. Ebenso wurde von uns damals deutlich gemacht, dass das in Kraft gesetzte Regelwerk weit über die Vorgaben der Europäischen Union hinausging.“ Die Konferenz lehnt die Vorratsdatenspeicherung grundsätzlich ab. Das Verbot der Totalerfassung gehöre zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland. Die Datenschutzbeauftragten fordern die Bundesregierung auf, sich für eine Aufhebung der Europäischen Richtlinie 2006/24/EG einzusetzen. Nach Ansicht der Konferenz müsse die Entscheidung des Bundesverfassungsgerichts auch über die Kommunikationsdaten hinaus Beachtung finden, etwa bei Flugpassagierdaten oder bei der Konzeption von Mautsystemen. Auch die zentrale ELENA-Datenbank müsse auf den Prüfstand (siehe hierzu **Anlage 3**).

Beim Einsatz von **Ganzkörperscannern** sieht die Konferenz der Datenschutzbeauftragten noch viele offene Fragen. Es müsse noch geklärt werden, was die Geräte technisch leisten können, ob damit ein nennenswerter Sicherheitsgewinn erzielbar ist und inwieweit Gesundheitsschäden entstehen können. Der Gesetzgeber habe nun über den Einsatz der Scanner zu entscheiden. Die Grundrechte der Betroffenen müssten dabei geschützt werden. Geschlechtsmerkmale oder künstliche Körperteile bzw. medizinische Hilfsmittel dürften nicht angezeigt werden (siehe hierzu **Anlage 4**).

Für einige **Sicherheitsgesetze** der letzten Jahre ist eine **Evaluierung** vom Gesetzgeber vorgesehen worden. Allerdings ist eine wirksame Erfolgskontrolle entscheidend davon abhängig, unter welchen Vorgaben und von wem sie durchgeführt wird. Die Datenschutzbeauftragten des Bundes und der Länder sehen mit Sorge, dass bei der derzeit vorgesehenen Evaluierung des Gemeinsame-Dateien-Gesetzes externer wissenschaftlicher Sachverstand nur eine Alibifunktion haben könnte. Es sollte eigentlich eine Selbstverständlichkeit sein, dass der Gesetzgeber diese Erfolgskontrolle von unabhängigen Experten, die nicht der die Sicherheitsgesetze vollziehenden Gewalt angehören, durchführen lässt. Dies gilt auch für die von der Bundesregierung vorgesehene Evaluierung der Kooperationszentren von Polizei und Nachrichtendiensten (siehe hierzu **Anlage 5**).

Das Bundesgesundheitsministerium plant, die bisherige Regelung zur Abrechnung hausärztlicher Leistungen und ambulanter Notfallbehandlungen im Krankenhaus durch **private Abrechnungsstellen in der gesetzlichen Krankenversicherung** um ein Jahr zu verlängern. Damit setzt sich der Bundesgesundheitsminister nicht nur über ein Urteil des Bundessozialgerichts hinweg. Auch die Datenschutzbeauftragten halten die derzeitigen Regelungen zur Datenverarbeitung höchst sensibler Daten durch private Stellen für völlig unzureichend. Sie fordern daher vom Gesetzgeber, schnell präzise Vorgaben für die Einschaltung privater Stellen bei der Abrechnung von Kassenleistungen im Sozialgesetzbuch zu verankern (siehe hierzu **Anlage 6**).

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 20. Dezember 2007 eine unzulässige Mischverwaltung bei den JobCentern festgestellt. Dies führte zu unklaren Zuordnungen von Verantwortlichkeiten in den Arbeitsgemeinschaften beim sozialrechtlichen Datenschutz im Bereich des Arbeitslosengelds II. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb für die anstehende **Neuorganisation der Arbeitsgemeinschaften/JobCenter** eindeutige gesetzliche Regelungen für die datenschutzrechtlichen Aufgaben und Kontrollzuständigkeiten, um die bisher bestehenden Unsicherheiten bei der Datenschutzkontrolle zu beseitigen. Keinesfalls dürfe es zu einer voraussetzungslosen Mehrfachspeicherung sensibler personenbezogener Daten bei den Leistungsträgern kommen, denn damit würden unvertretbare datenschutzrechtliche Risiken verbunden sein.

Zu folgenden Themen sind jeweils nähere Informationen angeschlossen:

1. Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle!
2. Ein modernes Datenschutzrecht für das 21. Jahrhundert - Zusammenfassung zum Eckpunktepapier
3. Keine Vorratsdatenspeicherung!
4. Körperscanner - viele offene Fragen
5. Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich
6. Klare gesetzliche Regelungen zur Abrechnung bei private Stellen in der gesetzlichen Krankenversicherung

Bei Rückfragen erreichen Sie uns unter der Telefonnummer 0711/615541-0. Weitere Informationen zum Datenschutz finden Sie im Internet unter www.baden-wuerttemberg.datenschutz.de oder unter www.datenschutz.de.
Die Pressemitteilung ist im Internet abrufbar unter www.baden-wuerttemberg.datenschutz.de/lfd/pm/default.htm.

Anlage 1

Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. März 2010

Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle!

Um das Grundrecht der Bürgerinnen und Bürger auf Datenschutz zu gewährleisten, bedarf es einer unabhängigen Datenschutzkontrolle. Der Europäische Gerichtshof hat festgestellt, dass die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in Deutschland nicht völlig unabhängig sind und die Bundesrepublik Deutschland damit gegen die Verpflichtung aus Art. 28 der Datenschutzrichtlinie (Richtlinie 95/46/EG) verstößt (Urteil vom 9. März 2010, C-518/07). Europarechtswidrig ist nicht nur die organisatorische Einbindung zahlreicher Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in die jeweiligen Innenministerien, sondern auch die Aufsicht der Regierungen über die Datenschutzbehörden. Darüber hinaus ist eine grundsätzliche Neuordnung der Datenschutzaufsicht in Deutschland geboten. Die Grundsätze dieser Entscheidung zur Unabhängigkeit sind auf die Datenschutzkontrolle der öffentlichen Stellen anzuwenden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Bund und Ländern auf, die Datenschutzaufsicht schnellstmöglich den Vorgaben der Richtlinie entsprechend umzugestalten.
Die Ausgestaltung der Unabhängigkeit der Datenschutzkontrollinstanzen muss insbesondere folgenden Kriterien entsprechen:

- Die Datenschutzkontrollstellen müssen ihre Aufgaben ohne jegliche unmittelbare und mittelbare Einflussnahme Dritter wahrnehmen können.
- Es darf keine Fach- und Rechtsaufsicht geben.
- Auch eine mögliche Dienstaufsicht darf nicht zu einer unmittelbaren oder mittelbaren Einflussnahme auf Entscheidungen der Datenschutzkontrollstellen führen.
- Eine Einflussnahme seitens der kontrollierten Stellen ist auszuschließen.
- Zu einer unabhängigen Amtsführung gehören ausreichende Eingriffs- und Durchsetzungsbefugnisse.
- Um eine unabhängige Wahrnehmung der Tätigkeit der Datenschutzkontrollstellen zu gewährleisten, muss ihnen die notwendige Entscheidungshoheit bei Personal, Haushalt und Organisation zustehen.

Anlage 2

79. Konferenz der
Datenschutzbeauftragten des Bundes und der Länder
vom 17./18. März 2010

Ein modernes Datenschutzrecht für das 21. Jahrhundert

Zusammenfassung

Jeder Mensch soll selbst bestimmen können, wer was wann über ihn weiß. Doch wie soll dieses Recht auf informationelle Selbstbestimmung im Zeitalter der allgegenwärtigen, oftmals unbemerkten Datenverarbeitung gewährleistet werden? Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat Eckpunkte formuliert, die Grundlage einer Diskussion über eine Reform des Datenschutzrechts sein sollen.

1. Konkrete Schutzziele und Grundsätze verankern

Das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze sollten als allgemeingültige datenschutzrechtliche Grundregelungen einen verbindlichen Mindeststandard festlegen. Sie sollten allgemeine Vorgaben enthalten, die als Grundlage aller datenschutzrechtlichen Regelungen und Maßnahmen für öffentliche und nichtöffentliche Stellen dienen. Ausgehend von den Schutzzielen sollten sanktionsbewehrte Grundsatznormen formuliert werden, die für alle Formen der Datenverarbeitung gleichermaßen gelten. Dies betrifft etwa den Grundsatz der Zweckbindung, also das Prinzip, dass personenbezogene Daten ausschließlich für den Zweck verwendet werden dürfen, für den sie erhoben worden sind. Neu eingeführt werden sollte zudem ein grundsätzliches Verbot der Profilbildung. Die Vorgaben des allgemeinen Datenschutzrechts können – soweit erforderlich – in Bezug auf bestimmte Anwendungsgebiete weiter konkretisiert werden.

2. Technikneutralen Ansatz schaffen

Den aus der technologischen Entwicklung resultierenden Gefährdungen sollte durch technikneutrale Vorgaben begegnet werden, die auf konkrete Systeme und Anwendungsfelder durch Auslegung und Normierung konkretisiert werden können. Anhand festgelegter Schutzziele können so einfache, flexible, und praxistaugliche gesetzliche Bedingungen geschaffen werden, die das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität

informationstechnischer Systeme durch technischen und organisatorischen Datenschutz sichern.

3. Betroffenenrechte stärken

Dreh- und Angelpunkt zur Durchsetzung des Datenschutzes ist der aufmerksame und kritische Betroffene. Die Datenverarbeitung muss für die Betroffenen transparenter werden, etwa indem die Wahrnehmung des Auskunftsanspruchs erleichtert wird. Die Freiwilligkeit der Einwilligung in eine Datenverarbeitung muss gestärkt werden.

4. Datenschutzrecht internetfähig machen

Ein modernes Datenschutzrecht muss internetfähig sein. Grundsätzlich muss eine unbeobachtete Kommunikation und Nutzung des Internets gewährleistet werden. Auch sind besondere Schutzmechanismen zur Gewährleistung und Durchsetzung der Datenschutzrechte der Betroffenen im Netz zu schaffen. Nationale Regelungen sollten durch internationale Vereinbarungen flankiert werden.

5. Mehr Eigenkontrolle statt Zwang

Datenschutz muss von den verantwortlichen Stellen als eigenes Anliegen begriffen werden. Dies kann etwa durch Einführung eines freiwilligen Auditverfahrens befördert werden. Daneben müssen die verantwortlichen Stellen dazu verpflichtet werden, durch interne Mechanismen die Einhaltung des Datenschutzes sicherzustellen, etwa durch verbindliche Datenschutzkonzepte.

6. Stärkung der unabhängigen Datenschutzaufsicht

Die Unabhängigkeit der Datenschutzaufsicht muss rechtlich, organisatorisch und finanziell abgesichert werden. Eine Fach- und Rechtsaufsicht oder die organisatorische Eingliederung in andere Verwaltungseinheiten ist mit der EG-Datenschutzrichtlinie nicht vereinbar. Erforderlich sind auch verstärkte Mitwirkungspflichten der kontrollierten Stellen bei Datenschutzkontrollen.

7. Wirksamere Sanktionen

Die immer noch vorhandenen Lücken im datenschutzrechtlichen Sanktionssystem müssen endlich geschlossen werden. Sie sollten ergänzt werden um für die Betroffenen einfach zu handhabende Haftungsansprüche, etwa einen pauschalierten Schadenersatzanspruch. Die Zuständigkeiten für die Verfolgung von Ordnungswidrigkeiten sollten bei den jeweiligen Datenschutzbehörden liegen. Auch der Bundesbeauftragte

für den Datenschutz und die Informationsfreiheit braucht insoweit wirksame Sanktionsbefugnisse.

8. Gesetz einfacher und besser lesbar machen

Das Datenschutzrecht ist durch wiederholte Änderungen und Ergänzungen selbst für Fachleute nur noch schwer verständlich und bedarf auch insoweit der Überarbeitung. Erforderlich sind etwa Änderungen in der Struktur und bei den Definitionen, die zusätzliche Spezialvorschriften entbehrlich machen.

Anlage 3

Entschließung
der 79. Konferenz der
Datenschutzbeauftragten des Bundes und der Länder
vom 17./18. März 2010

Keine Vorratsdatenspeicherung!

Das Bundesverfassungsgericht bewertet in seinem Urteil zur Vorratsdatenspeicherung vom 2. März 2010 (1 BvR 256/08) die anlass- und verdachtslose vorsorgliche Speicherung von Telekommunikationsdaten als einen „besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt“. Weil diese Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch aller Bürgerinnen und Bürger ermöglicht, lehnt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Vorratsdatenspeicherung grundsätzlich ab. Das Verbot der Totalerfassung gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, die auch in europäischen und internationalen Zusammenhängen zu wahren ist. Die Konferenz fordert deshalb die Bundesregierung auf, sich für eine Aufhebung der Europäischen Richtlinie 2006/24/EG einzusetzen.

Darüber hinaus betont das Bundesverfassungsgericht, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Daher strahlt die Entscheidung über den eigentlichen Entscheidungsgegenstand hinaus und muss auch in anderen Bereichen, etwa bei der diskutierten Speicherung der Daten von Flugpassagieren oder bei der Konzeption von Mautsystemen beachtet werden. Auch die zentrale ELENA-Datenbank muss jetzt auf den Prüfstand. Der Gesetzgeber ist bei der Erwägung neuer Speicherungspflichten oder -berechtigungen im Hinblick auf die Gesamtheit der verschiedenen Datensammlungen zu größerer Zurückhaltung aufgerufen.

Anlage 4

Entschließung
der 79. Konferenz der
Datenschutzbeauftragten des Bundes und der Länder
vom 17./18. März 2010

Körperscanner - viele offene Fragen

Der Anschlagsversuch von Detroit am 23. Dezember 2009 hat die Diskussion über den Einsatz von sog. Körperscannern bei der Passagierkontrolle am Flughafen neu entfacht. Mit dieser Technik sollen Sicherheitslücken geschlossen werden. Es ist aber noch weitgehend unklar, was diese Geräte technisch leisten können und wie sie sich in ein konsistentes Gesamtsystem zur Flugsicherheit einfügen lassen. Eine Entscheidung über den Einsatz solcher Geräte, die der Gesetzgeber zu treffen hätte, setzt zumindest die Erfüllung folgender Bedingungen voraus:

1. Es muss geklärt werden, ob mit diesen Geräten ein nennenswerter Sicherheitsgewinn erzielbar ist. Derzeit bestehen zumindest ernsthafte Zweifel an der technischen Leistungsfähigkeit und Effizienz dieser Technologie, vor allem im Hinblick auf die Detektierbarkeit von Materialien mit geringer Dichte, etwa pulverförmigen Substanzen, wie sie im Fall des Anschlagsversuchs von Detroit verwendet worden sind.
2. Es muss sichergestellt sein, dass die beim Einsatz der Körperscanner erhobenen Daten der Kontrollierten über den Scanvorgang hinaus nicht gespeichert werden. Auch die Anzeige der Körperkonturen gegenüber dem Kontrollpersonal und die Speicherung der erstellten Bilder über den Scanvorgang hinaus sind technisch auszuschließen.
3. Selbst wenn die vorstehenden Bedingungen erfüllt werden, darf der Einsatz von Scannern die Grundrechte der Betroffenen, insbesondere die absolut geschützte Menschenwürde und das Recht auf körperliche Unversehrtheit nicht verletzen. So dürften z.B. Geschlechtsmerkmale oder künstliche Körperteile bzw. medizinische Hilfsmittel (etwa Prothesen und künstliche Darmausgänge) nicht angezeigt werden. Gesundheitsschäden sind auszuschließen.
4. Die Erfüllung dieser Bedingungen ist in praktischen Tests und Erprobungen nachzuweisen.

Anlage 5

Entschließung
der 79. Konferenz der
Datenschutzbeauftragten des Bundes und der Länder
vom 17./18. März 2010

Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich

Die Bundesregierung beabsichtigt, nicht nur die in den vergangenen Jahren durch zahlreiche Gesetze neu geschaffenen Befugnisse und die bestehenden Sicherheitsdateien, sondern auch die Kooperationszentren, in denen Polizei und Nachrichtendienste zusammenarbeiten, zu evaluieren.

Die Datenschutzbeauftragten des Bundes und der Länder treten dafür ein, die Evaluierung zeitnah und vorbehaltlos nach wissenschaftlichen Kriterien durchzuführen. Kein Vorbild darf die im Mai 2005 vorgenommene „Evaluierung“ des Terrorismusbekämpfungsgesetzes 2002 sein. Diese war eine inhaltlich und methodisch defizitäre Selbsteinschätzung. Dagegen enthalten die in verschiedenen Gesetzen aufgenommenen Evaluationsklauseln sinnvolle Ansätze, die es weiter zu entwickeln gilt. Dies betrifft etwa die Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag zu bestellen ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt darauf hingewiesen, dass die Ausweitung der Befugnisse von Polizei und Verfassungsschutz, auch in das Vorfeld der Gefahrenabwehr, zur anlasslosen, oftmals massenhaften Erhebung personenbezogener Daten unbescholtener Bürgerinnen und Bürger führen kann.

Aufgrund der Eingriffsintensität der Regelungen ist eine systematische, ergebnisoffene und wissenschaftlich fundierte Überprüfung auf der Grundlage eines umfassenden Bewertungsansatzes erforderlich. Jede Evaluation, auch die landesrechtlicher Vorschriften, muss auf der Grundlage valider, strukturierter Daten unter Mitwirkung aller relevanten Stellen in einem transparenten Verfahren durch ein unabhängiges Expertengremium erfolgen. Die Nachvollziehbarkeit und Überprüfbarkeit der Evaluierung ist zu gewährleisten. Der Evaluationsbericht muss dem Gesetzgeber eine umfassende Bewertungsgrundlage zur Optimierung bestehender Regelungen zur Verfügung stellen.

Anlage 6

Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18. März 2010

Klare gesetzliche Regelungen zur Abrechnung durch private Stellen in der gesetzlichen Krankenversicherung

In seinem Urteil vom 10. Dezember 2008 hatte das Bundessozialgericht nach der damals bestehenden Rechtslage die Einschaltung privater Stellen bei der Abrechnung von ärztlichen Leistungen gegenüber den gesetzlichen Krankenkassen für unzulässig erklärt. Es betonte, dass bei der Einbeziehung von privaten Stellen ebenso detaillierte Regelungen über den Umfang der verarbeiteten Daten und über die erlaubten Datenflüsse vorliegen müssten, wie dies für die klassischen Abrechnungen über die Kassenärztlichen Vereinigungen der Fall ist. Es sei nicht nachvollziehbar, dass gerade bei der Einbeziehung von Privaten an diese geringere Anforderungen gestellt würden als an die öffentlich-rechtlichen Körperschaften. Infolge des Urteils war die Einbeziehung der privaten Stellen nur noch für einen Übergangszeitraum erlaubt.

Um die Abrechnung von Leistungen durch private Rechenzentren nicht einstellen zu müssen, hat der Gesetzgeber hierfür durch das Arzneimittelrechtsänderungsgesetz vom 17. Juli 2009 vorläufige Rechtsgrundlagen in den §§ 120 Abs. 6 und 295 Abs. 1b SGB V geschaffen, die bis zum 30. Juni 2010 befristet sind. Die Bundesregierung beabsichtigt nunmehr, die Geltung dieser Übergangsregelungen, die den vom Bundessozialgericht formulierten Anforderungen an den Datenschutz nicht entsprechen, um ein weiteres Jahr zu verlängern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für dringend geboten, unverzüglich materielle Vorgaben für die Einbeziehung privater Stellen bei der Abrechnung von ärztlichen Leistungen im Gesetz zu verankern. Dabei müssen präzise Regelungen geschaffen werden, die denselben Schutz der Sozialdaten garantieren, gleich ob die Daten unter Einschaltung privater oder öffentlich-rechtlicher Abrechnungsstellen verarbeitet werden. Die für die Abrechnung zu verwendenden Daten müssen wie bei den herkömmlichen Abrechungsregelungen für die Patienten transparent verarbeitet und auf das absolut Erforderliche für den konkreten Zweck normativ begrenzt werden. Weiterhin müssen die Datenflüsse in einer Weise definiert werden, dass die Rechte der Versicherten so wenig wie möglich gefährdet werden. Eine Rechtsaufsicht über die Datenverarbeitung ist sicherzustellen. Es ist zu gewährleisten, dass Krankenkassen bei der Beauftragung privater Abrechnungsstel-

len nicht mehr Sozialdaten erhalten als bei der Abrechnung über die Kassenärztliche Vereinigung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung auf, unverzüglich inhaltliche Vorschläge für eine verfassungskonforme Regelung zu erarbeiten.