Datenschutzverordnung des Hauptverbandes der österreichischen Sozialversicherungsträger für die gesetzliche Sozialversicherung - SV-Datenschutzverordnung 2001 - SV-DSV 2001

Geltungsbereich

§ 1. (1) Diese Verordnung gilt für

1. den Hauptverband der österreichischen Sozialversicherungsträger,
2. die Gebietskrankenkassen, und zwar die
   a) Wiener Gebietskrankenkasse
   b) Niederösterreichische Gebietskrankenkasse
   c) Burgenländische Gebietskrankenkasse
   d) Oberösterreichische Gebietskrankenkasse
   e) Steiermärkische Gebietskrankenkasse
   f) Kärntner Gebietskrankenkasse
   g) Salzburger Gebietskrankenkasse
   h) Tiroler Gebietskrankenkasse
   i) Vorarlberger Gebietskrankenkasse
3. die Betriebskrankenkassen, und zwar die
   a) Betriebskrankenkasse der Austria Tabak
   b) Betriebskrankenkasse der Wiener Verkehrsbetriebe
   c) Betriebskrankenkasse Semperit
   d) Betriebskrankenkasse Neusiedler
   e) Betriebskrankenkasse VOEST-ALPINE Donawitz
   f) Betriebskrankenkasse Zeltweg
   g) Betriebskrankenkasse Kindberg
   h) Betriebskrankenkasse Kapfenberg
   i) Betriebskrankenkasse Pengg
4. die Versicherungsanstalten, und zwar die
   a) Versicherungsanstalt des österreichischen Bergbaues
   b) Versicherungsanstalt der österreichischen Eisenbahnen
   c) Versicherungsanstalt öffentlich Bediensteter
   d) Sozialversicherungsanstalt der gewerblichen Wirtschaft
   e) Sozialversicherungsanstalt der Bauern
   f) Allgemeine Unfallversicherungsanstalt
   g) Pensionsversicherungsanstalt der Arbeiter
   h) Pensionsversicherungsanstalt der Angestellten
   i) Versicherungsanstalt des österreichischen Notariates

als Auftraggeber nach § 4 Z 4 DSG 2000 und Dienstleister nach § 4 Z 5 DSG 2000; für den Hauptverband auch als Betreiber eines Informationsverbundsystems nach § 4 Z 13 DSG 2000.

(2) Sie gilt sowohl für die Verwendung von Dateien im Sinn des DSG 2000 als auch für den Bereich des Grundrechts auf Datenschutz.

Hauptverband als Dienstleister

§ 2. (1) Der Hauptverband der österreichischen Sozialversicherungsträger ist nach § 31 Abs. 11 ASVG Dienstleister für die Sozialversicherungsträger. Dies gilt insbesondere für:

- die Vergabe einheitlicher Versicherungsnummern nach § 31 Abs. 4 Z 1 ASVG,
- die Einrichtung und Führung einer zentralen Anlage zur Aufbewahrung der für die Versicherung bedeutsamen Daten nach § 31 Abs. 4 Z 3 lit. a ASVG,
- die Auskunftserteilung nach § 31 Abs. 4 Z 3 lit. b ASVG,
- die Verwendung von Daten für Verrechnungszwecke auf Grund sozialversicherungsrechtlicher Bestimmungen sowie
- den Betrieb des elektronischen Verwaltungssystems ELSY nach § 31a Abs. 2 ASVG.

(2) Der Hauptverband der österreichischen Sozialversicherungsträger ist für die Sozialversicherungsträger im Rahmen des Informationsverbundsystems der österreichischen Sozialversicherung nach § 50 Abs. 1 DSG 2000 Betreiber dieses Systems. Die von ihm festgelegten Maßnahmen der Datensicherheit (§ 7) sind für die in diesem System tätigen Auftraggeber verbindlich (§ 31 Abs. 6 ASVG).

öffentlicher Bereich

§ 3. Die Datenanwendungen der Auftraggeber sind nach § 5 DSG 2000 dem öffentlichen Bereich zuzuordnen.

Aufgabengebiete

§ 4. Bei den Sozialversicherungsträgern und dem Hauptverband bestehen folgende Aufgabengebiete im Sinn des § 4 Z 12 DSG 2000:

1. Vollziehung des gesetzlichen Zuständigkeitsbereiches,
2. Wirtschaftsverwaltung einschließlich Finanz- und Beschaffungswesen sowie Kostenrechnung,
3. Personalverwaltung einschließlich Angelegenheiten der Versicherungsvertreter.

Grundsätze für die Verwendung von Daten

§ 5. (1) Daten dürfen vom Auftraggeber nur im Rahmen des § 6 DSG 2000 verwendet werden.

(2) Grundsätze für die Verwendung von Daten in der Sozialversicherung sind:

1. Daten dürfen nur in der Art und dem Umfang verwendet werden, als dies für den Auftraggeber zur Wahrnehmung der ihm gesetzlich übertragenen Aufgaben eine wesentliche Voraussetzung ist. Die Verwendung nicht notwendiger Daten (Ballastwissen, Überschusswissen) ist unzulässig.
2. Übermittlungen dürfen nur auf Grund einer ausdrücklichen Rechtsgrundlage durchgeführt werden und nicht schon dann, wenn eine solche Berechtigung im Wege einer Interpretation einer Bestimmung erschlossen werden könnte.
3. Die datenschutzrechtliche Zulässigkeit einer Datenverwendung begründet für sich allein noch keine Verpflichtung hiezu. Für eine Datenverwendung haben konkrete Gründe aus dem Vollziehungsbereich des jeweiligen Rechtsträgers im Sinn des § 6 DSG 2000 vorzuliegen.
4. Daten, die mit an Sicherheit grenzender Wahrscheinlichkeit nicht mehr benötigt werden, sind möglichst rasch zu löschen. Zu diesem Zweck sind Datenbestände regelmäßig auf die Notwendigkeit der darin enthaltenen Daten durchzusehen. Die bloße theoretische Möglichkeit, Datenbestände zur Vollziehung einer noch nicht absehbaren zukünftigen Regelung verwenden zu können, ist für sich allein kein ausreichender Grund, entsprechende Daten aufzubewahren.
5. Einem Ersuchen um Übermittlung darf ein Auftraggeber nur entsprechen, wenn folgende Voraussetzungen gemeinsam vorliegen:
   a) eine Rechtsgrundlage (Z 2) hiefür feststeht,
   b) bei Zweifeln an der Übermittlungszulässigkeit die ersuchende Stelle vor der Datenermittlung ihre Ermittlungsberechtigung glaubhaft gemacht hat,
   c) bei Online-Übermittlungsverfahren der Übermittlungsempfänger für die Dauer des Bestehens seiner Zugriffsberechtigung verpflichtet ist, regelmäßige Kontrollen durchzuführen, Kontrollmaßnahmen der übermittelnden Stelle zu unterstützen, dies auch tatsächlich geschieht und dies dem Auftraggeber gegenüber glaubhaft gemacht ist,
   d) sich Übermittlungsersuchen auf konkret umschriebene Daten oder Personen beziehen, wobei die Übermittlung nur allgemein beschriebener Datenbestände jedenfalls unzulässig ist,
   e) andere Möglichkeiten, ein überwiegendes und demnach berechtigtes Interesse zu wahren, nicht vorliegen oder nicht zumutbar sind.
6. Das gelindeste zur Verfügung stehende Mittel im Sinn des § 7 Abs. 3 DSG 2000 wird dann nicht mehr eingesetzt, wenn Daten aus Beständen der Sozialversicherung für Zwecke verwendet werden sollen, zu deren Unterstützung andere Register eingerichtet sind (z. B. für Adressenermittlungen die Melderegister, für Einkommenserhebungen jene der Finanzverwaltung).
7. Die Verantwortlichkeit des Auftraggebers bzw. Dienstleisters für die weitere Verwendung der Daten endet mit der Übermittlung dieser Daten an Dritte.

Verwendung von sensiblen Daten

§ 6. (1) Die Verwendung von sensiblen Daten ist ausschließlich in den Fällen, die in § 9 DSG 2000 taxativ aufgezählt sind, zulässig.

(2) Ein „wichtiges öffentliches Interesse“ im Sinn des § 9 Z 3 DSG 2000 kann auch ein wichtiges wirtschaftliches öffentliches Interesse sein (z. B. Evaluierung der Verwendung öffentlicher Mittel im Gesundheitswesen durch Aufsichtsbehörden und Rechnungshof, Controlling und Monitoring nach § 32b ASVG, Reporting nach § 32d ASVG, Einhaltung gesetzlicher Einsparungsvorschriften, z. B. nach § 588 Abs. 14 ASVG).

(3) Medizinische Diagnostik im Sinn des § 9 Z 12 DSG 2000 umfasst auch Untersuchungen für Zwecke der Rehabilitation oder der Erbringung anderer Leistungen durch Sozialversicherungsträger einschließlich des Verfahrens in Sozialrechtssachen vor den Arbeits- und Sozialgerichten.

(4) Die Verwendung von sensiblen Daten umfasst auch die Verwendung im Rahmen des Versuchs einer außergerichtlichen Streitbeilegung (z. B. Schiedsverfahren mit Vertragspartnern auf Grund von Gesamtverträgen nach den §§ 341 ff. ASVG etc.).

Datensicherheitsmaßnahmen

§ 7. (1) Auftraggeber und Dienstleister haben die Richtigkeit der Verarbeitungsergebnisse in regelmäßigen Abständen durch Stichproben oder Prüfprogramme zu überprüfen.

(2) Daten und Programme sind vor Entstellung, Zerstörung und Verlust sowie gegen unbefugte Verwendung und Weitergabe zu schützen.

(3) Der Auftraggeber (oder in dessen Auftrag der Dienstleister) hat für die Vernichtung unbrauchbarer oder nicht mehr benötigter Ausdrucke und sonstiger Datenträger Sorge zu tragen.

(4) Wird ein Fehler festgestellt, so haben der Auftraggeber und der Dienstleister alles zu unternehmen, um das Schadensausmaß gering zu halten, den Betroffenen unnötige Mühe zu ersparen, die Fehlerbehebung raschest einzuleiten und Folgefehler zu verhindern.

(5) Für die ordnungsgemäße und sichere Anwendung von Daten sind folgende Datensicherheitsmaßnahmen (§ 14 DSG 2000) zu setzen:

1. Es ist eine Ansprechstelle (Person, Organisationseinheit) für Datensicherheitsmaßnahmen zu benennen, welcher die Unterlagen (Organisationsbeschreibungen, Datensicherheitsmaßnahmen etc.) des Versicherungsträgers und des Hauptverbandes gesammelt zur Verfügung stehen.
2. Für die Programmverwaltung sind Zuständigkeiten und Regeln festzulegen. Zugriffsschutz zu personenbezogenen Daten und Datensicherheitsmaßnahmen sind nach Maßgabe des jeweiligen Standes der Technik zu organisieren; erteilte Zugriffsberechtigungen sind einfach lesbar auf nachvollziehbare Weise (inklusive des Berechtigungszeitraumes) zu dokumentieren. Bestehende Einrichtungen sind regelmäßig auf Verbesserungsmöglichkeiten zu untersuchen.
3. Zugriff auf Datenanwendungen darf nur eingeräumt werden, nachdem die Bestimmungen über das Datengeheimnis (§ 15 DSG 2000), die Datensicherheitsmaßnahmen und diese Verordnung zur Kenntnis gebracht wurden. Sammelzugriffsberechtigungen sind unzulässig.
4. Zugriffsberechtigungen sind möglichst nur befristet einzuräumen und jedenfalls zu beenden, wenn sie
   a) zur weiteren Arbeit nicht mehr benötigt werden oder
   b) vom Berechtigten Verstösse gegen Datensicherheitsvorschriften gesetzt wurden.
5. Datensichtgeräte (Bildschirme, etc.) sind so aufzustellen, dass der mit ihnen wiedergegebene Inhalt nicht von Unbefugten mitgelesen werden kann.
6. Von einer Einschau der Datenschutzkommission nach § 30 DSG 2000 betreffend das Informationsverbundsystem der österreichischen Sozialversicherung sind vom betroffenen Versicherungsträger jedenfalls der Hauptverband und jene Versicherungsträger zu verständigen (§ 321 ASVG, § 183 GSVG, § 171 BSVG, § 119 B-KUVG, § 87 NVG), welche Daten des Betroffenen verwenden.
7. Es sind alle dem jeweiligen Stand der Technik entsprechenden und wirtschaftlich zumutbaren Maßnahmen zu treffen, um eine Veränderung oder Vernichtung der Daten durch Programmstörungen zu verhindern, wie die Installation von Virenschutzprogrammen, fire-walls, Laufwerksperren, gestaffelte Zugriffsberechtigungen, etc.
8. Datenträger (Festplatten, Bänder, Disketten etc.) sind vor einer Veräußerung oder Entsorgung zu löschen oder sicher unlesbar zu machen.
9. Zugriff auf Datenverwendungen darf nur auf Grund persönlicher Benützerkennungen und Kennwörter (Passwörter) möglich sein. Die Kennwortvergabe hat vorzusehen, dass Kennwörter aus einer Mindestzahl von Zeichen und (wenn nicht schwer wiegende technische Gründe dagegen sprechen) einer Kombination aus Buchstaben, Ziffern (statt Ziffern auch Sonderzeichen) zu bestehen haben. Kennwörter sind geheim zu halten, ihre Änderung ist dem Zugriffsberechtigten innerhalb periodischer Zeiträume möglich zu machen. Das Kennwort muss von der Benutzerkennung verschieden sein.

(6) Über alle Datensicherheitsmassnahmen ist eine Dokumentation zu führen; diese ist mindestens elf Jahre aufzubewahren.

(7) Der Hauptverband als Betreiber nach § 50 Abs. 1 DSG 2000 hat gemeinsam mit den Versicherungsträgern durch Stichproben zu prüfen, ob die Verwendung der Daten den einschlägigen Bestimmungen entsprechend erfolgt und die erforderlichen Datensicherheitsmaßnahmen ergriffen worden sind.

(8) Bedient sich der Hauptverband oder ein Sozialversicherungsträger für den Datenverkehr eines Dienstleisters, so ist dieser zur Einhaltung aller datenschutzrechtlichen Bestimmungen und Ergreifung der in dieser Verordnung vorgesehenen Datensicherheitsmaßnahmen zu verpflichten.

Protokollierung

§ 8. (1) Protokolle sind regelmäßig zu prüfen und, soweit diese und andere Vorschriften keine anderen Aufbewahrungsfristen für Protokolle vorsehen, mindestens elf Jahre und höchstens 31 Jahre in automationsunterstützt lesbarer Form aufzubewahren.

(2) Protokollierungen (§ 14 Abs. 2 Z 7 DSG 2000) sind in leicht zugänglicher und für die zuständigen MitarbeiterInnen einfach lesbarer Weise vorzunehmen. Je nach Empfänger dürfen unterschiedliche Protokollierungsmethoden verwendet werden, solange die Auskunftsverpflichtung dadurch nicht beeinträchtigt wird. Die Protokollierung darf nur in folgenden Zusammenhängen entfallen:

1. Wenn Daten auf Grund einer
   a) Standardverordnung (§ 17 Abs. 2 Z 6 DSG 2000) oder
   b) Musterverordnung (§ 19 Abs. 2 DSG 2000)
   verwendet werden. In diesem Fall ist dem Betroffenen bei einer Anfrage nach § 26 DSG 2000 mitzuteilen, dass bestimmte Datenarten des Betroffenenkreises, zu dem auch der Betroffene gehört, an einen bestimmten Empfängerkreis planmäßig übermittelt werden. Die hievon betroffenen Datenarten, Betroffenenkreise und Empfängerkreise sind in der Auskunft zu nennen.
2. Wenn Daten nach § 46 DSG 2000 für wissenschaftliche Forschung und Statistik verwendet werden.
3. Wenn Daten gesammelt als Grundlage gesetzlich vorgesehener konkreter weiterer Verwendungen (z. B. zur Vorbereitung von Wahlen nach § 45 AKG 1992) übermittelt werden.
4. Wenn die Programme, mit denen Daten verwendet werden, vor Inkrafttreten dieser Verordnung fertig gestellt wurden und der Einbau eines Programmteils zur Protokollierung wegen des in absehbarer Zeit erfolgenden Einsatzes neuer Programme unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit unzweckmäßig wäre.

(3) Die Protokollierung ist so zu gestalten, dass auch Zugriffe der eigenen MitarbeiterInnen nachvollzogen werden können.

(4) Die Registrierung einer einzelfallbezogenen Datenübermittlung an Stellen außerhalb des Aufsichtsbereiches der obersten Aufsichtsbehörde der Sozialversicherung (z. B. im Rahmen von Amtshilfe) befreit nicht von der Verpflichtung, diese Übermittlungen zu protokollieren. Auftraggeber einer Standardanwendung haben jedermann auf Anfrage mitzuteilen (§ 23 DSG 2000), welche Standardanwendungen sie tatsächlich vornehmen.

Datengeheimnis

§ 9. (1) Allen Bediensteten und sonstigen Personen, denen Daten aus Datenanwendungen auf Grund ihrer Beschäftigung oder Funktion bei einem Auftraggeber oder Dienstleister anvertraut oder zugänglich geworden sind, ist es unbeschadet sonstiger Verschwiegenheitspflichten untersagt,

1. sich Daten unbefugt zu beschaffen,
2. Daten zu einem anderen Zweck als für ihre eigene Arbeit zu verwenden,
3. unbefugten Personen oder unzuständigen Stellen Daten mitzuteilen,
4. unbefugten Personen oder unzuständigen Stellen Daten zugänglich zu machen.

(2) Die im Abs. 1 genannten Personen sind zur Einhaltung dieser Verbote auch nach Beendigung ihres Dienstverhältnisses oder ihrer Funktion verpflichtet.

Information der Bediensteten

§ 10. (1) Alle Bediensteten eines Auftraggebers oder Dienstleisters sind von diesem in geeigneter Form über die für sie wesentlichen Bestimmungen des Datenschutzgesetzes und dieser Verordnung in Kenntnis zu setzen.

(2) Die Bediensteten, die mit der Durchführung von Datenanwendungen befasst sind, sind in einem erhöhten Maße über datenschutzrechtliche Bestimmungen, insbesondere über das Datenschutzgesetz und diese Verordnung, zu informieren.

Datenverarbeitungsregister

§ 11. (1) Jede Datenanwendung ist nach der Datenverarbeitungsregister-Verordnung, BGBl. II Nr. 520/1999, der Datenschutzkommission zur Eintragung in das Datenverarbeitungsregister zu melden, soweit nicht eine ausdrückliche Ausnahme nach § 17 DSG 2000 besteht oder die Anwendung bereits auf Grund des Übergangsrechts (§ 61 DSG 2000) als gemeldet gilt.

(2) Bei Übermittlungen und Mitteilungen an Betroffene, die in schriftlicher Form ergehen, ist die Registernummer in deren Text anzugeben.

(3) Bei Übermittlungen und Mitteilungen an Betroffene mittels maschinell lesbarer Datenträger ist die Registernummer auf den Begleitpapieren oder auf den Datenträgern anzugeben.

(4) Die Meldepflicht von Datenverarbeitungen an die Datenschutzkommission richtet sich nach den §§ 17 ff. DSG 2000.

Informationspflicht des Auftraggebers

§ 12. Die Informationspflicht nach § 24 DSG 2000 ist so auszuüben, dass der Betroffene dadurch in die Lage versetzt wird, ohne für ihn unzumutbare Anstrengungen, aber auch ohne unzumutbare und unnötige Belastung des Auftraggebers, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß sowie umfassend über die Bedingungen der Erhebungen informiert zu werden. Die Informationspflicht nach § 24 DSG 2000 besteht in jedem Fall unabhängig vom Einsichtsrecht in das Datenverarbeitungsregister.

Auskunftsrecht

§ 13. (1) Eine Auskunft darf unbeschadet der nachstehenden Bestimmungen nur erteilt werden, wenn die Identität des Betroffenen in unbedenklicher Form festgestellt werden kann.

(2) Auskünfte nach § 26 DSG 2000 dürfen nur in folgenden Fällen gegeben werden:

1. an den Betroffenen über die eigenen Daten (dies schließt die Anforderung einer Auskunft durch einen bevollmächtigten Dritten mit Zustellung an den Betroffenen nicht aus);
2. an behördlich bestellte Vertreter (Sachwalter, Kuratoren etc.) auf Grund ausdrücklicher Bestellungsurkunden, Beschlüsse oder Aufträge;
3. an gesetzliche Vertreter (Erziehungsberechtigte), jedoch in den Fällen, in denen ein Kind das 14. Lebensjahr bereits vollendet hat, nur dann, wenn vor der Auskunftserteilung bescheinigt ist, dass die Auskunftserteilung nicht gegen dessen Interessen verstößt. Diese Bescheinigung hat der Art der angeforderten Daten zu entsprechen und ist bei sensiblen Daten nachvollziehbar festzuhalten.

(3) Die Auskunft ist so zu erteilen, dass bei durchschnittlichem Verständnis vom Betroffenen erwartet werden kann, er werde Inhalt und Aussage der Auskunft zweifelsfrei verstehen. Abkürzungen dürfen in der Auskunft verwendet werden, wenn erwartet werden kann, dass der Betroffene sie versteht oder wenn ihre Bedeutung dem Auskunftsschreiben zu entnehmen ist.

(4) Die Auskunft darf dadurch erteilt werden, dass dem Betroffenen ein Ausdruck seiner Daten (z. B. eine Bildschirmkopie) mit Erläuterungen übersandt wird. Eine mündliche Auskunftserteilung ist nur dann ausreichend, wenn der Betroffene damit einverstanden ist. Auskünfte über Telefon, Telefax oder e-mail sind nur dann zulässig, wenn hiefür Sicherheitsvorkehrungen (Standleitungen, Rückruf, Verschlüsselungsverfahren, elektronische Signatur etc.) genützt werden.

(5) Das Auskunftsrecht umfasst Auskünfte aus Protokolldaten über Zugriffe auf Daten des Betroffenen. Personenbezogene Daten Anderer (Benützerkennzeichen) oder Sicherheitsdaten der abfrageberechtigten Stellen (Passwörter etc.) dürfen nur bei Vorliegen überwiegender Interessen des Auftraggebers oder eines Dritten bzw. überwiegender öffentliche Interessen nicht preisgegeben werden.

(6) Eine Auskunft schließt auch Daten des Auskunftswerbers ein, die unter einem Ordnungsmerkmal eines Dritten (z. B. eines Dienstgebers, behandelnden Arztes) gespeichert sind, soweit der Auskunftswerber einen geeigneten Hinweis zur Feststellung dieses Ordnungsmerkmales gibt. Auskunft über eigene Behandlungsdaten des Betroffenen (Diagnosen, verrechnete Leistungen etc.) darf nicht unter Berufung auf ein Geheimhaltungsinteresse des Behandlers verweigert werden. Honorarbeträge gehören nicht zu den Behandlungsdaten. Wenn eine Auskunft für den Betroffenen aus medizinischen Gründen schädlich sein könnte (therapeutischer Vorbehalt) und sie deswegen nicht erteilt wird, ist dies zu dokumentieren.

(7) Ein Betroffener wirkt jedenfalls dann im Sinn des § 26 Abs. 3 DSG 2000 am Verfahren mit, wenn er

1. in jenen Fällen, in denen Anhaltspunkte dafür vorliegen, dass mehrere Personen mit gleichen oder sehr ähnlichen Daten vorhanden sind, die notwendigen konkreten Hinweise zur Unterscheidung seiner Person von diesen anderen Personen gibt,
2. die Datenverarbeitungen bezeichnet, bezüglich derer er Betroffener sein kann und er bei umfangreichen Datenanwendungen auch den zeitlichen und inhaltlichen Zusammenhang der Verwendung seiner Daten nennt,
3. allenfalls durch die Vorlage von Unterlagen oder die Beschreibung von Lebensumständen glaubhaft macht, dass seine Daten irrtümlich oder missbräuchlich in Datenbeständen des Auftraggebers enthalten sind,
4. angibt, unter welchem Namen und Geburtsdaten (bzw. Namenschreibweisen) Daten über ihn aufgefunden werden könnten.

(8) Von der Bearbeitung eines Auskunftsersuchens ist abzusehen, wenn der Betroffene nicht am Verfahren mitwirkt. Auf diesen Umstand ist der Betroffene in einer Aufforderung zur Mitwirkung (Abs. 7, § 26 Abs. 4 DSG 2000) hinzuweisen.

(9) Auskünfte sind überdies nicht zu erteilen, wenn dies aus einem der in § 26 Abs. 2 DSG 2000 genannten weiteren Gründe unzulässig ist. Zu diesen Gründen zählen insbesondere jene Fälle der Datenübermittlung, in denen dem Betroffenen gegenüber (unbeschadet der ihm nach den maßgeblichen Verfahrensvor-

schriften zustehenden Rechte) nach Abwägung der Umstände des Einzelfalles wegen überwiegenden öffentlichen Interesses Daten geheim zu halten sind:

1. im Zuge eines gerichtlichen oder verwaltungsbehördlichen Strafverfahrens oder eines Disziplinarverfahrens sowie diesbezüglicher Vorerhebungen, solange das Verfahren noch nicht rechtskräftig abgeschlossen ist,
2. die Empfänger übermittelter Daten, sofern die Übermittlung für Zwecke eines gerichtlichen oder verwaltungsbehördlichen Strafverfahrens oder eines Disziplinarverfahrens durchgeführt wurde.

Pauschalierter Kostenersatz

§ 14. (1) Auskünfte nach § 26 DSG 2000 sind unentgeltlich zu erteilen, wenn sie den aktuellen und direkt abfragbaren Datenbestand einer Datenanwendung betreffen und wenn der Auskunftswerber im laufenden Kalenderjahr zum selben Aufgabengebiet noch kein Auskunftsersuchen an den Auftraggeber gestellt hat. In allen anderen Fällen kann ein pauschalierter Kostenersatz von 19 € verlangt werden. Ein höherer Kostenersatz darf nur dann verlangt werden, wenn tatsächlich höhere Kosten entstanden sind. Diese tatsächlichen Kosten sind an Hand der vollständigen Kosten der verbrauchten Arbeitszeit und konkreten Bezüge der hiefür eingesetzten Personen sowie des sonstigen Aufwandes (Material- und Sachaufwand etc.) zu errechnen (Vollkostenrechnung).

(2) Von der Einhebung eines Kostenersatzes ist abzusehen, wenn der Aufwand für die Vorschreibung und Einhebung des Kostenersatzes unverhältnismäßig höher liegen würde als der Aufwand für die Auskunftserteilung; hievon kann hinsichtlich aller von einem Auskunftsersuchen betroffenen Datenverarbeitungen oder einzelner dieser Datenverarbeitungen Gebrauch gemacht werden.

(3) Für die Beurteilung, ob ein Auskunftswerber im laufenden Kalenderjahr schon ein Auskunftsersuchen gestellt hat, ist das Eingangsdatum der Auskunftsersuchen beim Auftraggeber maßgebend.

(4) Unter aktuellen Daten im Sinn des Abs. 1 sind jene Daten zu verstehen, die zum Zeitpunkt der Antragstellung in den laufenden, automationsunterstützt oder manuell geführten Dateien des Auftraggebers unter einem Ordnungsmerkmal des Betroffenen gespeichert sind und auf die direkt zugegriffen werden kann.

Mitteilung des Kostenersatzes

§ 15. (1) Das Verlangen nach Kostenersatz ist dem Auskunftswerber unverzüglich nach Einlangen des - gegebenenfalls konkreter gefassten (§ 13 Abs. 7) - Auskunftsbegehrens mitzuteilen. Erfolgt diese Mitteilung schriftlich, ist auch eine Kontoverbindung anzugeben. Das Verlangen nach Bareinzahlung bei einer eigenen Stelle des Auftraggebers ist unzulässig.

(2) Von der Bearbeitung eines Auskunftsantrages ist abzusehen, wenn der nach Abs. 1 mitgeteilte Kostenersatz nicht entrichtet wurde.

Auskunftsfrist

§ 16. (1) Die in § 26 Abs. 4 DSG 2000 enthaltene Frist von 8 Wochen für die Erteilung von Auskünften beginnt bei unentgeltlich zu erfüllenden Auskunftsbegehren mit dem Einlangen des Auskunftsbegehrens beim Auftraggeber.

(2) Wurde ein Kostenersatz verlangt, so beginnt die Frist für die Auskunftserteilung mit Einlangen des Kostenersatzes bei der auskunftsverpflichteten Stelle (Auftraggeber bzw. Dienstleister, wenn dieser zur Auskunft verpflichtet ist).

(3) Wurde der Auskunftswerber aufgefordert, sein Auskunftsbegehren zu konkretisieren, so beginnt die Frist für die Auskunftserteilung mit dem Einlangen des konkretisierten Auskunftsbegehrens bei der auskunftsverpflichteten Stelle.

Andere Auskunftsvorschriften

§ 17. (1) § 26 DSG 2000 ist nicht anzuwenden, wenn Auskunftsbegehren auf einer anderen Grundlage als dem Datenschutzgesetz beruhen. Insbesondere werden die Vorschriften über Aufklärung und Information (§ 81 ASVG, § 27 B-KUVG, § 43 GSVG, § 41 BSVG, § 17 NVG) nicht berührt.

(2) Auskünfte über personenbezogene Daten sind außerhalb des Versicherungsverhältnisses des Betroffenen sowie außerhalb gesetzlicher oder vertraglicher Beziehungen (§ 42 ASVG, § 338 Abs. 4 ASVG u. a.) nach dem DSG 2000 und dieser Verordnung zu erteilen, soweit sich der Auskunftsberechtigte nicht ausdrücklich auf eine andere Rechtsgrundlage beruft, z. B. auf das Auskunftspflichtgesetz, BGBl. Nr. 287/1987.

Richtigstellung oder Löschung

§ 18. (1) Eine logische Richtigstellung oder Löschung (§ 27 DSG 2000) von Daten hat durch solche Maßnahmen zu erfolgen, die bei einer Abfrage die Unrichtigkeit der verarbeiteten Daten angeben und auf die richtigen Daten verweisen oder den Umstand der Löschung anzeigen. Das Recht auf Richtigstellung oder Löschung umfasst keinesfalls ein Recht auf Veränderungen in Programmabläufen.

(2) Bei Daten, die für Sicherungszwecke (Sicherungskopien ohne zusätzlichen Verwendungszweck) aufbewahrt werden, ist durch geeignete Maßnahmen sicherzustellen, dass im Falle eines Rückgriffes auf diese Daten allfällige Richtigstellungen und Löschungen wirksam bleiben.

(3) Daten, die für Zwecke der Dokumentation (z. B. Versicherungszeiten, Meldungsdaten nach den §§ 33 ff. ASVG) oder der internen Kontrolle aufbewahrt werden müssen, dürfen nur durch einen zweckentsprechenden Vermerk richtig gestellt werden. Solche Daten dürfen vor Ablauf der für sie geltenden Aufbewahrungsfrist nur dann physisch richtig gestellt oder gelöscht werden, wenn sie für ihre ursprünglichen Dokumentations- und Kontrollzwecke nicht mehr benötigt werden.

(4) Das Recht auf Richtigstellung betrifft nur solche Daten, deren Richtigkeit für den Zweck der Datenanwendung von Bedeutung ist; eine bloße Unvollständigkeit, die angesichts des Verwendungszwecks der Daten keine inhaltliche Änderung hervorrufen würde, bewirkt noch keinen Berichtigungsanspruch; insbesondere begründet ein Verlangen nach Ergänzung von Titeln oder akademischen Graden außerhalb der für die Führung dieser Bezeichnungen geltenden Rechtsvorschriften keinen Richtigstellungsanspruch.

(5) Der Beweis der Richtigkeit der Daten im Sinn des § 27 Abs. 2 DSG 2000 hat sich darauf zu beziehen, dass sie bei ihrer Ermittlung richtig waren oder ihre Richtigkeit (z. B. auf Grund einer unbestrittenen Dienstgebermeldung oder sonst unbedenklicher Urkunden) anzunehmen war. In solchen Fällen sind Richtigstellungen nur durch zusätzliche Anmerkungen, nicht jedoch durch Änderung der ursprünglichen Daten vorzunehmen.

(6) Mitteilungen und andere Erledigungen im Rahmen eines Richtigstellungs- oder Löschungsverfahrens sind keine Bescheide im Sinn des § 410 ASVG, auf die datenschutzrechtliche Grundlage ist im Text solcher Erledigungen ausdrücklich hinzuweisen.

(7) Ein Bestreitungsvermerk der Richtigkeit der Daten durch den Betroffenen ist nur dann beizufügen, wenn der Betroffene dies schriftlich verlangt hat.

Schlussbestimmung

§ 19. Diese Verordnung tritt nach § 31 Abs. 9a ASVG nach Ablauf des fünften Kalendertages ab dem Zeitpunkt der Freigabe der Verlautbarung zur Abfrage in Kraft. Gleichzeitig tritt die Datenschutzverordnung 1989, die in der Fachzeitschrift „Soziale Sicherheit" 1989, Seite 580, amtliche Verlautbarung Nr. 104/1989, kundgemacht wurde, außer Kraft.

Erläuterungen zum Entwurf der SV-Datenschutzverordnung 2001 für die gesetzliche Sozialversicherung (SV-DSV 2001)

I. Rechtsgrundlage

Durch das DSG 2000 ist die generelle Verpflichtung zur Erlassung von Datenschutzverordnungen weggefallen, dies wird (im Vorblatt zur Regierungsvorlage 1613 BlgNR XX GP, S. 29, Z 4) mit „Einsparungen vor allem für die Auftraggeber des öffentlichen Bereiches“ begründet. Dies vor dem Hintergrund, dass die ursprünglich in § 9 Abs. 2 DSG vorgesehenen Datenschutzverordnungen der aufsichtsbehördlichen Genehmigung und der Anhörung der Datenschutzkommission bedurften, was in Summe einen - wie die Praxis zeigt - vermeidbaren Verwaltungsaufwand nach sich zog.

Durch die Änderung des § 31 Abs. 12 ASVG durch das SRÄG 2000 ist der Hauptverband wie bisher verpflichtet, eine Datenschutzverordnung für alle Sozialversicherungsträger zu erlassen. Durch diese Sonderbestimmung des § 31 Abs. 12 ASVG sollen Verwaltungsvereinfachung und Einheitlichkeit der Vollzugspraxis weiterhin sichergestellt werden, angesichts der großen Bedeutung sozialversicherungsrechtlicher Datenspeicherungen ist es angezeigt, auch deren Rechtsgrundlagen möglichst transparent zu gestalten.

Grund des § 31 Abs. 9 ASVG war ursprünglich, zu vermeiden, dass jeder Sozialversicherungsträger für sich eine Datenschutzverordnung zu erlassen hätte (dies war früher in § 9 Abs. 2 DSG vorgesehen).

Es wird daher wie bisher eine Datenschutzverordnung des Hauptverbandes erlassen, welche bewirken soll, dass die grundlegenden Begriffe des österreichischen Datenschutzrechtes bei den Sozialversicherungsträgern einheitlich angewendet und ausgelegt werden.

Rechtsgrundlagen der Verordnung sind neben § 31 Abs. 12 ASVG die Bestimmungen über die Koordinationsfunktion des Hauptverbandes in § 31 Abs. 2 Z 3 ASVG (Richtlinien „...zur Einheitlichkeit der Vollzugspraxis der Sozialversicherungsträger...“) und im EDV-Bereich (§ 31 Abs. 5 Z 4 ASVG - Zusammenarbeit auf dem Gebiet der EDV und § 31 Abs. 5 Z 7 ASVG - Erhebung und Verarbeitung von Daten aller nach Bundesgesetzen versicherten Personen und Leistungsbeziehern) sowie die allgemeine Verordnungsgrundlage in Art. 18 Abs. 2 B-VG.

Zuständig für die Beschlussfassung über die Datenschutzverordnung ist die Geschäftsführung des Hauptverbandes (§ 442b ASVG bzw. die ansonsten bestehenden Aufgaben des Verwaltungsrates nach § 442a ASVG).

Die Erlassung des Textes als Verordnung belegt, dass die Rechtswirkungen dieses Textes über die bloße sozialversicherungsinterne Koordination hinaus gehen, was angesichts der zentralen Stellung der Datenspei-

cherung der österreichischen Sozialversicherung und der Außenwirkung datenschutzrechtlicher Regelungen (insbesondere hinsichtlich der Auskunftsrechte) angemessen erscheint.

Allerdings kann die Datenschutzverordnung des Hauptverbandes allgemeine (und daher auch in anderen Vollziehungsbereichen anzuwendende) Begriffe des Datenschutzrechts nicht allgemein rechtsverbindlich definieren, weil dies Bindungswirkungen außerhalb des Vollzugsbereiches der Sozialversicherung auslösen könnte.

Das Bundeskanzleramt hat diesbezüglich im Begutachtungsverfahren empfohlen, in der Verordnung nur jene Teile zu regeln, welche tatsächlich für Regelungen mit Außenwirkung in Frage kommen und jene Teile, welche den Charakter einer Verständnisanleitung für die Bediensteten der Sozialversicherungsträger haben, in den Erläuterungen darzustellen.

Diese Vorgangsweise wurde daher nach Abschluss des Begutachtungsverfahrens eingeschlagen. Auf diese Weise bleiben die vorgesehenen Detaillierungen und die in ihnen enthaltenen Gedanken offen gelegt, ohne jedoch normative Wirkung zu entfalten.

Eine Reihe von Bestimmungen ist aus der bisher geltenden Verordnung, kundgemacht in SozSi 1989, Seite 580, amtliche Verlautbarung Nr. 104/1989, übernommen; diese Bestimmungen werden nicht eigens erläutert (Beschluss des damals zuständigen Präsidialausschusses des Hauptverbandes vom 24. April 1989, Erlass des Bundesministeriums für Arbeit und Soziales vom 3. Oktober 1989, Zl. 26.498/16-5/89).

II. Keine Definitionen im Verordnungstext

Im ursprünglichen Begutachtungsentwurf waren eine Reihe von Definitionen vorgeschlagen, was sich im Begutachtungsverfahren nicht als zweckmäßig herausstellte (siehe Einleitung). Die Definitionen wurden daher (nicht zuletzt auf Vorschlag des Datenschutzrates) aus dem Verordnungstext entfernt.

Sie werden im Rahmen dieser Erläuterungen angeführt, weil sich aus ihnen bzw. den Einwänden dagegen Rückschlüsse auf die Auslegung des DSG gewinnen lassen (und sei es, dass eine bestimmte Auslegung aus einem hier genannten Grund nicht angewendet werden dürfte). Diese Vorgangsweise vermeidet im übrigen Diskussionen darüber, ob und inwieweit überhaupt Bestimmungen aus Rechtsvorschriften der Europäischen Union (hier: Datenschutzrichtlinie 95/46/EG) in innerstaatlichen Rechtsvorschriften der Mitgliedstaaten unterschiedlich näher ausgeführt werden dürften.

Zu einzelnen Definitionen des ursprünglichen Entwurfes

„Indirekt personenbezogene Daten“

Zur Diskussion stand im Begutachtungsverfahren folgender Standpunkt:

„Indirekt personenbezogene Daten“ im Sinn des § 4 Z 1 DSG 2000 liegen auch dann vor, wenn Datenbestände nur mit Versicherungsnummer, aber ohne Namen verwendet werden. Indirekt personenbezogene Daten könnten auch jene Daten sein, die in - sonst anonymisierten - Statistiken als Ergebnisse für Personengruppen von weniger als fünf Mitgliedern aufscheinen.

Gegen das Abstellen auf die statistische Wahrscheinlichkeit der Ermittlung des Betroffenen wurden Einwände erhoben, weil § 4 DSG 2000 sensible Daten ausschließlich nach deren Inhalt beurteile. Die in statistischen Zusammenhängen übliche Praxis (Nichtbekanntgabe von Werten kleiner Gruppen) kann damit zwar im Einzelfall eine vorsichtshalber anzuwendende Vorgangsweise bilden, aber nicht Normtext sein.

Die Definition der indirekt personenbezogenen Daten nennt im Sinn der Regierungsvorlage ausdrücklich zwei Hauptfälle solcher Daten: Es ist in der Praxis oft notwendig, personenbezogene Daten zu übermitteln (z. B. zur Prüfung volkswirtschaftlicher Auswirkungen oder für Gutachten), wobei für den Übermittlungsempfänger allerdings nur der Sachverhalt, nicht jedoch die konkrete Einzelperson relevant ist. In solchen Fällen werden Datenbestände mit Versicherungsnummer, aber ohne Namen (oder mit Geburtsdaten und nur den ersten Stellen des Familiennamens und Vornamens etc.) übermittelt. Dies deswegen, weil zur Prüfung der Plausibilität der Berechnungsergebnisse von der übermittelnden Stelle auf die tatsächlichen Datenbestände zurückgegriffen werden können muss. Dies ist insbesondere auch bei der Evaluierung von Maßnahmen im Gesundheitswesen notwendig (Bedarfsplanung von Krankenanstalten etc.).

Ein weiterer Fall indirekt personenbezogener Daten sind Statistiken, in denen (aus welchen Gründen immer) in einzelnen Feldern nur sehr geringe Personenzahlen vorkommen. Bisher war in solchen Fällen eine Angabe unzulässig (und damit die Statistik allenfalls wesentlich entwertet, falls dieser Fall in mehreren Situationen vorkam). Nunmehr können die konkreten Daten angeführt werden, weil sie zwar für den Bearbeiter der Statistikblätter, nicht aber für Außenstehende nachvollziehbar sind.

„Anonymisierte Daten“

Zur Diskussion stand im Begutachtungsverfahren folgender Standpunkt:

„Anonymisierte Daten“ sind nur Daten, die keinesfalls (auch nicht mit hohem technischen Aufwand) auf eine in ihrer Identität bestimmte Person zurückgeführt werden können.

Gegen diese Sichtweise erhoben sich im Begutachtungsverfahren keine Bedenken.

„Sensible Daten“

Zur Diskussion stand im Begutachtungsverfahren folgender Standpunkt:

„Sensible Daten“ im Sinn des § 4 Z 2 DSG 2000 liegen dann nicht vor, wenn ein Betroffener nur auf Grund statistischer Wahrscheinlichkeit ermittelt werden kann und danach mehr als fünf Personen Betroffene sein könnten. Der Begriff „Sensible Daten“ ist nach dem Verständnis- und Interpretationshorizont des durchschnittlichen Empfängers im jeweiligen Anwendungskontext auszulegen.

Die Formulierung, dass der Begriff sensible Daten nach dem Verständnis- und Interpretationshorizont des durchschnittlichen Empfängers im jeweiligen Anwendungskontext auszulegen ist, entspricht dem Kommentar zur EG-Datenschutzrichtlinie (Dammann-Simitis, EG-Datenschutzrichtlinie, Nomos 1997, Seite 162).

Es soll damit das - auch weiterhin unbestrittene - Motiv berücksichtigt werden, wonach nicht alle Daten, die „irgendwie“ in die Nähe des Gesundheits- oder eines sonstigen sensiblen Bereiches kämen, schon deswegen selbst als sensibel behandelt werden müssen. Dies wird mit folgenden Beispielen belegt:

Die Angabe „Mann, Angestellter, Österreicher, geboren 1945“ lässt es in Verbindung mit der Volksgesundheitsstatistik Österreichs z. B. zu, mit einer bestimmten Wahrscheinlichkeit das Vorliegen bestimmter Erkrankungen (Alterserscheinungen, Krebshäufigkeit, etc.) und damit Gesundheitsdaten zu ermitteln. Die Aussage, dass ein Mann mit diesen Daten „mit der Wahrscheinlichkeit XY %“ in den nächsten Jahren an Krebs sterben wird, wäre zwar statistisch-wissenschaftlich richtig, ist aber kein sensibles Datum im Sinn personenbezogener Datenspeicherung - andernfalls wären nahezu alle Angaben des täglichen Lebens „sensibel“, weil aus ihnen in irgendeiner Form/Wahrscheinlichkeit immer auf ein gesundheitsrelevantes Datum geschlossen werden kann (Benützung eines öffentlichen Verkehrsmittels im Berufsverkehr gleichbedeutend mit Nichtinvalidität, Gesundheit, etc.?).

Ebenfalls kann z. B. aus der Aussage „Bezieher von Krankengeld“ mit einer statistisch relevanten Sicherheit darauf geschlossen werden, dass der/die Betreffende an einer Krankheit leidet, welche schon länger (nämlich über die Entgeltfortzahlungsfristen des Arbeitsrechts hinaus) andauert und somit eine Aussage über ein wesentliches Gesundheitsdatum (nämlich den allgemeinen Gesundheitszustand dieser Person) getroffen werden, obwohl die Aussage als solche lediglich einen Leistungsbezug nach den §§ 138 ff. ASVG bezeichnet. Ein Schluss auf ein Dienstverhältnis wäre nicht zulässig, weil Krankengeldbezug ein solches nicht zwingend voraussetzt (vgl. § 41 AlVG). Gleiches gilt für die Begriffe „Bezieher einer Berufsunfähigkeitspension“ (hier wird der Gesundheitszustand nur durch die für diese Leistung notwendige Angestellteneigenschaft näher definiert), Wochengeldbezug (Hinweis auf Zeugungs- und Gebärfähigkeit), Karenzgeldbezug, etc.

Diese Sichtweise wird in der deutschen Literatur vertreten (vgl. Brühann: Erläuterungen zu Art. 8 der EG-Richtlinie, RZ 9, in „Das Recht der Europäischen Union“, Bd. 2 - Sekundärrecht, A - Verbraucher- und Datenschutzrecht, herausgegeben von Manfred Wolf, Verlag Beck, 16. ErgLfg. München 2000) und ist auch deswegen gerechtfertigt, weil das Faktum „finanzielle Situation“ ausdrücklich nicht (auch nicht in der EG-Richtlinie) zu den sensiblen Daten gerechnet wird. Angaben, welche einerseits gesundheitsorientierte, andererseits finanzielle Daten betreffen (gemischte Aussagen), müssen von den „rein sensiblen“ Angaben (z. B. Diagnosen, Heilmittelverbrauch) getrennt werden.

Ähnliches gilt für andere Bereiche, wie z. B. die Aussage „österreichischer Staatsbürger“: dies bedeutet in der Praxis eine Aussage über die (hohe) Wahrscheinlichkeit einer bestimmten „rassischen und ethnischen Herkunft“, stellt aber im allgemeinen Zusammenhang dennoch kein sensibles Datum dar (vor dem jeweiligen Anwendungskontext, z. B. der Anwendung des § 3 Abs. 2 lit. a ASVG oder eines internationalen Sozialversicherungsabkommens).

„Datei“

Zur Diskussion stand im Begutachtungsverfahren folgender Standpunkt:

„Datei“ im Sinn des § 4 Z 6 DSG 2000 ist eine strukturierte Sammlung von personenbezogenen Daten. Der Begriff umfasst nicht nur die computergestützte Datenverarbeitung, sondern auch die manuelle Datenanwendung nach einem Suchkriterium (z. B. Karteikästen, Listen). Eine strukturierte Sammlung ist dann vorhanden, wenn eine nach einheitlichen Kriterien vorhandene Ordnung der Daten auch ohne Verwendung zusätzlicher Programmabläufe erkennbar ist.

Keine Dateien im Sinn des DSG - wenn sie nicht nach bestimmten Kriterien strukturiert sind (vgl. Art. 2c der EG-Datenschutzrichtlinie 95/46/EG) - bilden daher

- Aktenablagen oder Archive, die nach Aktenzahlen, Datumsangaben, Sitzungsnummer, etc. sortiert sind,
- Textverarbeitungssysteme, Tabellenkalkulationssysteme, die auch personenbezogene Daten enthalten,
- Sachverständigengutachten, die in einem Zivilprozess erstattet wurden sowie

- Hilfsunterlagen wie Bibliothekssuchprogramme, Zettelkästen oder elektronische Fahrtenbücher, die nur zur Erschließung des Inhalts von Datenbeständen oder der Dokumentation nicht personenbezogen strukturierter Abläufe dienen.

Dem oben genannten Zitat aus der Datenschutzrichtlinie „...nur insoweit ausgenommen sind, als sie nicht nach bestimmten Kriterien strukturiert...“ kann jedenfalls die Ansicht entnommen werden, dass im umgekehrten Fall (keine Strukturierung nach bestimmen Kriterien) nicht von vornherein jede Textverarbeitungs-Speicherung unter den Begriff der Datensammlung fällt. Es kommt hier auf die - im Detail noch ungeklärte - Auslegung des Wortes „strukturiert“ an.

Bis zu einer eindeutigen Entscheidung erscheint die Ansicht vertretbar, eine nicht personenbezogen, sondern nach Datum oder Arbeitsgebieten organisierte Aufteilung von Textverarbeitungsdokumenten sei keine strukturierte Datei im Sinn des DSG 2000. Dass nach dem heutigen Stand der Technik jede Datensammlung mit mehr oder weniger Aufwand in eine personenbezogene Strukturierung umgeordnet werden kann, macht den zu Grunde liegenden Datenbestand nicht von vornherein zu einer personenbezogen strukturieren Daten im Sinn des Datenschutzrechts (vgl. die diversen Such-/und Sortierungsmöglichkeiten des Explorerprogrammes der Microsoft-Office Bürosoftware oder die Suchfunktionen der Internet-Suchmaschinen: in beiden Fällen ist es mehr oder weniger einfach, eine personenbezogene sortierte Liste der gefundenen Dateien zu erstellen). Das Gleiche gilt für die Verzeichnisse von Internet-Browsern (Netscape Navigator, Microsoft Explorer usw.) oder speziellen e-mail Programmen wie z. B. Lotus Notes mit seinen diversen Archivfunktionen.

Ein anderes Auslegungsergebnis dahin, dass jede elektronische Textdatei, die von einem frei wählbaren Programm personenbezogen sortiert werden könnte, bereits eine „strukturierte“ Datei wäre, würde bewirken, dass es in der Praxis keine unstrukturierten Dateien mehr gibt, weil die Sortierprogramme bereits einen hohen Stand erreicht haben und de facto alle Dateien „sortiert“ werden könnten. Damit wäre der gesetzliche Unterschied obsolet, was dem - 2000 beschlossenen - DSG nicht unterstellt werden dürfte.

Diese erläuternden Bemerkungen beziehen sich auf die OGH-Entscheidung 6 Ob 148/00h vom 28. 6. 2000, die (wohl zu verallgemeinernd) zu dem Ergebnis kommt, dass eine Struktur der Sammlung dann vorliegt, wenn sie - im Gegensatz zu einem Fließtext - eine äußere Ordnung aufweist, nach der die verschiedenen Arten von Daten in einer bestimmten räumlichen Verteilung auf dem oder den manuellen Datenträgern oder in einer bestimmten physikalischen oder logischen Struktur dargestellt sind. Darüber hinaus müssen die Daten nach bestimmten Kriterien zugänglich sein, d. h. es bestehen vereinfachte Möglichkeiten der inhaltlichen Erschließung, beispielsweise durch alphabetische oder chronologische Sortierung oder durch automatisierte Erschließungssysteme.

Es ist für die Wahrnehmung des Auskunftsrechts jedenfalls auch bedeutsam, dass es nicht Sinn des Datenschutzgesetzes sein kann, vermeidbaren Aufwand zu verlangen, im Gegenteil: Die Mitwirkungspflicht des Betroffenen nach § 26 Abs. 3 DSG 2000 hat ausdrücklich das Ziel, „ungerechtfertigten und unverhältnismäßigen Aufwand beim Auftraggeber zu vermeiden“. In diesem Sinn wurde die Mitwirkungspflicht des Betroffenen im Rahmen der SV-DSV näher definiert. Keinesfalls führt der Entfall der ursprünglichen Definition des Entwurfes dazu, dass auf Grund eines Auskunftsersuchens von vornherein alle (vielleicht tausende) PC-Festplatten (einschließlich Laptops) eines großen Betriebes nach möglicherweise vorhandenen personenbezogenen Daten durchsucht werden müssten.

„Zustimmung des Betroffenen“

Zur Diskussion stand im Begutachtungsverfahren folgender Standpunkt:

„Zustimmung des Betroffenen“ im Sinn des § 4 Z 14 oder des § 8 Abs. 1 Z 2 DSG 2000 muss nicht ausdrücklich und schriftlich vorliegen, sie kann auch stillschweigend (konkludent) erteilt sein.

Für eine solide Absicherung des Auftraggebers wird, soweit nicht ohnedies eine gesetzliche Ermächtigung vorhanden ist (z. B. nach § 42, § 338 Abs. 3, § 460e ASVG usw.), aus Gründen der Beweissicherung jedoch eine ausdrückliche schriftliche Zustimmung anzustreben sein.

„Zwang“

Zur Diskussion stand im Begutachtungsverfahren folgender Standpunkt:

„Zwang“ im Sinn der Bestimmungen über die datenschutzrechtliche Zustimmung ist als unrechtmäßiger oder seinem Ausmaß nach ungerechtfertigter Zwang zu verstehen. Die Einhaltung rechtmäßig geltender Verpflichtungen begründet keinen Zwang im Sinn des DSG 2000.

Daraus hätte sich ergeben, dass die Verpflichtung, einen freiwillig abgeschlossenen Vertrag einzuhalten, keinen „Zwang“ iSd Datenschutzrechts auslöst, es sei denn, die Freiwilligkeit des Vertragsabschlusses selbst wäre zweifelhaft. Hiefür hätten jedoch konkrete Anhaltspunkte vorzuliegen. Das gilt nicht nur für Kauf- usw. Verträge, sondern auch für die einer Anwaltsvollmacht, Hausverwaltungsvollmacht und einem Kreditvertrag zu Grunde liegenden Bevollmächtigungsverträge (Vertragsklauseln), nach welchen ebenfalls personenbezogene Daten verwendet werden.

Es ging in diesem Zusammenhang nur um die datenschutzrechtliche Auslegung des Wortes „Zwang“, nicht jedoch darum, wodurch bewirkt werden kann, dass eine dem Vertragsverhältnis fremde Stelle einem Vertragspartner Auskünfte gibt oder andere Dienste leistet. Dies wäre nach den jeweils hiefür geltenden Rechtsvorschriften zu beurteilen.

Das Erfordernis „ohne Zwang abgegebene Willenserklärung“ ist (auch) vor dem Hintergrund wirtschaftlicher oder gesellschaftlicher Zwänge zu sehen; die ausdrückliche Definition sollte dies ursprünglich klarstellen. Ein Zwang liegt dann nicht vor, wenn die Zustimmung abgegeben wird, um bestimmte Leistungen des täglichen Lebens zu erhalten (eine Wohnung, einen Kredit, die Übernahme in ein unkündbares Dienstverhältnis, etc.). Die Verpflichtung, eine rechtlich unbeanstandbare Situation zu bewältigen (einen Vertrag zu erfüllen, einen Antrag zu stellen, etc.) bedeutet keinen Zwang im Sinn dieser Gesetzesstelle, falls die Verpflichtung selbst nicht dazu eingegangen wurde, rechtlich vorgesehene Vorgangsweisen zu vermeiden/umgehen. Der Begriff Zwang ist auf unrechtmäßige (rechtswidrige) Vorgänge einzuschränken, gilt dann allerdings für jegliche Art von Zwang.

Allgemeine Formulierungen z. B. in vorgedruckten Vollmachtsformularen, allgemeine Geschäftsbedingungen, etc. begründen für sich allein nur dann eine ausreichende Zustimmungserklärung, wenn auf Grund konkreter Anhaltspunkte davon ausgegangen werden kann, dass dem Erklärenden dies bewusst war (vgl. § 6 KonsumentenschutzG, insbesondere Abs. 3).

Einwände:

Gegen diese Sichtweise erhoben sich Einwände, weil die Zustimmung nach dem Datenschutzrecht jederzeit zurückziehbar ist, was bei Verträgen nicht der Fall ist (Kündigungsfristen usw.).

„veröffentlicht“ oder „öffentlich zugänglich“

Zur Diskussion stand im Begutachtungsverfahren folgender Standpunkt:

Ob Daten „veröffentlicht“ (§ 8 Abs. 2 DSG 2000) oder „öffentlich zugänglich“ (§ 9 Z 1 DSG 2000) sind, ist nach dem Kreis an Öffentlichkeit zu beurteilen, für welchen die Veröffentlichung ursprünglich vorgesehen war.

Es gibt verschiedene Formen der „Öffentlichkeit“ (vgl. § 347 Abs. 5 ASVG - sog. „Parteiöffentlichkeit“, §§ 40 f. AVG 1991) je nachdem, welchen Zwecken die Offenlegung gewisser Fakten dienen soll. Was gegenüber den (vielleicht tausenden) Mitgliedern eines Vereines oder Mitarbeitern eines Unternehmens „öffentlich“ ist (z. B. bestimmte Zuständigkeiten, Funktionen, etc.), muss deswegen nicht auch bereits einer weiteren Öffentlichkeit zugänglich sein (öffentlich sind z. B. Einträge im Firmenbuch, aber nicht mehr Funktionen als Abteilungsleiter, etc.). Für Behörden und Gerichte kann als allgemein zugänglich/öffentlich die Eintragung im Amtskalender gelten, welcher jedoch nur Namen, Titel und Funktionsbereich, nicht jedoch nähere Angaben enthält.

Die Beurteilung einer Tatsache als „öffentlich“ soll entsprechend jener Öffentlichkeit zu erfolgen haben, für welche die Offenlegung ursprünglich vorgesehen war. Eintragungen in e-mailverzeichnisse eines Großunternehmens sind in der Regel tausenden Mitarbeitern zugänglich, deswegen aber noch nicht derart öffentlich, dass sie auch ohne weiteres in allgemeine Verzeichnisse („Telefonbuch für e-mail-Adressen“) aufgenommen werden dürften.

„ausdrückliche gesetzliche Ermächtigung oder Verpflichtung“

Zur Diskussion stand im Begutachtungsverfahren folgender Standpunkt:

Unter „ausdrücklicher gesetzlicher Ermächtigung oder Verpflichtung“ ist eine Bestimmung zu verstehen, deren Wortlaut die Ermächtigung oder Verpflichtung eindeutig entnommen werden kann.

Als ausdrückliche gesetzliche Ermächtigung sollte schon eine konkrete Bestimmung gelten, auch wenn die Datenarten nicht (wie in der Vergangenheit manchmal verlangt) angeführt sind (vgl. SozSi 1990, S. 438), unter der Voraussetzung, dass sich zumindest aus dem Zusammenhang (etwa aus anderen Bestimmungen im selben Gesetz) ergeben muss, welche Datenkategorien verwendet werden dürfen.

„überwiegendes berechtigtes Interesse“

Zur Diskussion stand im Begutachtungsverfahren folgender Standpunkt:

Ein „überwiegend berechtigtes Interesse“ liegt insbesondere dann nicht vor, wenn die Datenverwendung lediglich dazu dienen soll, ein gesetzlich geregeltes Verfahren zu vermeiden.

Ein überwiegend berechtigtes Interesse soll nicht als bestehend angesehen werden können, wenn z. B. jemand eine Datenübermittlung begehrt, um (sich) ein (GerichtsVerfahren zu ersparen oder Zustellungsvorschriften zu umgehen (Einschaltung von Arbeitgeber - Arbeitsplatz als Zustellort nach § 4 ZustG - und Ausforschung des Arbeitsgebers über die Krankenkasse anstatt Zustellung durch Hinterlegung, Edikt oder Kurator).

Für Adressermittlungen sei überdies auf die Meldegesetznovelle 2001, BGBl. I Nr. 28/2001 hingewiesen, mit welcher das bundesweite Melderegister in absehbarer Zeit durch § 16 und § 16a MeldeG samt einer Ab-

gleichungsmöglichkeit (aber nicht mit einer direkten Übernahme) mit den Sozialversicherungsdaten (§ 31 Abs. 4 Z 3 lit. a ASVG) eingeführt werden wird. Das Verwenden von Arbeitgeberdaten als „Melderegisterersatz“ wird dadurch noch weniger notwendig werden als bisher.

Andere Beispiele für eine - grundsätzlich abzulehnende, weil aufgabenfremde - „Fremdverwendung“ von Datenbeständen ergeben sich in folgenden Bereichen:

Wer einen rechtskräftigen Exekutionstitel besitzt, soll nicht (bevor er noch ein Exekutionsverfahren einleitet) durch Anfrage beim Sozialversicherungsträger feststellen können, ob überhaupt und wo ein entsprechendes Exekutionsobjekt (Gehalt, Pension, sonstige Leistung) vorhanden ist. Es gibt dafür keine gesetzliche Grundlage.

Wer eine andere Person sucht, soll nicht außerhalb des gerichtlichen (Abwesenheits-) Kuratorbestellungsverfahrens die Datenbestände der Sozialversicherung zu Erhebungen dahingehend nutzen können, ob und wo der/die Gesuchte zu finden ist. Gerichte sind online an die Datenspeicherung des Hauptverbandes angeschlossen, sodass sich solche Erhebungen erübrigen, vgl. SozSi 1999, S. 803 und SozSi 2000, S. 286 (das gilt auch für die Suche nach Erben in einem Verlassenschaftsverfahren).

Die Berechtigung zu Datenverwendungen kann auch nicht dazu führen, dass daraus Verpflichtungen abgeleitet werden könnten, entsprechende Auskünfte auch zu bearbeiten oder vielleicht sogar zusätzliche Programme/Programmschritte vorzusehen, welche erst die Auskunftserteilung möglich machen würden.

Amtshilfeberechtigungen sind von der Definition nicht betroffen. Rechts- und Amtshilfe bilden keine Auskünfte an den Betroffenen, sondern eigenständige rechtliche Tatbestände. In diesem Sinn bleiben die gesetzlichen Regeln z. B. des § 89h GOG über Auskünfte aus Sozialversicherungsdaten an die Gerichte unberührt. Festgehalten wird, dass eine Adressermittlung durch Anfrage bei der Sozialversicherung lediglich den Parteien untersagt ist, wohl aber dem Gericht online möglich bleiben soll. Durch die Einführung des § 89h GOG wurden die Sozialversicherungsträger (auch bei Fehlen einer expliziten Auskunftsverpflichtung) verpflichtet, den Gerichten auf deren Ersuchen Auskünfte über verfahrenserhebliche Umstände zu erteilen.

„gesetzlich übertragene Aufgaben“

Zur Diskussion stand im Begutachtungsverfahren folgender Standpunkt:

Zu den „gesetzlich übertragenen Aufgaben“ gehören im Allgemeinen, nicht aber immer, auch jene Tätigkeiten, die zur Erfüllung eines Aufgabenbereiches auf Grund der Organisation des Auftraggebers notwendig sind (Hilfsgeschäfte, z. B. Personalverwaltung, Beschaffungswesen).

Gemäß § 8 Z 4 iVm Abs. 3 Z 1 DSG 2000 ist die Verwendung von nicht-sensiblen Daten dann zulässig, wenn die Verwendung der Daten für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist. Das bedeutet aber noch nicht, dass Hilfsgeschäfte zu den „gesetzlich übertragenen Aufgaben“ selbst gehören.

„lebenswichtige Interessen“

Zur Diskussion stand im Begutachtungsverfahren folgender Standpunkt:

Eine genaue Definition erscheint derzeit nicht möglich; es wird aber jedenfalls für den Vollzugsbereich der Sozialversicherung vertretbar sein, „lebenswichtig“ nicht nur so auszulegen, dass ohne die entsprechenden Maßnahmen mit dem Tod des Betroffenen gerechnet werden müsste (Lebenserhaltungsprinzip). Daher scheint es zulässig, unter „lebenswichtig“ alles zu verstehen, was zum bisherigen Lebens-Standard des Betroffenen gehört hätte (Lebensstandardprinzip). Dies nicht zuletzt, weil z. B. sogar dem - aus wirtschaftlicher Sicht viel weniger schutzbedürftigen - Gemeinschuldner nach § 5 KO der zu einer bescheidenen Lebensführung unerlässliche Lebensunterhalt zu gewähren ist, wozu auch die Aufrechterhaltung einer Wohnung gehört und nach § 251 EO zumindest die unentbehrlichen Gegenstände exekutionsfrei sind.

Es scheint daher die Auffassung vertretbar, dass im vorliegenden Rechtsbereich „lebenswichtig“ im Sinn des DSG 2000 alles ist, was zur Aufrechterhaltung des Lebensstandards des Betroffenen unentbehrlich ist. Es wäre nicht nur das zulässig, was nach dem bürgerlichen Recht als „Geschäftsführung im Notfall“ (§ 1036 ABGB) zulässig wäre, sondern darüber hinaus alles, was als „Geschäftsführung zum Nutzen“ (§ 1037 ABGB) - der Aufrechterhaltung des Lebensstandards - zulässig ist.

Einwände:

Der Datenschutzrat lehnte diese Auslegung ab, „da der Begriff lebenswichtig' im Sinne der Richtlinie 95/46/EG restriktiv zu interpretieren ist.“

„rechtzeitig“

Zur Diskussion stand im Begutachtungsverfahren folgender Standpunkt:

Nicht im Sinn der allgemeinen Verwendung in der Rechtsordnung, sondern - angesichts der besonderen Schutzwürdigkeit sensibler Daten - enger auszulegen sein wird das Wort „rechtzeitig“ in § 9 Z 7 DSG 2000. Es

erscheint angebracht, es als „möglichst sofort, aber jedenfalls ohne unnötigen Aufschub, unverzüglich“ zu lesen.

III. Erläuterungen zu den einzelnen Bestimmungen

Zu § 1

Aufzählung der betroffenen Sozialversicherungsträger, Gliederung entsprechend der Satzung des Hauptverbandes.

Aus datenschutzrechtlicher Sicht sind die Tätigkeitsbereiche (Verantwortungsbereiche) Auftraggeber, Dienstleister und Betreiber des Informationsverbundsystemes ausdrücklich zitiert. Diese Zitate tragen der Tatsache Rechnung, dass datenschutzrechtliche Normen häufiger (als z. B. Regeln des Versicherungsrechts, welches im Allgemeinen nur von Beschäftigern/meldepflichtigen Stellen angewendet wird) von Privatpersonen zur Wahrung von deren Rechten auf Auskunft gelesen werden (vgl. den Zweck der Einleitungsbestimmungen oder Präambeln anderer Rechtstexte).

Auf Vorschlag des Datenschutzrates (Brief vom 21. März 2001, GZ K817.173/002-DSR/01) wird ausdrücklich festgehalten, dass die Verordnung auch den so genannten „Grundrechtsbereich“ des Datenschutzes umfasst, also jenen Bereich, für den der Bund - weil kein automationsunterstützter Datenverkehr erfolgt - keine Gesetzgebungskompetenz besitzt (§ 2 Abs. 1 DSG 2000). Dies ist keine bloß theoretische Klarstellung, weil Sozialversicherungsträger auch Landesrecht zu vollziehen haben können, z. B. bei der Beitragseinhebung landesgesetzlich eingerichteter Einrichtungen (Landarbeiterkammern, vgl. § 50 Abs. 3 oöLAKG, oöLGBl. Nr. 13/1997) oder im Krankenanstaltenrecht (vgl. § 460e ASVG letzter Satz).

Später hielt der DSR allerdings (Brief vom 2. Juli 2001, GZ: K817.173/004-DSR/01) fest: „Die hier vorgenommene Interpretation scheint nicht zutreffend und wirft kompetenzrechtliche Probleme auf. Es ist davon auszugehen, dass der Anwendungsbereich der Verordnung auf manuell verwendete Daten, die für Zwecke solcher Angelegenheiten verwendet werden, in denen die Zuständigkeit zur Gesetzgebung Bundessache ist, ausgedehnt werden kann.“

Eine Interpretation, welche die Anwendung der Datenschutzverordnung formell auch auf Bereiche landesrechtlicher Vollziehung ausdehnt, scheint damit nicht möglich.

Zu § 2 Abs. 1

Die Dienstleisterstellung des Hauptverbandes gründet sich formal auf § 31 Abs. 11 ASVG, sowie inhaltlich auf § 31 Abs. 4 ASVG, nach welchem der Hauptverband Versicherungsnummern zu vergeben (§ 31 Abs. 4 Z 1 ASVG) und eine gemeinsame Datenspeicherung der Sozialversicherungsdaten zu führen hat (§ 31 Abs. 4 Z 3 ASVG).

Die Aufzählung der Aufgabenbereiche in § 2 Abs. 1 des Entwurfes nennt die grundlegenden Tätigkeitsbereiche des Hauptverbandes, welche von der Verwaltung der Versicherungsdaten bis hin zur Unterstützung von Ausgleichsverrechnungen und Leistungsabrechnungen reichen (vgl. §§ 70 f., §§ 315 ff. ASVG, nach dem Krankenanstaltenrecht - § 447f ASVG oder den Ausgleichsfonds nach §§ 447a ff. ASVG).

Die Datenspeicherung beim Hauptverband ist so organisiert, dass jeder dem Hauptverband angehörende Sozialversicherungsträger die beim Hauptverband gespeicherten Daten im Rahmen seiner gesetzlichen Zuständigkeiten benützen darf (z. B. bei der Zusammenrechnung von Pensionsversicherungszeiten als Arbeitnehmer und Selbstständiger in der Pensionsversicherung - § 251a ASVG, § 129 GSVG, § 120 BSVG, bei der Berücksichtigung von Vorversicherungszeiten in der Krankenversicherung § 121 Abs. 4 Z 1 ASVG usw. oder bei der Ermittlung von Bemessungsgrundlagen der Unfallversicherung nach § 178 Abs. 1 ASVG). Es handelt sich um ein Informationsverbundsystem nach § 50 DSG 2000.

Die beim Hauptverband gespeicherten Daten stammen aus den Meldungen der Versicherungsträger, welche ihrerseits wieder auf den Sozialversicherungsmeldungen (z. B. der Dienstgeber, §§ 33 ff. ASVG usw.) beruhen.

Die Datenbestände sind vom Hauptverband im Rahmen des elektronischen Verwaltungssystemes nach § 31a ASVG (ELSY-Chipkartensystem) zu verwenden - für diese Datenanwendung ist nach § 31b Abs. 4 ASVG eine eigene Verordnung nach Maßgabe der technischen Entwicklung und der volkswirtschaftlichen Zweckmäßigkeit von Chipkartensystemen zu erlassen. Die Datenschutzverordnung beschäftigt sich somit nicht weiter mit diesem Bereich.

Ebenso einer eigenen Regelung vorbehalten bleiben die schon bisher gesondert geregelten Vorgangsweisen bei der Erfassung der Pensionsversicherungszeiten und der Erhebung der Versicherungsdaten der Pensionsversicherung.

Zu § 2 Abs. 2

Ausdrücklich in § 2 Abs. 2 des Entwurfes erwähnt sind die Bestimmungen (§ 7) über die Datensicherheitsmaßnahmen im Informationsverbundsystem. Diese Bestimmungen sind für die Sozialversicherungsträger im Interesse einer einheitlichen Vorgangsweise verbindlich, was durch § 31 Abs. 6 ASVG begründet ist.

Zu § 5

Anregung zu dieser Bestimmung gab § 6 Abs. 4 DSG 2000, welcher Verhaltensregeln vorsieht. Die im Textentwurf enthaltenen Grundsätze fassen die Grundlagen der bisherigen Datenverwendung der Sozialversicherung zusammen, wozu insbesondere auf § 5 Abs. 2 Z 3 hinzuweisen ist:

Es kam in der Vergangenheit (im Rahmen von Amtshilfeersuchen, etc.) immer wieder vor, dass ersuchende Stellen sich bloß darauf beriefen, eine Datenübermittlung an sie sei „zulässig", ohne konkrete Gründe für die Datenverwendung zu nennen. Dies wurde nicht als ausreichende Rechtsgrundlage für Auskünfte aus Sozialversicherungsdaten angesehen, es war stets eine zusätzliche gesetzliche Bestimmung oder ein sonst vorliegender konkreter Anlass für die Datenverwendung zu nennen.

Nicht alles, was datenschutzrechtlich zulässig ist, führt auch schon zu einer Verpflichtung der Sozialversicherung, ihre Daten hiefür bereitzustellen.

Dieser Linie folgt auch die Präzisierung zum Begriff der „gelindesten Mittel" des Grundrechtseingriffs, wie er in Z 6 näher erläutert wird.

Nach bisherigen Erfahrungen mit der Rechtsprechung der Datenschutzkommission kann allerdings nicht davon ausgegangen werden, dass Gesichtspunkte der Verwaltungsökonomie jedenfalls auch die Übermittlung nicht relevanter Daten unbedenklich machen würden. Beim Hauptverband wurde in diesem Zusammenhang in die Wege geleitet, möglichst flexible Auskunftsprogramme bzw. Zugriffsmöglichkeiten zu schaffen, um zumindest häufig auftretenden Übermittlungsbedarf jeweils konkret auf die notwendigen Daten eingegrenzt bearbeiten zu können, ohne die Vorteile der EDV zu verlieren.

Zu § 5 Abs. 2 Z 4

Die Formulierung „mit an Sicherheit grenzender Wahrscheinlichkeit" bezieht sich auf jene in der Praxis aufgetretenen Fälle, in denen teilweise über Jahrzehnte zurück Leistungsansprüche hätten zuerkannt werden können (§ 547 Abs. 4 ASVG: im Jahr 1990 rückwirkend bis 1955).

Mit solchen Fällen soll nicht gerechnet werden müssen, weil dies dazu führen würde, dass alle irgendwann ermittelten Daten auf Dauer aufzubewahren wären, weil nie mit Sicherheit ausgeschlossen werden könnte, dass nicht irgendwann in ferner Zukunft eine gesetzliche Regelung getroffen würde, für deren Vollziehung eine Angabe wichtig werden könnte. Als absehbar wird eine Änderung dann anzusehen sein, wenn für sie bereits Novellierungsvorschläge, Anregungen des Rechnungshofes, Entschließungsanträge, usw. vorhanden sind, mag auch noch kein Begutachtungsentwurf einer Novelle erstellt worden sein.

Andererseits ist damit zu rechnen, dass relativ häufig (auch mehrere) Jahre nach dem Tod eines Versicherten Ansprüche auf Hinterbliebenenleistungen geltend gemacht werden, sodass eine sofortige Löschung der Daten einer Person nach deren Tod (vgl. § 360 Abs. 5 ASVG) zu früh wäre. Eine zeitliche Grenze für solche Fälle wird aus Sicherheitsgründen weit zu ziehen sein, derzeitige Praxis ist eine Löschung 20 Jahre nach dem Tod einer Person oder frühestens 110 Jahre nach dem Geburtstag einer Person, wenn mindestens seit 20 Jahren keine Angaben mehr vorhanden sind (eine ähnliche Regelung existiert bereits: vgl. Punkt 3.1 der Richtlinien des Hauptverbandes zur Erhebung von Pensionsversicherungsdaten ab 1972, SozSi 1978, S. 331).

Eine Verpflichtung zur Datenlöschung ist ein erheblicher Unterschied zur Möglichkeit der Löschung nach Fristablauf. In manchen EDV-Programmen ist eine Löschung (z. B. von Zwischenspeichern) nicht eigens vorgesehen. Es wird daher nur vorgesehen, dass nicht mehr benötigte Daten möglichst rasch zu löschen sind: zu berücksichtigen war, dass manche noch immer laufende Programme - wie das Begutachtungsverfahren ergab - keine leicht durchführbaren Löschungsroutinen (von Arbeitsdateien, etc.) besitzen.

Kontrollmaßnahmen sind jedenfalls der jeweiligen Datenverarbeitung anzupassen: Hiezu hat sich bewährt, dass Zugriffe durch Zufallsprogramme ausgewählt und dann konkret nachvollzogen werden. Dies geschieht bereits seit Jahren bei den Datenübermittlungen des Hauptverbandes in dessen Funktion als Dienstleister der Sozialversicherungsträger nach § 31 Abs. 11 ASVG.

Zu § 5 Abs. 2 Z 6

Daten dürfen vom Auftraggeber im Rahmen des § 7 Abs. 2 DSG 2000 unter Beachtung des § 32 DSG 2000 und des § 81 ASVG, § 27 B-KUVG, § 43 GSVG, § 41 BSVG sowie des § 17 NVG übermittelt werden. Die hier genannten Bestimmungen über die Verwendung finanzieller Mittel der Sozialversicherung bewirken u. a. dass die Organisation der Sozialversicherung (und damit die Beiträge der Dienstnehmer, Dienstgeber und des Bundes) nicht für die Organisation von Auskunftsstellen verwendet werden dürfen. Ansonsten wäre es z. B. möglich, die Beschäftigungsdaten der Sozialversicherung als Adressdatenbestände (Zustellorte nach § 4 Zustellgesetz) zu verwenden, obwohl zur Ermittlung von Adressen (Meldedaten) das Melderegister nach § 16 Meldegesetz aus dem Budget des Innenressorts organisiert ist.

Zu § 7

Nach § 50 Abs. 1 DSG 2000 trifft den Betreiber eines Informationsverbundsystems die Verantwortung für die notwendigen Maßnahmen der Datensicherheit (§ 14 DSG 2000) in diesem System.

Im Begutachtungsverfahren wurde noch der Hinweis gegeben, dass der Hauptverband als Betreiber des SV-Informationsverbundsystems eigene Datensicherheitsvorschriften für die in diesem System Tätigen erlas-

sen wird. Aus systematischen Gründen und um eine Einheitlichkeit der Datenschutzvorschriften zu gewährleisten, wurden die detaillierten Regelungen zur Datensicherheit nunmehr doch in § 7 aufgenommen.

Die verbindlichen Bestimmungen in § 7 des Entwurfes sollen insbesondere dem § 14 DSG 2000 Rechnung tragen.

Zu § 7 Abs. 5 Z 2

Es soll sichergestellt werden, dass der Zugriffsschutz zu personenbezogenen Daten bzw. die Datensicherheitsmassnahmen nicht auf den Stand ihrer Einführung „eingefroren" bleiben, sondern ständig kontrolliert und gegebenenfalls verbessert werden.

Aus der Dokumentation über die erteilten Zugriffsberechtigungen muss sich (für etwaige Überprüfungen) ergeben, welcher Benutzer in welchen Zeitraum Zugriff auf welche Daten hatte. Im Falle der Beendigung einer Zugriffsberechtigung darf der Benutzername daher auch nicht „gelöscht" werden, sondern es ist das Ende der Zugriffsberechtigung zu vermerken.

Zu § 7 Abs. 5 Z 4

Es muss gewährleistet sein, dass Zugriffsberechtigungen auf Datenverwendungen nicht von vornherein unkontrolliert auf Dauer angelegt werden und diese auch im Bedarfsfalle gesperrt werden.

Zu § 7 Abs. 5 Z 5

Dem datenschutzrechtlichen Erfordernis, soweit als möglich die Einsicht von Außenstehenden auf Datenverwendungen des Hauptverbandes zu verhindern, soll durch diese Bestimmung Rechnung getragen werden.

Zu § 7 Abs. 5 Z 7

Z 7 trifft die Anordnung, dass bereits „an vorderster Front" bei den Eingabegeräten (Viren- bzw. sonstige) Schutzprogramme, die die meisten Softwareprodukten ohnehin teilweise bereits standardmäßig enthalten, die Vernichtung oder Veränderung der Daten hintanhalten sollen.

Da solche Schutzprogramme aber relativ rasch an Aktualität und damit an Wirksamkeit verlieren, ist auch vorzusehen, dass diese Programme entsprechend nachgerüstet werden.

Zu § 7 Abs. 5 Z 8

Z 8 soll verhindern, dass Berechtigungskennungen oder sonstige Daten, die sich auf Festplatten von PCs befinden, von Unberechtigten „gelesen" oder missbraucht werden können, wenn diese Geräte verkauft bzw. wegen technischer Veralterung endgültig ausgeschieden werden.

Zu § 7 Abs. 5 Z 9

Wie es in Netzwerken bereits gängiger Standard ist, soll Z 9 nur der Vollständigkeit halber anführen, dass ein Zugriff nur nach Eingabe einer Benutzerkennung und eines Kennwortes möglich sein soll.

Die Regelung, dass ein Kennwort nur aus einer Kombination aus Buchstaben und Ziffern oder Sonderzeichen bestehen sollte, dient der Sicherheit vor Passwort-Hackern:

Viele Benutzer verwenden (um eine höhere Merkbarkeit zu erreichen) „gängige" Wörter (z. B. Städtenamen) oder den Vornamen von Ehepartner, Kindern etc. - dies gefährdet aber die Sicherheit von Kennwörtern. Hacker, die Kennwörter „knacken" wollen, verwenden in der Regel Programmroutinen, die nach Wörtern aus dem Duden, Vornamen, Städte etc. suchen. Durch die Verwendung von Kombinationen mit Buchstaben und Zahlen und/oder Sonderzeichen müssten die Programmroutinen von Hackern ein Vielfaches von Kombinationen durchforsten, um gegebenenfalls auf diese Weise zu einem Passwort zu kommen. Dieser Aufwand wäre aber so hoch, dass auf diese Weise mehr Sicherheit besteht, dass davon Abstand genommen wird.

Die Ungleichheit des Passwortes mit der Benützerkennung könnte dadurch gewährleistet werden, dass ab einer Übereinstimmung von 50% die Passwort-Vergabe nicht mehr erlaubt ist.

Auf die Verwendung von Kombinationen mit Buchstaben und Zahlen und/oder Sonderzeichen bei der Kennwortvergabe sollte nur aus schwer wiegenden technischen Gründen verzichtet werden, wobei der Ankauf eines neuen bzw. eine Umprogrammierung eines bestehenden Softwareproduktes für sich genommen noch kein schwer wiegender technischer Grund ist.

Zu § 7 Abs. 6

Da sichergestellt werden muss, dass die Zulässigkeit einzelner Zugriffe auch im Nachhinein überprüft werden kann, ist es notwendig, über die Benutzerverwaltung Aufzeichnungen zu führen und diese eine bestimmte Zeit hindurch aufzubewahren.

Diese Regelung setzt die in § 14 Abs. 2 Z 7 DSG 2000 vorgesehene Protokollierungspflicht um.

Zu § 7 Abs. 7

Die Verantwortlichkeit für Datensicherheitsmaßnahmen begründet auch eine bestimmte Kontrollverpflichtung des Betreibers.

Zu § 8

Angesichts der Bedeutung der Datenbestände der Sozialversicherung auch für andere Vollziehungsbereiche (§ 89h GOG usw.) und insbesondere für das Chipkartensystem nach §§ 31a ff. ASVG (vgl. die Überlegungen zur Bürgerkarte) wird die Protokollierung weiter verfeinert.

Die Protokollierungsregeln entsprechen der bewährten langjährigen Praxis im Hauptverband, welche es möglich gemacht hat, auch Jahre zurückliegende Zugriffe leicht nachzuvollziehen. Sie entsprechen weiters der Tatsache, dass es angesichts der technischen Entwicklung (vgl. die Kapazitäten von Proxy- und Cache-Servern/Speicherungen im Internet) derzeit keine wesentliche Zusatzbelastung mehr darstellt, Zugriffsdaten usw. auch in größeren Mengen aufzubewahren, bzw. längere Zeit zu speichern und einfach abfragbar zur Verfügung zu halten.

Ein weiteres, wesentlich gewichtigeres Argument für die im nunmehrigen Entwurf wenigstens für neue Programme vorgesehene detaillierte Protokollierung der Zugriffe ist der in absehbarer Zeit zu erwartende Einsatz des so genannten „elektronischen Aktes“, also der elektronischen Vorgangsbearbeitung und Archivierung:

Für die damit verbundenen Abläufe wurde bereits ein Standardprodukt der Sozialversicherung beschlossen. Im Rahmen elektronischer Aktenbearbeitung wird auf die exakte Protokollierung der Zugriffe auf den Akt großer Wert gelegt werden müssen, um den Entscheidungsablauf nachvollziehen zu können. Dies wird eine wesentlich intensivere Auseinandersetzung mit dem Thema „Protokollierung“ bedingen als es dies in den letzten Jahren üblich war. Zugriffsdaten werden in wesentlich größerer Menge protokolliert und nachvollziehbar gespeichert werden müssen als dies bisher der Fall war. Protokollierungstechnik und gespeicherte Protokolldatenmenge werden schon aus diesem Grund verfeinert bzw. erhöht werden müssen. Die Datenschutzverordnung trägt dieser Entwicklung nur Rechnung, führt aber von sich aus keine neue Entwicklung ein.

Die Sachbearbeiter/Fachabteilungen werden hievon de facto nicht betroffen sein: Die Datenschutzverordnung verlangt keine organisatorischen Umstellungen, es ist lediglich an eine automatisch mitlaufende, automationsunterstützt wiedergewinnbare Protokollierung gedacht.

Zu § 8 Abs. 1

Die Elfjahresfrist beruht darauf, dass nach dem Krankenanstaltenrecht (§ 10 Abs. 1 Z 3 KAG) Krankengeschichten mindestens zehn Jahre aufzubewahren sind, wobei damit zu rechnen ist, dass Vorgänge (Feststellungsklagen etc.), für welche Protokolldaten relevant sind, knapp vor Ende dieser Aufbewahrungsfrist eingeleitet werden und der Beweisbeschluss erst im elften Jahr gefällt wird. Eine andere Sichtweise, nämlich jene aus Richtung der Verjährungsfrist für qualifizierten Amtsmissbrauch nach § 302 Abs. 2 iVm § 57 Abs. 3 zweiter Fall StGB (zehn Jahre, zwischenstaatliche Einrichtungen [Qualifizierungsgrund] bestehen z. B. als Verbindungsstellen der internationalen Sozialversicherungsabkommen, vgl. Art. 42 Abs. 3 AbkSozSi Deutschland, BGBl. Nr. 280/1975, usw.), führt ebenfalls zu einer zehn Jahre übersteigenden Mindestfrist für die Aufbewahrung von Protokollen.

Die Obergrenze für die Aufbewahrung beruht darauf, dass das bürgerliche Recht mit dreissig Jahren allgemein die Verjährung eintreten lässt. Eine längere Aufbewahrungsdauer für Protokolle, welche sich an der Aufbewahrung der zu Grunde liegenden Daten orientiert, hätte im vorliegenden Zusammenhang zur Folge, dass Protokolle der Zugriffe auf Pensionsversicherungsdaten über die durchschnittliche Lebensdauer eines Betroffenen hinaus aufzubewahren wären (weil sich daraus Hinterbliebenenansprüche ableiten könnten), obwohl Schadenersatz- und Strafansprüche längst erloschen bzw. verjährt wären. Ein solches praktisch sinnloses Ergebnis darf dem Gesetzgeber nicht unterstellt werden und wäre nicht sachgerecht.

Da die Aufbewahrung heute bereits vollständig elektronisch erfolgen kann und Protokolle auch elektronisch gelesen werden können, wird diese Vorgangsweise ausdrücklich vorgesehen.

Zu den weitgehend mit der technischen Entwicklung begründeten Einwänden gegen eine detaillierte Speicherung ist auf die beim Hauptverband seit Jahren geübte Praxis zu verweisen, nach welcher eine Wiedergewinnung der Protokolldaten in den jeweiligen Einzelfällen problemlos innerhalb weniger Stunden möglich ist, also - wenn überhaupt - nur geringe technische Hindernisse mehr bestehen.

Festzuhalten ist auch hier, dass die exakte und über viele Jahre zurückreichende Aufzeichnung der Zugriffe beim Hauptverband zumindest seit Mitte der 80er-Jahre ständige Praxis ist. Sie hat den Hauptverband - und damit dessen verantwortliche Funktionäre und die gesamte Datenspeicherungspraxis der Sozialversicherung - bereits mehrfach vor massiven Vorwürfen bewahrt, weil detailliert dokumentierbar war, wer wann auf welche Datenbestände zugegriffen hatte (inbesondere bei Auskunftserteilungen an Verwaltungsbehörden und Gerichte). Solche Fälle mögen selten sein - die durch eine exakte Protokollierung erzielbare Glaubwürdigkeit in Datensicherheitsfragen ist jedoch ein Wert, der nicht gering geschätzt werden dürfte.

Im Auge zu behalten wären auch die Vorschriften über die Rechnungsführung und Rechnungslegung der Sozialversicherungsträger und des Hauptverbandes, welche schon jetzt in deren §§ 58 f. Aufbewahrungsfristen von drei Jahren bis 20 Jahre nach dem Tod des Betroffenen vorsehen, welche jedenfalls über die im DSG 2000 enthaltene Mindestdauer hinausgehen.

Die Protokollierungfristen der Datenschutzverordnung werden diese teilweise sehr langen Fristen deutlich verkürzen. Damit wird auch eine immer wieder gestellte Frage entschieden, ob Protokolldaten Teil jener Daten

wären, auf welche zugegriffen wurde (damit würde für Protokolldaten die Aufbewahrungsfrist jener Daten gelten): Dies soll nicht so sein.

Zu § 8 Abs. 2

Unterschiedliche Protokollierungsarten können dann sinnvoll sein, wenn die Übermittlungsempfänger für die auskunftsverpflichtende Stelle in unterschiedlicher Weise greifbar sind: Akten eines anderen Sozialversicherungsträgers (und damit die Übermittlung an diesen Träger) sind leicht nachvollziehbar, weil nach § 321 ASVG usw. jederzeit die entsprechenden Unterlagen zur Verfügung gestellt werden müssten. Übermittlungen aus dem Sozialversicherungsbereich hinaus an andere Stellen, die derselben Aufsichtsbehörde unterstehen, werden zwar eingehender, aber unter Hinweis auf die gemeinsame Zentralstelle (Ressort, Aufsichtsbehörde) ebenfalls noch in vereinfachter Weise protokolliert werden können, während die Übermittlungen an sozialversicherungsfremde Stellen (z. B. Gerichte) in exakter Weise mit Aktenzahl o. ä. zu protokolliert wären, um den jeweiligen Übermittlungsempfänger genau feststellen zu können.

Protokolldaten über Übermittlungen an sozialversicherungsfremde Stellen haben daher eigene Datenbestände zu sein, wobei die Tatsache, dass eine derartige Stelle Daten eines Betroffenen abgefragt hat, ein eigener Datensatz zu sein hat, der jederzeit wieder abrufbar sein muss. Dies beinhaltet auch den Fall, dass eine Anfrage einer sozialversicherungsfremden Stelle zwar Personendaten aufgerufen hat, aber die Auskunft inhaltlich „keine einschlägigen Daten vorhanden“ ergeben hat - auch dies ist ein Zugriff auf Daten des Betroffenen gewesen, der nachvollziehbar bleiben muss (wenn z. B. die Auskunft erteilt wird, für jemand sei kein Versicherungsverhältnis vorgemerkt).

Zu § 8 Abs. 2 Z 2 und Z 3

Ebenso erscheint es nicht zweckmäßig zu sein, (ohnedies gesetzlich vorgesehene) Bekanntgaben größerer Datenmengen auf Grund konkreter Anlässe in jedem Einzelfall zu protokollieren.

Registrierte Übermittlungen an Empfänger im Einflussbereich der gemeinsamen obersten Aufsichtsbehörde der Sozialversicherung müssen nicht protokolliert werden. Als Beispiele dazu seien Datenübermittlungen anlässlich von AK-Wahlen oder an Wirtschaftsforschungsinstitute etc. zur Ausarbeitung von Statistiken (§ 46 DSG 2000), an die Behörden der Finanzverwaltung im Leistungsbereich (Steuerpflicht von Leistungen der SV) und Melde- und Beitragsbereich, an das AMS, an gesetzliche berufliche Interessenvertretungen (z.B. an Ärztekammern in Zusammenhang mit der Abfuhr der Wohlfahrtsfondsbeiträge), an die Vertragspartner usw. genannt.

Die bisherige Vorgangsweise bei der Erstellung volkswirtschaftlich relevanter Studien durch Wirtschaftsforschungsinstitute, Akademien usw. ist auch dann hievon umfasst, wenn eine solche Studie nicht von einem Sozialversicherungsträger (Auftraggeber für die Datenverwendung), sondern vom Hauptverband bzw. dem Sozialministerium durchgeführt wird. Letztere Stellen haben auf Grund ihrer Unterstützungs- und Amtshilfeberechtigungen die Möglichkeit, die Daten von den Versicherungsträgern zu erhalten (also „zulässigerweise zu ermitteln“ iSd § 46 Abs. 1 Z 2 DSG 2000, vgl. § 321 ASVG, § 183 GSVG, § 171 BSVG, § 119 B-KUVG, § 87 NVG, § 449 Abs. 2 ASVG, usw.). Eine Befassung der Datenschutzkommission nach § 46 Abs. 3 DSG 2000 ist in diesen Regelfällen daher nicht notwendig.

Übermittlungen außerhalb des Einflussbereiches der Sozialversicherung (z. B. an Gerichte und Verwaltungsbehörden wie Jugendämter, Sozialhilfeträger, Finanzämter) müssen jedenfalls protokolliert werden, unabhängig davon, ob sie registriert sind oder nicht.

Eine Einschränkung auf neue Programme, Umstellung von Altprogrammen ist daher nicht notwendig.

Zu § 8 Abs. 3

Diese Bestimmung soll die technische Nachvollziehbarkeit, Auffindbarkeit des zu Grunde liegenden Aktes, des Datenverwendungsanlasses einschließlich der abfragenden Stelle absichern, aber keinen darüber hinaus gehenden zusätzlichen Auskunftsanspruch des Betroffenen (insbesondere nicht hinsichtlich besonderer Sortierung, Übersichtlichkeit, Aufnahme bestimmter Datenarten in die Protokollierung usw.) begründen. Insbesondere ist dadurch nicht verpflichtend vorgesehen, den Namen der abfragenden Person jedenfalls schon im Protokoll aufzuzeichnen, wenn dieser Name auf Grund anderer Unterlagen (z. B. Akteneinsicht in die zu der verzeichneten Aktenzahl vorhandenen Unterlagen, Auskunftspflichtgesetz, Protokollierung des Abfragegerätes, dessen Zugriffsberechtigungen und der exakten Abfragzeit) auffindbar ist. Auch Zutrittscodes müssen - wenn die soeben genannten Kriterien auf andere Weise erfüllbar sind - nicht jedenfalls in den Protokolldatensätzen aufscheinen. Passwörter dürfen schon aus Sicherheitsgründen in den Protokolldatensätzen nicht aufscheinen.

Zu § 11

Die bisher notwendige Anführung der Registernummer (§ 17 Abs. 1 DSV) ist nach § 25 DSG 2000 dahingehend eingeschränkt, dass im Wesentlichen diese Registernummer nur mehr bei Mitteilungen an Betroffene angeführt werden muss.

Die bisher bei der Verwendung von Registernummern im sozialversicherungsinternen Datenverkehr (zwischen Auftraggebern und Dienstleister) notwendigen Vorgangsweisen können damit ersatzlos entfallen. Dass bei entsprechenden Mitteilungen, wie Bescheiden, einfachen Schreiben etc., die DVR-Nummer des jeweiligen Versicherungsträgers/Hauptverbandes angeführt werden muss, bleibt jedoch aufrecht.

Das Datenverarbeitungsregister ist seit 1. Jänner 2000 von der Datenschutzkommission zu führen, daher sind die Meldungen an diese Behörde zu richten (Hohenstaufengasse 3, 1010 Wien, die früheren Adressen Bäckerstraße und Ballhausplatz sind wegen Übersiedlung des DVR nicht mehr brauchbar).

Zu § 12

Im Regelfall wird davon ausgegangen werden können, dass die Einsichtnahme (und der Verweis darauf) in öffentliche Register zumutbar ist, das darf aber im Einzelfall nicht zu einer Einschränkung der Informationspflicht führen: ein 15-jähriges Kind kann z. B. im Umgang mit Internetanfragen wesentlich mehr Erfahrung haben als ein 55-jähriger. Je nach Situation des Falles werden somit auch Inhalte aus solchen Registern bekannt gegeben werden müssen (insbesondere, solange das Datenverarbeitungsregister nicht im Internet allgemein abfragbar zur Verfügung steht).

Zu § 13 Abs. 1

Was eine „unbedenkliche Feststellung“ sein kann, wird von den örtlichen Gegebenheiten abhängen (eindeutige persönliche Bekanntheit/Feststellbarkeit des Betroffenen bei der auskunftspflichtigen Stelle - z. B. Versicherter als Patient - kann im Einzelfall bereits zur Feststellung der Identität ausreichen).

Ebenso könnte die allenfalls langjährige Bekanntheit der Zustelladresse einer Person eine Zustellung mit Rückschein oder Zustellungsbestätigung unnötig werden lassen.

Anfragen eines Betroffenen z. B. über Versicherungsdaten (Versicherungsdatenauszug, vgl. SozSi 1996, S. 488) oder in beitragsrechtlichen Angelegenheiten werden auch dann ausreichend sicher beantwortet werden können, wenn sich aus dem Inhalt des Anrufes im Vergleich mit den gespeicherten Versicherungsdaten (z. B. Übereinstimmung des Genannten mit dem gespeicherten Arbeitgeber) zunächst eine plausible Bescheinigung der Identität ergibt, welche durch qualifizierte Zustellung bestätigt werden kann.

Wenn aber weder Person noch Zustelladresse vor der Auskunftsanforderung bekannt sind, empfiehlt sich die Einhaltung der seit Jahren - auch in der datenschutzrechtlichen Literatur - akzeptierten Zustellung der Auskunft durch RSa-Brief (Rundschreiben des BKA vom 26. 11. 1987, Zl. 810.031/1-V/3/87, abgedruckt bei: Dohr-Pollirer-Weiss, DSG, Anm. 2 zu § 11 DSG). Nicht nachvollziehbare Auskünfte „auf anonymen Zuruf ohne weitere Formalitäten“ entsprechen keinesfalls den Sicherheitskriterien.

Es bestehen in diesem Sinn keine Einwände dagegen, auch Auskunftsanforderungen durch Notare, Rechtsanwälte, Wirtschaftstreuhänder, Beratungsinstitutionen (Kammern, Interessenvertretungen), welche sich auf die „erteilte Vollmacht“ berufen und die Adresse des Klienten nennen, durch direkte Übermittlung der Auskunft an diese Adresse zu erledigen (bei Fehlen weiterer Identitätsfeststellungsmöglichkeiten empfiehlt sich im Allgemeinen in solchen Fällen die RSa-Zustellung bzw. die Zustellung durch „Übernahmeschein eigenhändig“).

Zu § 13 Abs. 2 Z 3

Die vorgeschlagenen Formulierungen haben bei der Einführung einer Altersgrenze jene Fälle im Auge, in denen mündige Minderjährige auf Grund eigener Beschäftigung versichert sind (Lehrlinge etc.) und damit auch eigene Krankenscheine erhalten. Weiters sollen jene Fälle erfasst werden, in denen eine z. B. 17-jährige eine z. B. psychotherapeutische, gynäkologische oder dermatologische Behandlung benötigt, über die sie aus Gründen, welche die Versicherung nicht zu interessieren haben, mit ihren Eltern (aus welchen Gründen immer) nicht sprechen möchte.

Die hier erwähnte „Bescheinigung“ wird von der anfordernden Stelle zu erbringen sein, wobei die konkrete Ausformung davon abhängen wird, über welche Daten Auskunft gegeben werden soll: Die bloße Frage „Ist mein Kind X schon als mein Angehöriger gespeichert?“ wird keiner weiteren Bescheinigung bedürfen, wohl aber die Frage „Wegen welcher Diagnose war meine Tochter beim Gynäkologen?“

Es soll zwar der Betroffene die Möglichkeit haben, eigene Daten im Weg des Auskunftsrechts zu erhalten, es soll aber nicht möglich sein, dass gerade jene Erziehungsberechtigten, mit denen das Kind darüber nicht gesprochen hat/sprechen möchte, diese Daten im Wege der Auskunftsverpflichtung kraft Elternrechts (und somit gegen den Willen des/der Betroffenen) ohne weiteres erhalten können (der Weg über das Jugendamt bzw. Pflegschaftsgericht bleibt solchen Erziehungsberechtigten nach wie vor offen). Er erscheint angesichts der in solchen Fällen gegebenen Misstrauenssituation und der Schwere des Grundrechtseingriffes angemessen.

In diesem Zusammenhang ist auch an die Fälle von Kindesmissbrauch etc. zu denken, in denen ebenfalls zu vermeiden ist, dass unbefugten Familienangehörigen auf einfache Weise Daten zugänglich werden.

Die 14-Jahresgrenze ist § 361 Abs. 2 ASVG entnommen. Wegen des Gleichklangs mit dieser Bestimmung wurde nicht nur der Begriff „mündiger Minderjähriger“ (vgl. § 21 Abs. 2 ABGB) verwendet, welcher dem Nichtjuristen keine klare Altersgrenze nennt. Die Altersgrenze beruht auf einer Abwägung, welche sich an die Mündigkeitsgrenzen des bürgerlichen Rechts sowie des Außerstreitgesetzes und somit an allgemein anerkannte Altersunterschiede anlehnt. Diese 14-Jahres-Grenze wurde nunmehr auch für die „familiengerichtliche Verfahrensfähigkeit Minderjähriger“ in § 182a AußStrG festgelegt (vgl. BGBl. I Nr. 135/2000).

Es war dabei bewusst, dass die Sozialversicherungsgesetze ab dem Jahr 2003 eine Information über die erbrachten Leistungen (auch für Angehörige) an den Versicherten vorsehen (siehe § 81 Abs. 3 ASVG, § 43

GSVG, § 41 BSVG, § 27 B-KUVG, jeweils letzter Satz idF. BGBl. I Nr. 92/2000). Diese ausdrückliche gesetzliche Sondernorm wird angesichts des Grundrechts auf Datenschutz restriktiv auszulegen sein und wird - zumindest bis zu gegenteiligen Entscheidungen - nicht zur Interpretation des Auskunftsrechts nach § 26 DSG 2000 herangezogen werden können.

Zu § 13 Abs. 5

Ursprünglich war folgender Standpunkt vorgesehen: Das bloße Interesse an der Kenntnis des Sachbearbeiternamens wird noch kein „überwiegendes Interesse“ sein, wenn dieses Faktum auf Grund der in einem Verfahren zustehenden Akteneinsicht geklärt werden kann und die hiefür notwendigen Daten (Aktenzahlen, Behörde) im Rahmen der Auskunftsbearbeitung bekannt gegeben werden. Der Name des Sachbearbeiters ist aber nicht jedenfalls von vornherein geheimhaltungswürdig, weil ansonsten die Geltendmachung von Befangenheitsgründen (§ 7 AVG usw.) verhindert werden könnte.

Der Datenschutzrat hielt dazu fest: „Nicht der Auskunftswerber, sondern der Auftraggeber hätte allenfalls ein überwiegendes Interesse des Auftraggebers oder eines Dritten geltend zu machen, wenn er bestimmte Auskünfte, wie etwa den Namen des Sachbearbeiters, nicht erteilt.“

Zu § 13 Abs. 6

Es wird nur bestimmt, dass ein Geheimhaltungsinteresse des Behandlers für sich allein kein Grund sein kann, einem Patienten z. B. Auskunft darüber zu verweigern, welche Leistungen für ihn mit der Versicherung verrechnet und welche Diagnosen über ihn gespeichert wurden. Ob eine Auskunft aus anderen Gründen verweigert werden darf, ist nach den jeweils einschlägigen Regeln zu entscheiden. Zum letzten Satz wird auf die Regeln über die Einsichtnahme in Krankengeschichten verwiesen (therapeutische Vorbehalte bei der Information des Patienten usw.). Vom Grundsatz, dass über Behandlungsdaten in erster Linie der Behandler Auskunft zu geben hätte, wird dadurch nicht abgewichen. Dies kann aber nicht bedeuten, dass solche Daten, die bei einem Versicherungsträger verwendet würden, keiner Auskunftspflicht unterlägen (schon wegen möglicher Interessenkonflikte zwischen Patient und Arzt werden solche Auskünfte möglich sein müssen).

Hiezu wurde im Begutachtungsverfahren vorgeschlagen, dass Auskünfte über Behandlungsdaten primär vom Behandler erlangt werden sollten und für Auskünfte der Versicherung ein Grund angegeben werden sollte. Dies konnte jedoch nicht in den Verordnungstext aufgenommen werden, weil das DSG 2000 das Auskunftsrecht nicht an eine Begründung koppelt (vgl. § 1 Abs. 3 DSG 2000). Es trifft jedoch zu, dass Patienten Auskünfte über Behandlungsdaten in erster Linie vom Behandler erhalten sollten, weil in der Regel nur dieser auf Grund seiner Kenntnis des Behandlungsablaufes bzw. -Planes in der Lage sein wird, auch entsprechende Erläuterungen abzugeben.

Zu § 13 Abs. 7

In jenen Fällen, in denen mehrere Personen gleiche oder sehr ähnliche Namen tragen (insbesondere dann, wenn die Geburtsdaten gleich sind), ist es notwendig, über die allgemeinen Hinweise auf die Datenverarbeitung nähere Daten vom Betroffenen zu erhalten, um ausschließen zu können, dass ihm nicht Daten Unbeteiligter bekannt gegeben werden (und damit deren Datenschutzrechte verletzt werden). Dies gilt auch für jene Fälle (Z 4) in denen jemand seinen Namen gewechselt hat, aber Angaben über ihn noch unter dem früheren Namen verzeichnet sind (Namenswechsel müssen der Sozialversicherung nicht von vornherein gemeldet werden).

In diesem Zusammenhang war auch auf die gegliederte Organisationsform der Datenverwendung einzugehen: Bei Sozialversicherungsträgern sind wie bei allen größeren Unternehmen mittlerweile an tausenden Arbeitsplätzen PCs installiert, welche meist einerseits Zugriff auf (betriebsinterne) Netzwerke haben, andererseits aber auch jeder für sich eine eigene Festplatte besitzen. Wollte man kein einschlägiges Mitwirkungsrecht des Betroffenen vorsehen, könnte ein allgemeines Auskunftsersuchen zur Folge haben, dass österreichweit alle Festplatten aller PCs eines Betriebes (samt Laptops oder Handy-Adressverzeichnisse) zu durchsuchen wären. Dies entspricht nicht der Zumutbarkeitsregel des § 26 Abs. 3 DSG 2000.

Was im Sinn dieser Bestimmung „ungerechtfertigter und unverhältnismäßiger Aufwand beim Auftraggeber“ sein werden, kann nur im Einzelfall entschieden werden. Im Sinn des DSG wird hier zwar kundenfreundlich vorzugehen sein, was aber nicht bis zur Blockierung der Arbeitsabläufe der auskunftsverpflichteten Stelle gehen kann. „Zusammenhang“ in diesem Sinn werden z. B. „Beitragsverrrechung 1998“, „Leistungsabrechnung mit Dr. XY im ersten Quartal 2001“, „Insolvenzverfahren des Gerichts xy zur Zahl ...“ sein.

Zu § 14

Diese Kostentragungsregel hat nichts mit der Finanzierung der Amtshilfeverpflichtungen der Sozialversicherung z. B. auf Grund des Art VII der ZVR-Novelle 1986, BGBl. Nr. 71/1986, zu tun. Dies wird auf Grund der Anmerkungen des Justizministeriums im Begutachtungsverfahren ausdrücklich klargestellt.

Zu § 17

Die Festlegung der Verfahrensregeln (im Zweifel mangels anderer Festlegung hat das grundrechtlich abgesicherte Auskunftsrecht nach dem DSG Vorrang) ist notwendig, weil die Auskunftsrechte nach dem DSG und dem Auskunftspflichtgesetz unterschiedliche Verfahrenswege eröffnen und von Anfang an klar sein muss, in welchem Verfahren ein Antrag abzuwickeln ist (das Auskunftsrecht kennt z. B. Bescheidpflichten der auskunftsverpflichteten Stelle nach § 4 AuskPflG, das DSG nicht). Die achtwöchige Frist des § 26 Abs. 4 DSG

2000 und des § 3 Auskunftspflichtgesetz können zu unterschiedlichen Zeitpunkten zu laufen beginnen, weil das AuskPflG keine Mitwirkungspflichten und keinen Kostenersatz des Betroffenen kennt.

Auch ein allfälliger „Beschwerde-/Instanzenzug“ (DSK und danach VfGH zuständig oder Bescheidbeschwerdemöglichkeit an VwGH gegen einen Bescheid nach § 4 AuskPflG?) muss wegen des verfassungsgesetzlich gewährleisteten Rechts auf den gesetzlichen Richter nach Art. 83 Abs. 2 B-VG und Art. 6 MRK klar sein.

Zu § 18 Abs. 1

Logische Löschung oder Richtigstellung erfolgt durch eine Änderung/Ergänzung der zu korrigierenden Datenbestände insoweit, dass zusätzliche Anmerkungen (Bestreitungsvermerke usw.) vorgenommen oder Zugriffsrechte so verändert werden, dass auf die - vorhanden bleibenden - Daten nicht mehr zugegriffen werden kann. Physische Löschung ist das nicht rekonstruierbare Vernichten (Überschreiben) von Daten.

Zu § 18 Abs. 5

Abs. 5 geht auf jene Fälle ein, in denen ausländische Arbeitnehmer bei Arbeitsantritt unbedenkliche Urkunden über ein bestimmtes Geburtsdatum vorlegten, aber Jahr(zehnte) später in ihrem Heimatland dieses Geburtsdatum zurückverlegen ließen (in manchen Ländern ohne ausgefeiltes Personenstandswesen war dies zumindest in der Vergangenheit relativ einfach) und damit rascher ein pensionsrechtlich relevantes Anfallsalter erreichten. Das Datenschutzrecht soll nicht dazu zwingen, dieses neue Geburtsdatum ohne Weiteres annehmen zu müssen (vgl. SozSi 1996, S. 506, FN 191; SozSi 1999, S. 426).

Zu § 18 Abs. 6

Bei Mitteilungen etc., die ein Sozialversicherungsträger oder der Hauptverband nach dem DSG zu erlassen hätte, kann es sich nicht um Bescheide im Sinn des Verwaltungsverfahrens der Sozialversicherung handeln, weil für die Bescheide der Sozialversicherung andere Verfahrenswege vorgesehen sind (Landeshauptmann, Bundesminister, Verwaltungsgerichtshof), aber das Recht auf Datenschutz nicht von diesen Behörden, sondern von den nach dem DSG eingerichteten Kontrollorganen, insbesondere der Datenschutzkommission, zu beurteilen ist (vgl. § 35 Abs. 1 DSG 2000).

Dies soll durch eine explizite Erwähnung in der Datenschutzverordnung ausdrücklich festgehalten werden. Dagegen ergaben sich im Begutachtungsverfahren keine Einwände des für das Verwaltungsverfahrensrecht zuständigen Bundeskanzleramtes.