REPUBLIK ÖSTERREICH DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN
GZ ● BKA-817.434/0003-DSR/2012
TELEFON ● (+43 1) 53115/2527
FAX ● (+43 1) 53115/2702
E-MAIL ● DSRPOST@BKA.GV.AT
DVR: 0000019

An den
Hauptverband der
Österreichischen
Sozialversicherungsträger

Mit E-Mail:

Ref.12-stellungnahmen@
hvb.sozvers.at

posteingang.allgemein@hvb.soz
vers.at

recht.allgemein@hvb.sozvers.at

Betrifft: Entwurf einer Datenschutzverordnung des Hauptverbandes der österreichischen Sozialversicherungsträger für die gesetzliche Sozialversicherung
(SV-Datenschutzverordnung 2012 – SV-DSV 2012)

Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner 212. Sitzung am 12. März 2012 **einstimmig beschlossen**, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

I. Allgemeines:

Die derzeit gültige Datenschutzverordnung des Hauptverbandes (SV-DSV 2001), AVSV Nr. 1/2002, wurde am 18. Dezember 2001 beschlossen.

Seither hat sich Bedarf nach einigen Änderungen ergeben, weiters sind aufgrund praktischer Erfahrungen, Namensänderungen, Zitatanpassungen und der DSG-Nov 2010 einige inhaltliche Anpassungen notwendig. Da das Datenverarbeitungs-

register auf elektronische Eingabe- und Abfragemöglichkeiten umgestellt werden soll, ist auch darauf einzugehen. Daneben sind die Entwicklungen im Bereich E-Government zu berücksichtigen.

Der Hauptverband ist als Betreiber des Informationsverbundsystems der österreichischen Sozialversicherung nach § 50 Abs. 1 DSG 2000 für die notwendigen Maßnahmen der Datensicherheit (§ 14 DSG 2000) im Informationsverbundsystem verantwortlich. Die Regeln der vorliegenden Verordnung sind Teil dieser Datensicherheitsmaßnahmen.

II. Rechtliche Anmerkungen:

1.) Anmerkungen zum Entwurf des Gesamttextes einer SV-DSV 2012:

a.) Vorweg wird festgehalten, dass offenbar angedacht ist, die SV-Datenschutzverordnung 2001 (SV-DSV 2001), AVSV Nr. 1/2002, im Rahmen einer SV-Datenschutzverordnung 2012 (SV-DSV 2012) allenfalls auch **als Ganzes neu zu erlassen**. Aus diesem Grund wird zu dem vorgelegten **Gesamttext** einer SV-DSV 2012 sowie zu den geplanten Änderungen zur SV-DSV 2001 Stellung genommen.

b.) In Anbetracht des allfälligen Vorhabens einer **Neuerlassung**, wird im Hinblick auf den Umfang der **Kompetenz** zur Erlassung einer **Durchführungsverordnung** durch den Hauptverband darauf hingewiesen, dass mit der Verordnung **Freiräume**, die das Gesetz erkennbar offen lässt, für den Bereich der Sozialversicherung durch sachspezifische Regelungen ausgefüllt werden können, um die Einheitlichkeit und Treffsicherheit der Vollziehung im Sozialversicherungsbereich zu erhöhen.

Das Vorliegen dieser Voraussetzung, nämlich die Ausfüllung von Freiräumen, scheint jedoch bei einem Teil der Regelungen der vorliegenden Verordnung nicht zweifelsfrei gegeben. Wenn etwa Begriffe des DSG 2000 in genereller, aus dem sozialversicherungsrechtlichen Kontext nicht sichtbar erforderlichen Weise interpretiert werden, und zwar überdies in einer möglicherweise abändernden Weise, so kommt dies der Inanspruchnahme einer **Gesetzgebungskompetenz** gleich.

Insofern würde der Hauptverband dann seine Kompetenz zur Erlassung einer Durchführungsverordnung wohl überschreiten.

Es wird daher allgemein empfohlen, den vorliegenden Verordnungsentwurf nochmals – auch im Hinblick auf die Anmerkungen in der einschlägigen Literatur zur SV-

DSV 2001 (vgl. *Lehner*, Datenschutz durch die Gebietskrankenkassen [2007]) – dahingehend zu prüfen, welche Regelungen im Rahmen des Ausfüllens von „**Freiräumen**“ der datenschutzrechtlichen Vorgaben erfolgen und welche allenfalls darüber hinausgehen, und insbesondere **jene Regelungen zu überarbeiten bzw. erforderlichenfalls zu streichen, in welchen in genereller, aus dem sozialversicherungsrechtlichen Kontext nicht sichtbar erforderlichen Weise Definitionen des DSG 2000 – allenfalls sogar in abändernder Weise – interpretiert werden.**

In diesem Sinne wird im Hinblick auf eine allfällige Erlassung des vorgelegten **Gesamttextes als SV-DSV 2012** insbesondere auf nachfolgende Punkte hingewiesen.

c.) Im Hinblick auf die Regelung des § 6 Abs. 3 SV-DSV 2012, wonach die „Medizinische Diagnostik“ im Sinne des § 9 Z 12 DSG 2000 auch **Untersuchungen für Zwecke der Rehabilitation** oder der **Erbringung anderer Leistungen** durch Sozialversicherungsträger einschließlich des Verfahrens in Sozialrechtssachen vor den Arbeits- und Sozialgerichten umfasst, wird darauf hingewiesen, dass in den Fällen des § 9 Z 12 DSG 2000 die Verwendung sensibler Daten jeweils durch **ärztliches Personal** oder sonstige Personen erfolgen muss, die einer entsprechenden Geheimhaltungspflicht unterliegen. Dieser entscheidende Aspekt sollte auch im Hinblick auf eine Präzisierung der „Medizinischen Diagnostik“ berücksichtigt werden, sodass **nicht von vornherein jede Untersuchung und jede weitere Verwendung (etwa in der Folge auch durch nicht-ärztliches Personal) als eine Verarbeitung von Daten zum Zweck der „Medizinischen Diagnostik“ im Sinne des § 9 Z 12 DSG 2000 gewertet werden kann.** Darüber hinaus wird darauf hingewiesen, dass dieser Begriff nur im Rahmen der Vorgaben des Art. 8 Abs. 3 der Datenschutz-Richtlinie 95/46/EG interpretiert werden darf.

Der Datenschutzrat vertritt die Auffassung, dass jeder Bedienstete und Auftragnehmer an die Geheimhaltungsbestimmungen gebunden ist und keine Daten intern oder extern entgegen den Bestimmungen des DSG 2000 weitergegeben werden dürfen. In Bezug auf § 9 des Verordnungsentwurfes vertritt der Datenschutzrat die Ansicht, dass jeder Bedienstete gemäß § 15 DSG 2000 zur Einhaltung des Datengeheimnisses ausdrücklich zu verpflichten ist. Dritte Personen als Dienstleister sind mit entsprechenden Vereinbarungen

gemäß den §§ 10 und 11 DSG 2000 zur Einhaltung der datenschutzrechtlichen Vorgaben zu verpflichten.

d.) Im Sinne des **Verhältnismäßigkeitsgrundsatzes** und des **Grundsatzes der Datensparsamkeit** sollten personenbezogene Daten – wenn sie nicht mehr benötigt werden – grundsätzlich **nicht nur bloß logisch gelöscht** werden, da derart gelöschte Daten unter Umständen auch wieder hergestellt werden können. Dies gilt umso mehr, wenn es sich dabei um sensible Daten handelt. In Anbetracht der seit dem Jahr 2001 wohl gestiegenen Gefahr des Datenmissbrauchs und der nach heutigem Stand vergleichbar einfachen technischen Möglichkeiten, logisch gelöschte Daten wiederherstellen zu können, wird angeraten, in § 18 SV-DSV 2012 („Richtigstellung und Löschung“) **in jedem Fall, in welchem eine Löschung (etwa auch im Zuge einer Richtigstellung) vorgenommen werden muss, eine physische Löschung der Daten verpflichtend vorzusehen**, außer die Löschung oder Richtigstellung von Daten kann auf ausschließlich automationsunterstützt lesbaren Datenträgern aus Gründen der Wirtschaftlichkeit **nur zu bestimmten Zeitpunkten** vorgenommen werden. Nur in diesem Fall sind nach § 27 Abs. 6 DSG 2000 die zu löschenden Daten **bis dahin** für den Zugriff zu sperren und die zu berichtigenden Daten mit einer berichtigenden Anmerkung zu versehen.

Zudem sollte auch in § 7 Abs. 5 Z 8 SV-DSV 2012 eine **physische Löschung** der Datenträger **vor einer Veräußerung oder Entsorgung** in jedem Fall ausdrücklich vorausgesetzt werden.

Im Hinblick auf die Richtigstellung und Löschung ist zu § 18 Abs. 5 SV-DSV 2012 auch anzumerken, dass § 27 Abs. 3 DSG 2000 eine Richtigstellung nicht schon dann ausschließt, wenn Daten bei ihrer Ermittlung richtig waren oder ihre Richtigkeit anzunehmen war, sondern nur soweit der **Dokumentationszweck** einer Datenanwendung nachträgliche Änderungen nicht zulässt.

e.) § 8 Abs. 2 SV-DSV 2012 sieht **Ausnahmen von der Protokollierungspflicht** vor. Diesbezüglich wird angemerkt, dass § 14 Abs. 2 Z 7 DSG 2000 vorsieht, dass – soweit dies im Hinblick auf § 14 Abs. 1 DSG 2000 letzter Satz erforderlich ist – Protokoll zu führen ist, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können. Der letzte Satz des § 14 Abs. 1 DSG 2000 stellt dabei auf die Art der verwendeten Daten, den Umfang und

Zweck der Verwendung, den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit ab. **Aufgrund dieser Vorgaben ist eine Abwägung im Einzelfall bei jeder Datenanwendung erforderlich.**

In Anbetracht dessen sollte daher überprüft werden, ob die in § 8 Abs. 2 SV-DSV 2012 angeführten, **generellen Ausnahmen** tatsächlich den Vorgaben des § 14 DSG 2000 entsprechen.

f.) Die in § 11 Abs. 1 SV-DSV 2012 festgelegte Meldeverpflichtung nimmt zwar auf Ausnahmen aufgrund von § 17 DSG 2000 Bezug. Nicht angeführt werden jedoch Ausnahmen von der Meldepflicht, die sich aufgrund von § 50c Abs. 2 DSG 2000 im Hinblick auf die dort genannte **Videoüberwachung** in Fällen der Echtzeitüberwachung oder wenn eine Speicherung (Aufzeichnung) nur auf einem analogen Speichermedium erfolgt, ergeben können.

Im Übrigen wiederholt auch § 11 Abs. 4 SV-DSV 2012 – zusätzlich zu Abs. 1 – die Verpflichtung zur Meldung. Nachdem der **doppelte Verweis auf Meldepflichten** in § 11 SV-DSV 2012 nicht erforderlich erscheint, könnte mit einer einmaligen Verweisung auf die Meldepflichten aufgrund des DSG 2000 und der Datenverarbeitungsregister-Verordnung das Auslangen gefunden werden.

g.) Zur **Informationspflicht des Auftraggebers** verweist § 12 SV-DSV 2012 auf § 24 DSG 2000. Nach § 24 Abs. 3 Z 3 DSG 2000 darf die Information etwa dann entfallen, wenn sie angesichts der Unwahrscheinlichkeit einer Beeinträchtigung der Betroffenenrechte einerseits und der Kosten der Information aller Betroffenen andererseits einen **unverhältnismäßigen Aufwand** erfordert, dies jedoch nur dann, wenn Daten nicht durch Befragung des Betroffenen, sondern durch Übermittlung von Daten aus anderen Aufgabengebieten desselben Auftraggebers oder aus Anwendungen anderer Auftraggeber ermittelt werden. Die Regelung des § 12 SV-DSV 2012, dass die Informationspflicht „ohne zumutbare und unnötige Belastung des Auftraggebers“ auszuüben ist, **entspricht in dieser Allgemeinheit nicht den Vorgaben des § 24 DSG 2000**. Zur Vermeidung der Festlegungen von abweichenden Regelungen zum DSG 2000 sollte daher einfach auf den § 24 DSG 2000 verwiesen werden.

h.) Die **Auskunft** nach § 26 DSG 2000 ist gemäß § 26 Abs. 6 DSG 2000 **unentgeltlich** zu erteilen, wenn sie den **aktuellen Datenbestand** einer Datenanwendung betrifft und der Auskunftswerber **im laufenden Jahr noch kein Auskunftsersuchen**

an den Auftraggeber zum selben Aufgabengebiet gestellt hat. Hingegen sieht § 14 SV-DSV 2012 vor, dass die Auskunft dann unentgeltlich zu erteilen ist, wenn sie den aktuellen **und** direkt abfragbaren Datenbestand betrifft. Hinsichtlich der Voraussetzung des Vorliegens eines **direkt abfragbaren** Datenbestandes sollte überprüft werden, ob damit nicht allenfalls eine Einschränkung der Vorgaben des § 26 Abs. 6 DSG 2000 im Hinblick auf die Unentgeltlichkeit der Auskunft vorgenommen wird. Gleiches gilt für § 14 Abs. 4 SV-DSV 2012 im Hinblick auf die Auslegung des Begriffes der „**aktuellen Daten**“, welche nach dieser Bestimmung (offenbar nur) solche Daten umfassen sollen, auf welche „**direkt zugegriffen**“ werden kann, wobei insbesondere überprüft werden sollte, ob mangels eines unter Direktzugriff stehenden Datenbestandes auch der **letztgültige Datenbestand** unentgeltlich zu beauskunften ist (siehe dazu *Dohr/Pollirer/Weiss/Knyrim*, DSG^2 [9. Erg.-Lfg. 2009] § 26 Anm. 30).

Im Übrigen wird hinsichtlich der Auskunft auf die Vorgaben für den Betreiber eines Informationsverbundsystems gemäß § 50 Abs. 1 DSG 2000 sowie überdies im Falle einer Auftragserfüllung für einen Dritten auch auf § 26 Abs. 10 DSG 2000 hingewiesen.

2.) Zu den Änderungen der SV-DSV 2001

Vorbemerkungen:

In der Promulgationsklausel von Verordnungen, Kundmachungen und Entschließungen sind die bundesgesetzlichen Bestimmungen, auf die sie sich gründen, im Einzelnen anzugeben. In der Verordnung sollte daher angeführt werden, **auf welche bundesgesetzlichen Bestimmungen** sich die SV-DSV 2012 gründet.

Zu § 6 Abs. 2:

Der Hinweis auf § 32b ASVG sollte entfallen, weil eine Aufhebung dieser Bestimmung durch das 2. Stabilitätsgesetz 2012 beabsichtigt ist.

Zu § 6 Abs. 4:

Nach § 6 Abs. 4 werden **sensible Daten** auch im Rahmen eines Versuches der **außergerichtlichen Streitbeilegung** verwendet.

Schutzwürdige Geheimhaltungsinteressen werden bei der Verwendung sensibler Daten jedoch ausschließlich dann nicht verletzt, wenn eine der in § 9 Z 1 bis 13

DSG 2000 aufgezählten Voraussetzungen erfüllt sind. Nachdem **außergerichtliche Streitbeilegungen** in § 9 Z 1 bis 13 DSG 2000 nicht explizit angeführt sind, sollte dargelegt werden, auf welche der Vorrausetzungen des § 9 DSG 2000 diese Datenverwendung gestützt werden soll.

Zu § 7 Abs. 5:

§ 7 Abs. 5 Z 11 schließt für **Datenübermittlungen** diverse mobile Datenträger aus, die **undokumentierte nachträgliche Veränderungen** oder ein **nicht nachvollziehbares Löschen von Daten** ermöglichen. Die Erläuterungen verstehen darunter auch die Verwendung einer CD-ROM. Diesbezüglich wird darauf hingewiesen, dass auf einer CD-ROM (ebenso wie auf einer DVD) – mit Ausnahme von wiederbeschreibbaren Medien – eine nachträgliche Veränderung oder ein nicht nachvollziehbares Löschen auf dem Medium in der Regel **nicht** möglich ist und damit die Verwendung von CD-ROM sowie DVD aufgrund des Verordnungstextes eben **nicht** ausgeschlossen wäre. Dies insbesondere auch deswegen, weil aus dem Verordnungstext – im Gegensatz zu den Erläuterungen – nicht deutlich erkennbar ist, dass auch solche Datenträger ausgeschlossen sein sollen, die **auf vergleichsweise einfache Weise durch ein anderes Stück ersetzt werden** können.

In Anbetracht dessen, dass auch sensible Daten verwendet werden können und § 14 DSG 2000 hinsichtlich der Datensicherheitsmaßnahmen insbesondere auf die Art der verwendeten Daten und den Umfang und Zweck der Verwendung abstellt, wird auch darauf hingewiesen, dass Datenübermittlungen auf CD-ROM oder DVD im Lichte aktueller Entwicklungen im Bereich der Datensicherheit nicht ausreichend sicher sind und bei Verlust oder Diebstahl derartiger Datenträger eine vergleichsweise große Datenmenge betroffen sein kann. Von einer allfälligen Datenübermittlung mit mobilen Datenträgern sollte daher Abstand genommen werden. Soweit mobile Datenträger derzeit noch vorhanden sind, sollte zumindest vorgegeben werden, in welcher Form diese aufbewahrt und wie diese vor physischem Zugriff durch unberechtigte Personen geschützt werden sollen.

Allgemein wird auch angemerkt, dass sensible Daten vor einer Übermittlungen nach dem Stand der Technik verschlüsselt werden müssten und überdies protokolliert werden müsste, an wen die Daten jeweils weitergegeben bzw. von wem die Daten allenfalls geändert wurden.

§ 7 Abs. 5 Z 13 sollte im Übrigen sprachlich und grammatikalisch überprüft werden.

13. März 2012
Für den Datenschutzrat:
Der Vorsitzende:
MAIER

Elektronisch gefertigt