

**HAUPTVERBAND DER ÖSTERREICHISCHEN SOZIALVERSICHERUNGSTRÄGER**

A-1031 WIEN

KUNDMANNGASSE 21

POSTFACH 600

DVR 0024279

VORWAHL Inland: 01, Ausland: +43-1

TEL. 711 32 / KI. 1211

TELEFAX 711 32 3775

Zl. 12-REP-43.00/08 Ht/Er

Wien, 20. Mai 2008

An das  
**Bundeskanzleramt**  
Ballhausplatz 2  
1014 Wien

**Per E-Mail**

An das  
**Präsidium des Nationalrates**

**Per E-Mail**

An das  
Bundesministerium  
**für Gesundheit, Familie und Jugend**

**Per E-Mail**

Betr.: Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2008)

Bezug: Ihr E-Mail vom 11. April 2008;  
GZ: BKA-810.026/0002-V/3/2008

Sehr geehrte Damen und Herren!

Der Hauptverband der österreichischen Sozialversicherungsträger nimmt wie folgt Stellung:

**Zu den §§ 1 und 4 Abs. 1 Z 3**

Das Grundrecht auf Datenschutz – mit all den damit verbundenen Rechten wie Auskunftsrecht und dergleichen – soll künftig nur noch natürlichen Personen (bisher auch juristischen Personen) zukommen. Der vorgeschlagene Wortlaut ist unseres Erachtens dahin zu interpretieren, dass natürliche Personen auch dann geschützt bleiben, wenn sie unternehmerisch tätig sind (vgl. die Situation „neuer Selbstständiger“). Das Thema sollte zur Klarstellung in den Erläuterungen behandelt werden.

Die Einschränkung der Auskunftsberechtigung auf natürliche Personen hat weiters die Auswirkung, dass eine Korrekturmöglichkeit gestrichen wird, welche auch für Unternehmen relevant ist: Wenn über ein Unternehmen Falschmeldungen verbreitet werden, gab es bisher die Möglichkeit eines Auskunftsbegehrens nach dem DSGVO. Diese Möglichkeiten wurden im Vorfeld der Datenschutzkommission wahrgenommen, sodass die Verfahrenszahl dieser Behörde keine Aussage über die tatsächlichen Verhältnisse ermöglicht.

### **Zu § 15a - Datenschutzbeauftragte**

Der zusätzliche Auftrag des Gesetzes zur Bestellung eines Datenschutzbeauftragten könnte in der Praxis zu einer Entlastung des jeweils verantwortlichen Auftraggebers führen, weil dieser sich darauf verlassen könnte, dass der Datenschutzbeauftragte ja die Pflicht habe, Unstimmigkeiten aufzuzeigen (Abs. 3 – Überwachung!). Dass Abs. 6 die Verantwortung des Auftraggebers nicht ändert, könnte vielleicht nur rechtlich-theoretisch relevant bleiben (keine Verschuldensteilung im Schadenersatzrecht etc.).

Diese Situation könnte in größeren Betriebsorganisationen in der Praxis für den Datenschutz nachteilig werden, da nicht alle Mitarbeiter auf Einhaltung der datenschutzrechtlichen Vorschriften kontrolliert werden können und es einer Einzelperson schon kapazitätsmäßig unmöglich ist, alle Datenanwendungen eines größeren Betriebes auch nur ansatzweise zu beobachten, geschweige denn mit den zeitlichen Rahmenbedingungen, die das Gesetz aufstellt.

Da die Datenschutzbeauftragten auch zu personenbezogenen Daten Zutritt haben werden, um ihre Funktion sinnvoll ausüben zu können, werden sie in gravierende Interessenkonflikte kommen können. Die Kündigungsschutzbestimmung dürfte nicht ausreichend sein, sondern bedarf es eines erhöhten Kündigungs- und Entlassungsschutzes wie er für Betriebsratsmitglieder vorgesehen ist (§ 120 ff. ArbVG).

Die Bestimmung ist nicht auf die Wahrung der Dienstnehmerinteressen eingeschränkt, sondern würde für alle Datenverwendungen eines Betriebes gelten. Die Erläuterungen dazu erwecken einen anderen Eindruck. Wir bitten, dieses Thema nochmals zu überarbeiten. Die Beachtung des Datenschutzes sollte weiterhin allein im Verantwortungsbereich des Auftraggebers liegen, der seine eigenen Datenverarbei-

tungen zu überwachen hat und geeignete Maßnahmen umzusetzen hat, und nicht bei einer einzelnen Person konzentriert werden können.

### **Zu den §§ 17 und 20 bis 22**

Die verpflichtende Anwendung des Bürgerkartenkonzepts statt fehleranfälliger und zeitaufwändiger Code- und Passwortverwaltungen wird ausdrücklich begrüßt.

Es wäre unangemessen, wollte man allen Stellen, die in Österreich Daten verwalten, eine zusätzliche Code- und Passwortedokumentation nur für die (selten notwendige) Registrierung auferlegen oder gar die bisherigen umfangreichen Papierformulare weiter vorschreiben.

Wo keine Passwörter mehr benötigt werden, entfallen auch die damit verbundenen Missbrauchsquellen, Zugriffe und Änderungen werden besser nachvollziehbar. Für die Eintragung von Stellen, die nicht ohnedies in öffentliche Register eingetragen sind, stehen die Möglichkeiten des E-Government (Ergänzungsregister) zur Verfügung.

Der Entwurf sieht hinsichtlich der *nicht* vorabkontrollpflichtigen Datenanwendungen die Meldung in elektronischer Form vor, wobei eine automationsunterstützte Vollständigkeits- und Plausibilitätsprüfung erfolgen soll. Nur wenn bei dieser Prüfung eine Fehlermeldung auftritt, kommt es zu einer vollständigen Prüfung der Meldung. Bei Fehlerfreiheit soll die Meldung sofort registriert werden, womit auch die entsprechende Datenverarbeitung sofort aufgenommen werden kann und die bisherigen Zeitverzögerungen entfallen. Diese Situation wird angesichts der bisher üblichen Zeitverzögerungen bei normalen (nicht-sensiblen) Meldungen ebenfalls ausdrücklich begrüßt.

Zu § 18 sei festgehalten, dass die Vorabkontrolle nicht dazu führen darf, dass die Vollziehung von Rechtsvorschriften behindert wird: Da Novellen im Sozialversicherungsrecht manchmal nur Legisvakancen von wenigen Tagen aufweisen, werden auch in Zukunft entsprechende Kapazitäten der Datenschutzkommission zur Vorabkontrolle verfügbar zu halten sein.

Hinzu kommt, dass sowohl im Falle einer Verbesserung gemäß § 20 Abs. 2 als auch Abs. 4 DSGVO neu keine Fristen, innerhalb derer die Prüfung und Registrierung von Datenanwendungen durch das Datenverarbeitungsregister zu erfolgen hat, normiert sind. Diesbezüglich gelten die allgemeinen Vorschriften des AVG. Diese er-

scheinen jedoch in Anbetracht des Zeitdrucks der Umsetzung von Datenverarbeitungen und der damit verbundenen Zielsetzungen oftmals zu lang.

Es wäre die Entscheidungsfrist der Datenschutzkommission deutlich zu verkürzen und bei Nichtentscheidung vorzusehen, dass die Datenverarbeitung als genehmigt gilt. Dass das möglich ist, zeigen die Bestimmungen über das Bundesvergabeamt, welches im Regelfall auch in komplizierten Fällen innerhalb weniger Tage zumindest vorläufige Entscheidungen zu treffen in der Lage ist.

### **Zu § 50b Abs. 2**

Die Verpflichtung zur Löschung der aufgezeichneten Daten nach grundsätzlich 48 Stunden wird als zu kurz erachtet. Vielfach ist in Betrieben über das Wochenende bzw. über Feiertage grundsätzlich kein Dienstbetrieb gegeben, sodass Schäden nicht sofort ersichtlich sind, und bis zur Anforderung von Aufzeichnungen durch die Polizei auch ein gewisser Zeitraum verstreichen kann.

Sonntage und gesetzliche Feiertage sollten den Ablauf der Frist hemmen.

### **Zu § 50e**

Die Bestimmung des § 50e des Gesetzesentwurfes über das Auskunftsrecht wird in der Praxis schwer umsetzbar sein. Einerseits werden nicht alle Auskunftsansuchen innerhalb der 48-Stunden-Frist erfolgen, andererseits würde bei einer Einsichtnahme auf den Lesegeräten in die Rechte dritter, auf der Aufzeichnung sichtbarer Personen eingegriffen.

Es sollte auch klar sein, ob die bloße Tatsache, dass sich auf einer Aufzeichnung auch andere Personen befinden, schon ausreicht, um die Auskunft zu verweigern.

### **Zu § 50c Abs. 2**

In § 50c Abs. 2 des Gesetzesentwurfes wurde zweimal fälschlicherweise auf § 50a Abs. 1 anstatt auf § 50a Abs. 3 verwiesen.

### **Zu § 60 Abs. 4**

Ein rückwirkendes Inkrafttreten des Gesetzes ist unnötig.

- 5 -

Im Gegenteil: es muss eine längere Legisvakanz vorgesehen werden, um die bestehenden Datenanwendungen allenfalls auf den neuen Stand bringen zu können.

Weiters muss auch die Verordnung über das Datenverarbeitungsregister und die anderen Verordnungen bei Inkrafttreten der Novelle auf dem dann aktuellen Stand sein, ebenso muss die Infrastruktur des Datenverarbeitungsregisters bereits zur Verfügung stehen.

Mit freundlichen Grüßen  
Für den Hauptverband: