



Das Land Steiermark

AMT DER STEIERMÄRKISCHEN LANDESREGIERUNG

Fachabteilung 1F

An das
Bundeskanzleramt - Verfassungsdienst

Ballhausplatz 2
1014 Wien

E-Mail: v@bka.gv.at

➔ **Verfassungsdienst und
Zentrale Rechtsdienste**

Bearbeiter: Mag. Christian Freiberger
Tel.: (0316) 877 -4110
Fax: (0316) 877 -4395
E-Mail: fa1f@stmk.gv.at

Bei Antwortschreiben bitte
Geschäftszeichen (GZ) anführen

GZ: FA1F-52.01-19/2007-3 Bezug: BKA-810.026/0005-
V/3/2009

Graz, am 15. Juni 2009

Ggst.: DSG-Novelle 2010;
Stellungnahme des Landes Steiermark

Sehr geehrte Damen und Herren!

Zu dem mit do. Schreiben vom 20. Mai 2009, obige Zahl, übermittelten Entwurf eines Bundesgesetzes, mit dem das Bundes-Verfassungsgesetz, das Datenschutzgesetz 2000 und das Sicherheitspolizeigesetz geändert wird (DSG-Novelle 2010), wird seitens des Landes Steiermark folgende Stellungnahme abgegeben:

Zu den einzelnen Bestimmungen:

Artikel 1 (Änderung des Bundes-Verfassungsgesetzes)

Das Land Steiermark hat immer eine einheitliche Gesetzgebungszuständigkeit für Datenschutz in Österreich befürwortet.

Derzeit existiert in der Steiermark ein eigenes Landes-Datenschutzgesetz. Da mit der Neuregelung der Kompetenzverteilung durch Artikel 1 und die gleichzeitige Behebung des § 2 DSG 2000 für die Länder keine Gesetzgebungszuständigkeit mehr bestehen würde, würde dieses Gesetz mit Inkrafttreten des Artikel 1 (geplant: 1.Jänner 2010) verfassungswidrig. Es sollte daher überlegt werden, gleichzeitig die landesrechtlichen Bestimmungen aufzuheben.

8010 Graz Burgring 4 •

Wir sind Montag bis Freitag von 8:00 bis 12:30 Uhr und nach telefonischer Vereinbarung für Sie erreichbar
Öffentliche Verkehrsmittel: Straßenbahn Linien ..., Haltestelle ...

DVR 0087122 • UID ATU37001007 • Landes-Hypothekenbank Steiermark: BLZ: 56000, Kto.Nr.: 20141005201

IBAN AT 375600020141005201 • BIC HYSTAT20
Dieses Dokument wurde mittels e-Mail von Verfassungsdienst zur Verfügung gestellt. Für die Richtigkeit und Vollständigkeit des Inhaltes wird von der Parlamentsdirektion keine Haftung übernommen.

www.parlament.gv.at

Artikel 2 (Änderung des Datenschutzgesetzes 2000)

Zu Z. 1 und. 2 (§ 1) sowie Z. 52 und 54:

Im aktuellen Entwurf bleibt der Begriff „jedermann“ unverändert. Daraus ist zu schließen, dass - im Gegensatz zum Entwurf einer DSG-Novelle 2008 - auch juristische Personen weiterhin im Schutzbereich des Grundrechts verbleiben sollen.

Ob dies tatsächlich so ist, ist nicht völlig klar: In der Textgegenüberstellung wird in § 4 Abs. 1 Z. 3 der Begriff „Betroffener“ als „jede vom Auftraggeber (Z 4) verschiedene natürliche Person, deren Daten verwendet werden (Z8)“ definiert. Da diese Änderung allerdings nicht im Entwurfstext enthalten ist, geht die Steiermärkische Landesregierung von einem Versehen in der Textgegenüberstellung aus. Darüberhinaus sind nach der derzeitigen Rechtslage auch „Personengemeinschaften“ als Betroffene anzusehen. Zwar wird in § 30 das Recht, sich an die Datenschutzkommission zu wenden, jedermann, also auch juristischen Personen und Personengemeinschaften, eingeräumt, die Neufassung der §§ 31 und 32 sehen allerdings bloß Beschwerden und Ansprüche von „Personen“ vor, wonach zweifelhaft ist, wer nun tatsächlich darunter fällt. Eine Klarstellung und Vereinheitlichung wäre wünschenswert.

Zusätzlicher Vorschlag:

Die derzeitige Einschränkung auf das lebenswichtige Interesse des Betroffenen führt in der Praxis der Verwaltungsbehörden immer wieder zu Schwierigkeiten. Dies insbesondere in den Fällen, in denen die Behörde auf Grund durchzuführender Verfahren Informationen über bestimmte Personen besitzt, die auch für andere Bereiche wesentlich wären. Dies betrifft insbesondere die gesundheitliche Eignung, die für den Entzug von Lenkberechtigungen oder den Entzug von Waffen von Bedeutung ist.

Die Datenschutzkommission hat zwar versucht, der Problematik Herr zu werden, indem sie im Einzelfall die Übermittlung von Gesundheitsdaten an die Führerscheinbehörde für rechtmäßig erklärt hat, musste dafür aber das Argument der „Gefahr des Lenkers für sich selbst“ heranziehen (vgl DSK vom 5. 4. 2002, K120.766). Dies ist allerdings nur eine Hilfskonstruktion, mit der die fehlende Möglichkeit, Grundrechtsbeschränkungen auch im „Interesse des Schutzes der Allgemeinheit“ vornehmen zu können, hilfsweise saniert wird. Es sollte daher überlegt werden, einen Eingriff auch „zum Schutz der Allgemeinheit“, wenn auch unter strengen Kriterien, vorzusehen.

Zu Z. 36 (§ 17 Abs. 1a):

Auf Grund des neuen Abs. 1a sollen alle Meldungen über eine Internetanwendung eingebracht werden. Diese aus Sicht des DVR sicher zu begrüßende Vorgangsweise der ausschließlichen elektronischen Einbringung wird damit begründet und sachlich gerechtfertigt, dass der Kreis der Meldepflichtigen ausschließlich Personen umfasst, die Datenanwendungen einsetzen. Dabei wird aber übersehen, dass dadurch der Aufwand der meldenden Stellen keinesfalls geringer wird, denn jede Meldung wird in der Internetanwendung manuell einzugeben sein – unabhängig davon, ob der Auftraggeber die Dateien automationsunterstützt oder händisch führt.

Meldungen für komplexe Verarbeitungen können nicht einfach in eine Bildschirmmaske eingegeben werden. Sie erfordern im Vorfeld die Zusammenarbeit mehrerer Personen und zu meist mehrerer Abstimmungsrunden. Das Land Steiermark setzt derzeit ein internes datenbankgestütztes Workflow-System ein, mit dem alle Datenanwendungen der meisten Landesdienststellen (Amt der Landesregierung, Bezirksverwaltungsbehörden) intern verwaltet werden; aus diesem heraus werden auch die Meldungen an das DVR automationsunterstützt erstellt und per E-Mail versendet.

Der Aufwand wird nur dann gering gehalten, wenn die Möglichkeit besteht, bereits derzeit bei Auftraggebern eingesetzte interne Systeme mit dem geplanten System der Interneteinbringung zu verbinden. Es sollte daher nicht nur ein Formular sondern auch eine entsprechende Schnittstelle zur Übermittlung zwischen IT-Systemen vorgesehen werden. Ein Online-Formular sowie die erwähnte Schnittstelle soll im Bereich der öffentlichen Verwaltung im Wege des etablierten Portalverbundes authentifiziert und berechtigt werden.

Zu Z. 39 (§ 20):

Das neue System stellt einen gewagten Sprung dar, wenn man bedenkt, dass derzeit gerade einmal Winword- oder PDF-Formulare über E-Mail eingebracht werden können und schon lange von einer Anwendung zur Abgabe der Meldungen geredet wird. Es stellen sich diesbezüglich Fragen, die große praktische Auswirkungen haben: Was heißt Plausibilitätsprüfung? Was wird dabei geprüft und was ist der Unterschied zur Prüfung auf Mangelhaftigkeit, die bei der Vorabkontrolle erforderlich ist? Was passiert, wenn die Anwendung holprig läuft? Zu diesen Fragen geben die Erläuterungen keine Antwort.

Gemäß Art. I Abs. 2 Z. 36 EGVG hat die DSK das AVG anzuwenden. Es ist – auch nach der Neuformulierung des § 20 – davon auszugehen, dass für das Prüf- und Verbesserungsverfahren das AVG gilt (vgl. Dohr-Pollirer-Weiss, DSG², Anm. 2 zu § 20). Es dürfte daher verfahrensrechtlich nicht zulässig sein, nach einem nicht korrigierten Verbesserungsauftrag die Registrierung der Meldung gemäß § 20 Abs. 5 bloß durch schriftliche Mitteilung abzulehnen (es handelt sich dabei nämlich um eine das Verfahren abschließende Erledigung, mit der über Parteirechte abgesprochen wird) und erst

als zweiten Schritt – nämlich nach ausdrücklichem Verlangen der Partei (also des Auftraggebers) – einen Bescheid auszustellen; zumindest ist kein Grund für ein erforderliches Abweichen vom AVG gemäß Art. 11 Abs. 2 B-VG erkennbar.

Zu Z. 48 (§ 30 Abs. 2a):

Es wird darauf hingewiesen, dass § 30 keinen Abs. 1a besitzt, auf den verweisen werden könnte.

Zu Z. 76 (§ 46 Abs. 3a):

Die Neufassung des § 46 führt zwar zu einer Klarstellung, wer sich um die Genehmigung der Datenschutzkommission bemühen muss, löst aber nicht die bestehenden Probleme.

Die in Abs. 3a vorgesehene Erklärung, dass dem Auftraggeber die Datenbestände zur Verfügung gestellt werden, ist eine für die Datenschutzkommission praktikable Vorgangsweise, um unnötigen Aufwand zu vermeiden. Allerdings stellt sich die Frage, welche Qualität eine derartige Erklärung aus datenschutzrechtlicher Sicht besitzt. Immer wieder sollen wissenschaftliche Untersuchungen durchgeführt werden, deren Ausgangsmaterial Daten sind, die bei Behörden im Rahmen der Hoheitsverwaltung angefallen sind. Für die Übermittlung derartiger Daten sind aber – entsprechend § 1 Abs. 2 DSGVO – Gesetze als Eingriffsgrundlage in das Grundrecht erforderlich. Gemäß § 7 Abs. 2 DSGVO dürfen bei Übermittlungen u.a. die schutzwürdigen Geheimhaltungsinteressen nicht verletzt werden.

Ob § 46 Abs. 2 DSGVO selbst eine Übermittlungsgrundlage darstellt, scheint zweifelhaft. Nach Abs. 2 Z. 3 dürfen „Daten ... mit Genehmigung der Datenschutzkommission gemäß Abs. 3 verwendet werden“. Dieses „Verwenden“ bezieht sich allerdings nur auf den Auftraggeber, der Daten ermitteln will, denn die Daten dürfen nur mit Genehmigung verwendet werden, nicht jedoch auf Grund einer Genehmigung. Darüber hinaus bezieht sich die Genehmigung nach Abs. 3 ausschließlich auf das Ermitteln (vgl. den 2. Satz: „Sollen sensible Daten ermittelt werden...“, als zusätzliche Voraussetzung gegenüber dem Ermitteln von sonstigen Daten). Es ist daher davon auszugehen, dass „verwenden“ im Abs. 2 nicht die Übermittlung meint.

Eine Übermittlung könnte daher allenfalls nach § 8 DSGVO gerechtfertigt sein: Gemäß § 8 Abs. 1 Z. 4 sind gemäß § 1 Abs. 1 bestehende schutzwürdige Geheimhaltungsinteressen bei der Verwendung nicht sensibler Daten dann nicht verletzt, wenn überwiegende berechnete Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern. Zur Konkretisierung legt nun Abs. 3 fest, dass schutzwürdige Geheimhaltungsinteressen aus dem Grunde des Abs. 1 Z. 4 insbesondere dann nicht verletzt sind, wenn die Verwendung der Daten nach Z. 1 bis 7 erfolgt. Das Wort „insbesondere“ drückt aus, dass es auch noch andere Kriterien und Gründe für eine Datenverwendung (also auch eine Übermittlung) geben muss. Auch entsprechend der Erläuterungen handelt es sich bei den in Abs. 3 aufgezählten

Fällen nicht ausschließlich um Zulässigkeitsvoraussetzungen, sondern diese Punkte haben vielmehr die Bedeutung einer Leitlinie bei der Interessenabwägung. Eine Übermittlung von Daten (z.B. auch durch Einsichtnahme an einen Forschenden) könnte daher dann gerechtfertigt sein, wenn eine Genehmigung der Datenschutzkommission vorliegt, wenn kein Zweifel daran besteht, dass der Forscher bzw. die Einrichtung sorgsam mit den Daten umgeht und alle Auflagen der Datenschutzkommission eingehalten werden.

Um alle Zweifel auszuschließen, ob eine Genehmigung der Datenschutzkommission für einen Auftraggeber, bestimmte Daten zu ermitteln, ausreicht, auch die Übermittlung für den die Daten besitzenden Auftraggeber zu rechtfertigen, sollte dies im Gesetz ausdrücklich klargestellt werden.

Zu Z. 82(§ 50a):

In Österreich werden – im Gegensatz zur deutschen Rechtslage – Verwendungsbestimmungen für Daten in bestimmten Bereichen noch relativ selten (allerdings mit steigender Tendenz) gesetzlich geregelt. Daher wird es begrüßt, dass erstmals generelle Regelungen über Videoaufnahmen geschaffen werden.

Trotz der vielen Verbesserungen im Hinblick auf den Entwurf 2008 scheint die Bestimmung des Abs. 3 Z. 2 weiterhin unklar. Danach wird ein Betroffener nicht in seinen schutzwürdigen Geheimhaltungsinteressen verletzt, wenn Daten über ein Verhalten verarbeitet werden, das ohne jeden Zweifel den Schluss zulässt, dass es darauf gerichtet war, öffentlich wahrgenommen zu werden. Die Erläuterungen führen dazu lediglich aus, dass gewisse Verhaltensweisen insbesondere im öffentlichen Raum typischerweise darauf gerichtet sind, von jedermann wahrgenommen zu werden und daher einer Zustimmung gleichzuhalten sind. Als Beispiele führen die Erläuterungen lediglich „Straßenkunst“ oder Auftritte im Rahmen von Veranstaltungen an. Die gewählte Formulierung scheint daher - auch gemeinsam mit den Erläuterungen - als Abgrenzungskriterium nicht ausreichend geeignet. Fraglich ist insbesondere, ob bereits das gewöhnliche Gehen auf der Straße davon umfasste sein kann, zumal davon ausgegangen werden kann, dass es von jedermann wahrgenommen werden kann. Ebenso verhält es sich mit dem Benutzen von öffentlichen Verkehrsmitteln. Bei einem derart weiten Verständnis würden bei jedem Verhalten im öffentlichen Raum schutzwürdige Geheimhaltungsinteressen nicht vorliegen.

Es scheint daher erforderlich, die Abgrenzungskriterien in Z. 2 deutlicher herauszuarbeiten, um Missverständnisse zu vermeiden und rechtswidrige Eingriffe von vornherein zu vermeiden.

Zu Z. 82 (§ 50c):

Da Videoaufnahmen potentiell sensible Daten enthalten, unterliegen sie auch immer einer Vorabkontrolle. Bei diesen Meldungen sind auch die bestimmten Tatsachen im Sinne von § 50a Abs. 1 Z. 5 und die Anspruchsverfolgung nach § 50a Abs. 1 Z. 7 (richtig wohl: Abs. 3 Z. 7) glaubhaft zu machen. Daher scheint es nicht gerechtfertigt, bloß aus dem Grunde, die Aufnahme werde mit einem analogen Medium gemacht, auf eine Registrierung zu verzichten und solche Aufzeichnungen damit derartig zu privilegieren.

Zu Z. 82 (§ 50e):

Die Auskunftserteilung wird sich in der Praxis als problematisch erweisen. Zum einen deswegen, weil die Aufbewahrungsdauer gemäß § 50b mit 48 Stunden begrenzt ist, zum anderen deswegen, weil die Anonymisierung nicht beteiligter Dritter problematisch bis unmöglich ist, der Auskunftswerber aber an der bloßen Beschreibung seines Verhaltens (Abs. 2) möglicherweise nicht interessiert sein wird.

Dem Präsidium des Nationalrates werden unter einem 25 Abdrucke dieser Stellungnahme zugeleitet. Eine weitere Ausfertigung ergeht an die E-Mail Adresse begutachtungsverfahren@parlament.gv.at.

Mit freundlichen Grüßen

Für die Steiermärkische Landesregierung

Der Landesamtsdirektor

(Dr. Gerhard Ofner)