- Datenpost

Newsletter der österreichischen Datenschutzkommission (DSK)

Nr. 2/Februar 2007 (Versand: 22 Februar 2007)

A - DSK-Entscheidungen

Die Datenschutzkommission möchte auf folgende ihrer Entscheidungen, die kürzlich in die DSK-Entscheidungsdokumentation im Rechtsinformationssystem des Bundes aufgenommen worden sind, hinweisen:

---

1. Bescheid Beschwerde GZ: K121.224/0011-DSK/2006 vom 29.9.2006

Recht auf Löschung, Datenverwendung für Zwecke der gesetzgebenden Gewalt, Parlamentshomepage, Zurechnung des Ergebnisses von Suchmaschinenabfragen, Unzuständigkeit der DSK (Zurückweisung). Der Beschwerdeführer wandte sich mit Beschwerde gegen die Parlamentsdirektion (Beschwerdegegnerin) und brachte vor, in einer auf der Homepage des Parlaments (http://www.parlament.gv.at) veröffentlichten schriftlichen Anfrage von Nationalratsabgeordneten an die Bundesministerin für Justiz würden ihn betreffende personenbezogene Daten (Hinweis auf eine gegen den Beschwerdeführer erstattete Strafanzeige) verwendet. Er habe sich deswegen mit einem Löschungsbegehren an die Beschwerdegegnerin gewandt; dieses sei aber unzureichend erfüllt worden (aus dem Text der schriftlichen Anfrage auf dem Server der Parlamentshomepage wurde der Name des Beschwerdeführers nachweislich gelöscht), da die entsprechenden Daten mit Hilfe einer gebräuchlichen Internetsuchmaschine noch immer gefunden und abgerufen werden könnten (diese Tatsache wurde vom Beschwerdeführer bescheinigt). Die DSK wies die Beschwerde mit der tragenden Begründung zurück, bei der Datenverwendung für Zwecke des parlamentarischen Frage- bzw. Interpellationsrechts handle es sich um eine Datenverwendung für Zwecke der Staatsfunktion „Gesetzgebung“ (Mitwirkung des Nationalrats an der Vollziehung), die gemäß § 1 Abs 5 DSG 2000 von der Zuständigkeit der DSK ausgenommen ist. Weiters führte die DSK aus, dass dem Betreiber einer Website als datenschutzrechtlichem Auftraggeber die Suchergebnisse in Internetsuchmaschinen keinesfalls zugerechnet werden können, weil diese vom Suchalgorithmus der Maschine erzeugt werden, sodass der Anbieter des Suchdienstes als Auftraggeber (§ 4 Z 4 DSG 2000) allfälliger personenbezogener Ergebnisse anzusehen ist. Auch aus diesem Blickwinkel sei die Zuständigkeit der DSK nicht gegeben (Anbieter des Suchdienstes war ein Auftraggeber des privaten Bereichs mit Sitz in einem Drittstaat).

Direktlink (Volltext): GZ: K121.224/0011-DSK/2006

---

2. Bescheid Beschwerde GZ: K121.220/0001-DSK/2007 vom 2.2.2007

Recht auf Auskunft, Negativauskunft, Umfang (Teilstattgebung). Die Sozialversicherungsanstalt der gewerblichen Wirtschaft (Beschwerdeführerin) verlangte vom Inhaber einer Wirtschaftsauskunftei (Einzelunternehmen, Beschwerdegegner) Auskunft über die zu ihrer Person verarbeiteten Daten, nachdem einige Versicherte sich darüber beschwert hatten, dass von der Beschwerdeführerin angestrengte Exekutionsverfahren wegen Beitragsrückständen aus Datenanwendungen dieser Wirtschaftsauskunftei ersichtlich seien. Der Beschwerdegegner lehnte das Auskunftsbegehren zunächst mit der Begründung ab, die Beschwerdeführerin sei nicht Betroffene, ergänzte dies dann aber um die Angabe, es würden keine Daten der Beschwerdegegnerin verwendet. Die Sozialversicherung erhob darauf Beschwerde an die DSK wegen Verletzung im Recht auf Auskunft. Das Ermittlungsverfahren ergab, dass die Datenanwendung (Schuldnerdatenbank) des Beschwerdegegners in etwa 2,2 Millionen Datensätze enthält. Eine Suche nach den Gläubigern der in der Datenanwendung erfassten Schuldner ist über die zur Verfügung stehende Suchmaske nicht möglich. Die Gläubiger werden im Übrigen regelmäßig nicht namentlich sondern nur mit einer Branchenbezeichnung wie – im Falle der Beschwerdeführerin – „SVA“ (hier für: Sozialversicherungsanstalt allgemein) oder „Sozialversicherung“ erfasst. Die namentliche Erfassung von Gläubigern in Einzelfällen kann aber nicht ausgeschlossen werden. Rechtlich kam die DSK zu dem Schluss, dass der Beschwerdeführer (im zweiten Anlauf) zumindest eine minimale Negativauskunft erteilt hat. Aus § 26 Abs 4 DSG 2000 ist ein jedermann zustehendes Recht auf Auskunft darüber ableitbar, ob überhaupt Daten über ihn in einer Datenanwendung verarbeitet werden; die gegenteilige Ansicht des Beschwerdegegners (nur der tatsächlich Betroffene, dessen Daten verarbeitet würden, habe ein Recht auf Auskunft) ist unzutreffend. Auf Grundlage des Suchergebnisses war die Negativauskunft, es würden keine Daten der Beschwerdeführerin verwendet, aber richtig; insoweit war die Beschwerde abzuweisen. Da man aber nicht ausschließen könne, dass eine (wesentlich aufwändigere) sequentielle oder eine gezielte Suche nach Daten der Beschwerdeführerin (über die Namen von Schuldnern) vielleicht doch Daten der Beschwerdeführerin liefern würde, hätte der Beschwerdegegner aber – direkt gegenüber der Beschwerdeführerin - zumindest eine nähere entsprechende Begründung für seine Negativauskunft geben müssen; insoweit war die Auskunft inhaltlich unvollständig, eine entsprechende Ergänzung wurde bescheidmäßig aufgetragen.

Direktlink (Volltext): GZ: K121.220/0001-DSK/2007
Direktlink (Rechtssatz): GZ: K121.220/0001-DSK/2007 - RS1

B – gerichtliche Judikatur

Auf folgende (höchst-)gerichtliche Entscheidungen, die über Entscheidungen der DSK ergangen sind oder doch für das Datenschutzrecht relevant sind, möchte die DSK hinweisen:

---

1. VwGH Erkenntnis Zl. 2004/01/0086 vom 9. Mai 2006

Datenermittlung für sicherheitspolizeiliche Zwecke durch Observation, Zuständigkeitsabgrenzung UVS-DSK (Stattgebung einer Amtsbeschwerde) Mit dem angefochtenen Bescheid hatte ein Unabhängiger Verwaltungssenat (UVS) einer Beschwerde wegen der Observation eines Hauses durch Polizeibeamte (die hier, nach dem vom UVS festgestellten Sachverhalt, nicht im Dienste der Strafjustiz tätig waren) gemäß § 88 Abs 2 SPG Folge gegeben. Der Bescheid wurde auf Grund einer Amtsbeschwerde des Bundesministers für Inneres (BMI) vom VwGH aufgehoben. Der VwGH begründet dies mit der Unzuständigkeit des UVS: § 54 SPG sehe für die Ermittlung personenbezogener Daten im Rahmen der Sicherheitspolizei besondere Bestimmungen vor und lege in seinem Abs. 2 die Voraussetzungen für die Zulässigkeit derartiger Vorgänge durch Beobachten (Observation) fest. Die polizeiliche Überwachung (in diesem Sinne) sei weder als Befehl mit unverzüglichem Befolgungsanspruch noch als Anwendung physischen Zwangs und damit auch nicht als Ausübung unmittelbarer verwaltungsbehördlicher Befehls- und Zwangsgewalt gegen eine bestimmte Person zu beurteilen. Es liege vielmehr eine Verwendung personenbezogener Daten vor. Daraus folge, dass die Rechtmäßigkeit von Ermittlungsmaßnahmen zur Erhebung personenbezogener Daten im Rahmen der Sicherheitspolizei, die keine Akte unmittelbarer Befehls- und Zwangsgewalt sind, als Unterfall des „Verwendens“ derartiger Daten gemäß § 90 SPG von der Datenschutzkommission zu überprüfen ist.

Direktlink (Volltext): Zl. 2004/01/0086

---

2. VwGH Erkenntnis Zl. 2006/06/0283 vom 23. Jänner 2007

Recht auf Geheimhaltung, Datenverwendung für Zwecke der Judikaturdokumentation Justiz im RIS, Bundeskanzleramt nicht Auftraggeber (Abweisung) Mit dem angefochtenen Bescheid, GZ: K120.917/0008-DSK/2004 vom 28. Mai 2004, hatte die DSK eine Beschwerde gegen das Bundeskanzleramt (BKA) abgewiesen, in der eine Verletzung im Grundrecht durch eine unvollständig anonymisierte und zeitweilig online abrufbare Entscheidung des Obersten Gerichtshofes (OGH) geltend gemacht worden war. Der Beschwerdeführer hatte dabei ausdrücklich vorgebracht, das BKA sei als Auftraggeber für das Rechtsinformationssystem des Bundes (RIS) verantwortlich. Der VwGH bestätigte nunmehr diesen Bescheid der DSK. Die DSK habe im Beschwerdefall aus Bestimmungen des DSG 2000, des OGHG und des BGBlG zu Recht gefolgert, dass das BKA nicht als Auftraggeber verantwortlich gemacht werden kann (weder der Bundeskanzler noch das BKA als sein Hilfsapparat). Die Frage, ob der OGH im gegebenen Zusammenhang vor der DSK hätte belangt werden können, wurde vom VwGH nicht erörtert. (VwGH-Erkenntnis noch nicht im RIS)

Direktlink (Volltext): Zl. 2006/06/0283 (RIS-Auswertung in Arbeit!)
Direktlink (Volltext): GZ: K120.917/0008-DSK/2004

---

3. deutscher Bundesgerichtshof (BGH) Beschluss vom 31. Januar 2007 - StB 18/06 ("Bundestrojaner")

Verdeckte Online-Durchsuchung unzulässig (Verwerfung einer Beschwerde des deutschen Generalbundesanwalts gegen einen Beschluss des Ermittlungsrichters beim BGH) Die heimliche Durchsuchung der im Computer eines Beschuldigten gespeicherten Dateien mit Hilfe eines Programms, das ohne Wissen des Betroffenen aufgespielt wurde (verdeckte Online-Durchsuchung), ist nach der Strafprozessordnung unzulässig. Es fehlt an der für einen solchen Eingriff erforderlichen Ermächtigungsgrundlage. Das hat der 3. Strafsenat des Bundesgerichtshofs auf die Beschwerde des Generalbundesanwalts gegen einen Beschluss entschieden, mit dem der Ermittlungsrichter des Bundesgerichtshofs den Antrag auf eine verdeckte Online-Durchsuchung abgelehnt hatte. Nach der Entscheidung ist die verdeckte Online-Durchsuchung insbesondere nicht durch § 102 StPO (Durchsuchung beim Verdächtigen) gedeckt, weil die Durchsuchung in der Strafprozessordnung als eine offen durchzuführende Ermittlungsmaßnahme geregelt ist. Dies ergibt sich zum einen aus mehreren Vorschriften des Durchsuchungsrechts zu Gunsten des Beschuldigten - Anwesenheitsrecht (§ 106 Abs. 1 Satz 1 StPO) und Zuziehung von Zeugen (§ 105 Abs. 2, § 106 Abs. 1 Satz 2 StPO) -, deren Befolgung als zwingendes Recht nicht zur Disposition der Ermittlungsorgane steht. Zum anderen folgt dies aus einem Vergleich mit den Ermittlungsmaßnahmen, die - wie die Überwachung der Telekommunikation (§§ 100 a, b StPO) oder die Wohnraumüberwachung (§§ 100 c, d StPO) - ohne Wissen des Betroffenen durchgeführt werden können, für die aber deutlich höhere formelle und materielle Anforderungen an die Anordnung und Durchführung bestehen. Auch andere Befugnisnormen der Strafprozessordnung gestatten die verdeckte Online-Durchsuchung nicht. (Quelle: Pressemitteilung des BGH)

anonymisierter Volltext (PDF-Dokument): StB 18/06

---

4. OGH Beschluss AZ: 9 ObA 109/06d vom 20. Dezember 2006

Biometrische Identifizierung, Zeiterfassungssystem, Sicherung der Mitbestimmungsrechte der Belegschaft, einstweilige Verfügung (Nicht-Folgegebung) Ein Organ der Belegschaft (Betriebsausschuss eines Krankenhauses) begehrt mit arbeitsgerichtlicher Unterlassungsklage die Untersagung der Verarbeitung personenbezogener biometrischer Daten (Fingerabdruckscan) für Zwecke eines Zeiterfassungssystems („biometrische Stechuhr“), da die gemäß § 96 ArbVG zwingend erforderliche Zustimmung (in Form des Abschlusses einer Betriebsvereinbarung) nicht vorliege. Einem Antrag auf einstweilige Verfügung wurde in erster und zweiter Instanz stattgegeben. Der OGH bestätigte diese Provisorialentscheidungen nunmehr im Wege des (ordentlichen) Revisionsrekurses. Begründend führt der OGH aus, es handle sich bei der Einführung eines derartigen Kontrollsystems um eine Maßnahme gemäß § 96 Abs 1 Z 3 ArbVG. Der OGH kommt, nach umfassenden Erwägungen unter Würdigung der bestehenden Lehre und Judikatur und einer Abwägung der widerstreitenden Interessen, zu dem Schluss, dass durch ein solches System die „Menschenwürde“ der betroffenen Arbeitnehmer berührt wird. Jeder Mensch habe auch während der Zeit, in der er zur Arbeitsleitung in einem Arbeitsverhältnis verpflichtet ist, unter anderem ein Recht auf „Unversehrtheit der Intimsphäre“. Doch auch die

Kontrolle rein dienstlichen Verhaltens könne gemäß § 96 Abs 1 Z 3 ArbVG zustimmungspflichtig sein, wenn eine über das für die Erreichung des Kontrollzwecks notwendige Ausmaß hinausgehende Kontrolldichte erreicht werde. Die Intensität sei entscheidend (Art, Dauer, Umfang und Sensibilität der erfassten Datenarten). Die Menschenwürde werde dann „berührt" (der OGH unterscheidet dabei scharf zwischen „berühren" und „verletzen"; ersteres sei zustimmungspflichtig, zweiteres unzulässig), wenn durch eine Kontrollmaßnahme oder ein Kontrollsystem die vom Arbeitnehmer in den Betrieb mit eingebrachte Privatsphäre kontrolliert werde. Es sei stets das schonendste - noch zum Ziel führende – Kontrollmittel zu wählen. Die Erfassung und Kontrolle der geleisteten Arbeitszeit begründe keine Beeinträchtigung der Persönlichkeit des Arbeitnehmers, Aufzeichnungen darüber seien (in einer Krankenanstalt) auch gesetzlich vorgeschrieben. Die Verwendung von Vorrichtungen zur Zeiterfassung und Anwesenheitskontrolle (Stechuhren, einschließlich solcher mit Magnetkarten) sei nicht zustimmungspflichtig, solange keine Erstellung eines arbeitnehmerbezogenen Bewegungsprofils ermöglicht werde. Die Verwendung eines so genannten „Templates" (aus einem biometrischen Merkmal, hier dem Fingerabdruck, errechneter Referenzdatensatz, der im Normalfall keine Rekonstruktion des vollständigen biometrischen Merkmals [des Fingerabdruckmusters] ermöglicht) stelle eine Verwendung personenbezogener Daten dar. Eine Verwendung solch biometrischer Daten ohne Berührung der Menschenwürde wäre denkbar (etwa: Zutrittskontrollsystem, das nur zwischen „berechtigt" und „unberechtigt" unterscheidet, ohne dies mit einer bestimmten Person zu verknüpfen, laut OGH ein Fall der Verwendung indirekt personenbezogener Daten). Im vorliegenden Fall liege aber ein Fall der Verwendung direkt personenbezogener Daten der einzelnen Arbeitnehmer vor. Vom Träger des Krankenhauses (gefährdende Partei vor dem OGH) angeführte Vorteile des Systems (höhere Betriebssicherheit, keine Diebstahls- oder Manipulationsmöglichkeiten) vermochten im Provisorialverfahren jedoch nicht zu überzeugen, das der Eingriff (im Vergleich mit „herkömmlichen" Zutrittskontrollsystemen) das gelindeste Mittel sei. Daher berühre er die Menschenwürde der Betroffenen. Da aber keine Betriebsvereinbarung abgeschlossen worden sei und die gefährdende Partei im Verfahren bekräftigt habe, an der Maßnahme festhalten zu wollen, komme dem Betriebsausschuss das Recht auf Sicherung seines Mitbestimmungsanspruchs durch Erlassung einer einstweiligen Verfügung gemäß § 381 Z 1 EO zu.

anonymisierter Volltext (PDF-Dokument): 9 ObA 109/06d

Impressum: Medieninhaber, Herausgeber und Redaktion: Datenschutzkommission (DSK, Bundesbehörde gemäß §§ 35ff DSG 2000), Ballhausplatz 1, 1014 Wien.
Kontakt: dsk@dsk.gv.at
Website: http://www.dsk.gv.at
RIS-Entscheidungsdokumentation der DSK: http://www.ris.bka.gv.at/dsk/
Für die (dauerhafte) Funktion von direkten Hyperlinks und PDF-Verknüpfungen zu einzelnen RIS-Dokumenten kann leider keine Gewähr übernommen werden.
Dieser Newsletter (Medium gem § 1 Abs. 1 Z 5a lit c MedienG) erscheint nach Bedarf (mindestens viermal jährlich) und wird per E-Mail verbreitet. Grundlegende Richtung: Informationen über wichtige Entscheidungen der DSK (Informationspflicht gem § 39 Abs 4 DSG 2000), sonstige Tätigkeit der DSK und datenschutzrechtliche Fragen.
Der Bezug ist kostenlos.
An-/Abmeldung: E-Mail an dsk@dsk.gv.at
Information gemäß § 24 DSG 2000: Nach Anmeldung werden Name und E-Mail-Adresse des Beziehers von der Datenschutzkommission als Auftraggeber (DVR: 0000027, die Datenverwendung erfolgt gedeckt durch die Standardanwendung SA030 „Öffentlichkeitsarbeit und Informationstätigkeit durch

öffentliche Funktionsträger und deren Geschäftsapparate„ gemäß Standard- und Muster-Verordnung 2004 (StMV 2004), BGBl. II Nr. 312/2004) verarbeitet (gespeichert und für Zwecke der Versendung benützt). Es werden keinerlei Daten zum Übermittlungsvorgang (Zustell- oder Lesebestätigungen) ermittelt. Nach Abmeldung vom Bezug werden die Daten aus dieser Datenanwendung gelöscht. Eine Übermittlung dieser Daten ist nicht vorgesehen. Die Datenanwendung für Zwecke dieses Newsletters (einschließlich der zur Verbreitung benützten Mailserver) wird auf EDV-Anlagen des Bundeskanzleramts (Dienstleister der DSK) gehostet.