



# - Datenpost

Newsletter der österreichischen Datenschutzkommission (DSK)

Nr. 4/Juli 2008 (Versand:17. Juli 2008)

## 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 Registrierung GZ: K600.054-001/0002-DVR/2008 vom 20. 6. 2006**  
**Bescheid Registrierung GZ: K600.055-001/0002-DVR/2008 vom 20. 6. 2006**

**Videoüberwachung an Schulen als Mittel der Aufsicht und Erziehung mangels gesetzlicher Grundlage unzulässig, bei allgemein zugänglichen Flächen jedoch als Mittel des hausrechtlich begründeten Eigen- und Verantwortungsschutzes unter Auflagen zulässig** ([Teil-]Ablehnung, Auflagen) In zwei Fällen waren Registermeldungen von Schulleitern zu prüfen, die die Notwendigkeit der Videoüberwachung (mit Bildaufzeichnung) zur Verhinderung von „Schülerdelikten“ und zur Verstärkung der Aufsicht auf Gängen, in Garderoben und auf anderen nur für Schulangehörige zugänglichen Flächen während der Zeit des Unterrichts argumentierten. Im zweiten Fall wurde zusätzlich die Überwachung des von außen frei zugänglichen Fahrradabstellraums gemeldet. In beiden Registrierungsverfahren waren sicherheitsrelevante Vorfälle an den betreffenden Schulen bescheinigt worden. Die DSK lehnte die Registrierung im ersten Fall zur Gänze ab, im zweiten Fall wurde sie nur hinsichtlich der Fahrradabstellanlage unter Erteilung von Auflagen vorgenommen. Die DSK vertrat dabei den Standpunkt, die im SchUG geregelte schulische Erziehung samt Aufsicht stelle einen hoheitlichen Eingriff einer „staatlichen Behörde“ in das Grundrecht auf Geheimhaltung dar, der gemäß § 1 Abs. 2 DSG 2000 einer gesetzlichen Ermächtigung bedürfe. Da das Schulrecht keine solche vorsehe, sei die Videoüberwachung als Mittel der schulischen Aufsicht nicht zulässig. Jedoch könne sich eine Schule außerhalb der Schulzeit und hinsichtlich von Räumen, die für Dritte zugänglich und nicht Unterrichtszwecke vorbehalten seien (wie z.B. dem gegenständlichen Fahrradabstellraum) auf Zwecke des Eigen- und Verantwortungsschutzes im Rahmen der Privatwirtschaftsverwaltung berufen, und für diese Zwecke Videoüberwachung einsetzen.

Direktlink (RIS-Volltext): [GZ: K600.054-001/0002-DVR/2008](#) (RIS-neu, Format PDF)  
Direktlink (RIS-Volltext): [GZ: K600.055-001/0002-DVR/2008](#) (RIS-neu, Format PDF)

---

- 2. Bescheid Beschwerde GZ: K120.922/0006-DSK/2007 vom 12. 4. 2007**

**Sicherheitspolizei, Erkennungsdienstliche Daten, DNA-Daten, Zulässigkeit der Datenermittlung im Zusammenhang mit Suchtmittelkriminalität** (Abweisung) In dieser Sache war eine (teilweise) Neuentscheidung in Folge einer Entscheidung des VwGH (Erkenntnis vom 19. September 2006, ZI. 2005/06/0018) über einen negativen Zuständigkeitskonflikt zwischen UVS und DSK zu Gunsten des ersteren notwendig geworden. Der Beschwerdeführer war unter Verdacht von Suchtmitteldelikten auf richterlichen Befehl hin verhaftet worden und wurde während seiner Anhaltung er-kennungsdienstlich behandelt (Fingerabdrücke, Lichtbilder, Mundhöhlenabstrich/DNA-Probe). Die DSK befand, dass auf Grund der Fakten (eingestandener langjähriger, wiederholter Gebrauch und vielfache Weitergabe von Cannabisprodukten; Verdacht nach § 28 Abs. 2 SMG), die Prognose getroffen werden konnte, der Beschwerdeführer habe als Verdächtiger gewohnheitsmäßig und unter ständiger Missachtung der Gesetze gegen den Suchtmittelgebrauch gehandelt und sei deswegen als „gefährlich“ in dem Sinne anzusehen, als er wiederum gefährliche Angriffe nach § 16 Abs. 2 Z 4 SPG begehen würde, so nicht durch sicherheitspolizeiliche Präventivmaßnahmen wie die Verarbeitung seiner er-kennungsdienstlichen Daten die Risikoschwelle für die Betretung bei einer strafbaren Handlung gegen das SMG spürbar hinaufgesetzt würde. Dem Vorbringen des Beschwerdeführers, der unter anderem (unter Behauptung entsprechender kriminalstatistischer Erkenntnisse) die Eignung des Mittels der DNA-Untersuchung zur Gewinnung relevanter er-kennungsdienstlicher Daten zur Identifizierung Verdächtiger bei Suchtmittelkriminalität ganz allgemein bestritten hatte, sei daher zu entgegnen, dass § 67 Abs. 1 SPG nur die Eignung des Mittels der DNA-Untersuchung im Einzelfall, nicht aber dessen erwiesene kriminalpolitische Effektivität über den Einzelfall hinaus fordere. Das Gesetz biete auch keine Grundlage dafür, dass der Anwendungsbereich von § 67 Abs. 1 SPG (= Ermächtigung zur Verarbeitung von DNA-Daten) auf Fälle des Verdachts von Sexual- und Körperverletzungsdelikten beschränkt sein soll.

Direktlink (RIS-Volltext): [GZ: K120.922/0006-DSK/2007](#) (RIS-neu, Format PDF)

### **3. Bescheid Beschwerde GZ: K121.262/0006-DSK/2007 vom 15. 6. 2007**

**Keine Datenschutzverletzung durch Übersendung von Verwaltungsstrafakten an die (Wohn-)Sitzgemeinde des Beschuldigten zwecks Gewährung von Akteneinsicht** (Abweisung) Der Beschwerdeführer wurde von einer räumlich von seinem Wohn- bzw. Unternehmenssitz entfernten Bezirkshauptmannschaft (Beschwerdegegnerin) einer luftfahrtrechtlichen Verwaltungsübertretung beschuldigt. Der Beschwerdeführer verlangte Akteneinsicht durch Übersendung einer vollständigen Kopie der Verwaltungsstrafakten. Die Beschwerdegegnerin übersendete stattdessen die Originalakten, verbunden mit einem Amtshilfeersuchen um Durchführung der Akteneinsicht (Verständigung des Beschwerdeführers, Einsichtsgewährung), kurzzeitig an das Gemeindeamt der (Wohn-)Sitzgemeinde. Die DSK wies die daraufhin erhobene Beschwerde wegen Verletzung des Rechts auf Geheimhaltung ab. Die Vorgehensweise der Beschwerdegegnerin finde in § 17 Abs. 1 AVG Deckung. Ausschlaggebend für diese Auslegung des Verfahrensrechts war einerseits, dass nach der Rechtsprechung des VwGH kein Anspruch der Partei auf Übersendung einer Aktenkopie bestehe, andererseits § 40 Abs. 3 VStG bei großer Entfernung sogar eine Einvernahme des Beschuldigten im Amtshilfeweg durch die Gemeinde seines Aufenthaltsortes vorsehe. Wenn der Gesetzgeber eine solche – als Sonderfall der Amtshilfe nach Art. 22 B-VG zu deutende – Vorgangsweise für Einvernahmen unter Umständen als zweckmäßig erachte, so müsse dies auch als denkmögliche Ermessens-

übung bei der Wahl der Form, in der Akteneinsicht gewährt werden soll, angesehen werden.

Direktlink (RIS-Volltext): [GZ: K121.262/0006-DSK/2007](#) (RIS-neu, Format PDF)

---

#### **4. Bescheid Beschwerde GZ: K121.278/0018-DSK/2007 vom 3.10. 2007**

**Auskunftsrecht, Personenversicherung, Ablehnung eines Versicherungsantrags, Datenaustausch zwischen Versicherungen** (Statteburg) Die B\*\*\* Versicherung AG Österreich (Beschwerdegegnerin) war von einer mit dem Beschwerdeführer geschlossenen Kapitallebensversicherung zurückgetreten. Bei einem Versuch, eine Versicherung (ebenfalls in der Sparte „Leben“, dazu zählen u.a. Kranken-, Unfall- und Lebensversicherungen) bei der AVY\*\*\* Personenversicherung AG abzuschließen, wurde sein Antrag abgelehnt. Die Beschwerdegegnerin hatte den Beschwerdeführer betreffende Daten (Faktum des Rücktritts vom ersten Versicherungsvertrag) über den als „ZIS“ bekannten „Mitteilungsverband“ der österreichischen Versicherungswirtschaft an die AVY\*\*\* Personenversicherung AG übermittelt. Der Beschwerdeführer richtete ein gezieltes Auskunftsbegehren an die Beschwerdegegnerin, ob weitere Daten (insbesondere zu den medizinischen Diagnosen, die für den Rücktritt wahrscheinlich den Ausschlag gegeben hatten) übermittelt worden waren. Nach einer in diesem Punkt verneinenden Auskunft der Beschwerdegegnerin wandte sich der Beschwerdeführer an die DSK. Das Ermittlungsverfahren ergab, dass die Beschwerdegegnerin den Beschwerdeführer betreffende Gesundheitsdaten telefonisch übermittelt hatte (die AVY\*\*\* Personenversicherung AG hatte entsprechende Kontakte schriftlich bestätigt). Die DSK hielt fest, dass eine Verwendung von automatisationsunterstützt gespeicherten Gesundheitsdaten unabhängig von der Form der Speicherung vorliegt. Es mache in Bezug auf das Bestehen des subjektiven Auskunftsrechts daher keinen Unterschied, ob die Daten in einer genau strukturierten und entsprechend aufbereiteten Datenbank verarbeitet oder in einem grafisch gespeicherten Textdokument (etwa einem als Scan gespeicherten ärztlichen Befund) enthalten sind. Das entscheidende Abgrenzungskriterium sei jeweils die Auffindbarkeit der Daten, also die Frage, ob sie mit den beim Auftraggeber üblichen Suchroutinen gefunden und mit der Person des Betroffenen in Zusammenhang gebracht werden können. Dementsprechend wurde der Beschwerdegegnerin die Ergänzung der Auskunft aufgetragen. U.a. dieses Verfahren diene als Anlassfall für eine im Frühjahr 2008 begonnene amtswegige Prüfung (§ 30 Abs. 3 DSG 2000) mehrerer österreichischer Versicherungsunternehmungen durch die DSK (Datenschutz-Audits).

Direktlink (RIS-Volltext): [GZ: K121.278/0018-DSK/2007](#) (RIS-neu, Format PDF)

---

#### **5. Bescheid Beschwerde GZ: K121.327/0002-DSK/2008 vom 18. 1. 2008**

**Konkurrenz von Auskunfts- und Löschungsrecht, Löschungssperre geht jedenfalls bis zum Ende der Viermonatsfrist des § 26 Abs. 7 DSG 2000 vor** (Abweisung) Der Beschwerdeführer verlangte von einer Bundespolizeibehörde (Beschwerdegegnerin) im Abstand von etwas mehr als einem Monat zuerst Auskunft über und sodann die Löschung von Daten, die sich auf ein gegen ihn geführtes Ermittlungsverfahren wegen des Verdachts von Sexualstraftaten bezogen (der Beschwerdeführer war vom Gericht freigesprochen worden). Die Beschwerdegegnerin

lehnte die Löschung ab und begründete dies mit der auf Grund des Auskunftsbegehrens für mindestens vier Monate geltenden Löschungssperre gemäß § 26 Abs. 7 DSG 2000. Der Beschwerdeführer hatte keinerlei Erklärung zur Frage des Auskunftsrechts abgegeben. Die Datenschutzkommission bestätigte die Ansicht der Beschwerdegegnerin und wies die wegen Verletzung im Recht auf Löschung erhobene Beschwerde ab. Während eines anhängigen Auskunftsbegehrens und eines darauf folgenden Beschwerdeverfahrens vor der Datenschutzkommission sei jede Löschung von Daten des Betroffenen gemäß § 26 Abs. 7 DSG 2000 gesetzlich verboten. Der Begriff 'vernichten' in § 26 Abs. 7 DSG 2000 umfasse dabei sowohl das Löschen von Daten in automationsunterstützt geführten Datenanwendungen wie auch das Unleserlichmachen von Daten auf oder die physische Zerstörung von sonstigen Datenträgern einer (manuellen) Datei (Hinweis auf die Strafdrohung in § 52 Abs. 1 Z 4 DSG 2000). Stelle ein Betroffener daher gleichzeitig oder in knapper zeitlicher Abfolge ein Auskunfts- und ein Löschungsbegehren, so gehe § 26 Abs. 7 DSG 2000 als *lex specialis* § 27 Abs. 1 und 4 DSG 2000 vor, auch dann, wenn grundsätzlich die Voraussetzungen für die Löschung gegeben seien. Die Daten dürften in einem solchen Fall erst gelöscht werden, wenn das Auskunftsbegehren im Sinne von § 26 Abs. 7 DSG 2000 als erledigt gelten könne (Ablauf der Viermonatsfrist bzw. Beendigung eines all-fälligen Beschwerdeverfahrens vor der Datenschutzkommission).

Diesen Bescheid hat der Beschwerdeführer inzwischen gemäß Art 131 Abs. 1 und 144 Abs. 1 B-VG mit parallelen Beschwerden bei beiden Höchstgerichten des Öffentlichen Rechts (VfGH Zl. B 423/08, VwGH Zl. 2008/17/0080) angefochten.

Direktlink (RIS-Volltext): [GZ: K121.327/0002-DSK/2008](#) (RIS-neu, Format PDF)

## 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. OGH Urteil und Beschluss AZ: 6 Ob 6/06k vom 28. 3. 2007

**Unterlassungsanspruch des Eigentümers gegen eine von einem Nachbarn auf sein Grundstück gerichtete Kameraattrappe; § 16 ABGB berechtigt nicht nur zur Abwehr tatsächlicher Überwachung sondern auch zum Schutz der Privatsphäre (Geheimsphäre) gegen die Schaffung des Eindrucks ständiger Überwachung** (Teil-Folgegebung) § 16 ABGB ist nicht bloß Programmsatz, sondern Zentralnorm unserer Rechtsordnung, mit normativem subjektive Rechte gewährenden Inhalt. Sie anerkennt die Persönlichkeit als Grundwert. Aus ihr wird - ebenso wie aus anderen durch die Rechtsordnung geschützten Grundwerten (Art 8 EMRK, § 1 DSG 2000, § 77 UrhG u.a.) - das jedermann angeborene Persönlichkeitsrecht auf Achtung seines Privatbereiches und seiner Geheimsphäre abgeleitet. Entscheidend für den jeweiligen Schutz ist eine Güterabwägung und Interessenabwägung. Musste sich der Kläger immer kontrolliert fühlen, wenn er sein Haus betritt oder verlässt oder sich in seinem Garten aufhält, so bewirkten die mit Einverständnis des Beklagten getroffenen Maßnahmen, selbst wenn das Gerät nur eine Attrappe einer Videokamera gewesen sein sollte, eine schwerwiegende Beeinträchtigung der Privatsphäre (Geheimsphäre) des Klägers. Da dem Beklagten die Überwachung oder die Schaffung des

Eindrucks der Überwachung des eigenen Grundstücks erlaubt ist, kann er nicht zur begehrten Entfernung der Videokamera bzw Videokameras vortäuschender Attrappen verurteilt werden. Wohl aber kommt die Verpflichtung des Beklagten zur Änderung der Einstellung der Kamera oder der Attrappe in Betracht (veröffentlicht in ÖJZ-LS 2007/52 = MR 2007,127 = Zak 2007/382 S 216 – Zak 2007,216 = RdW 2007/548 S 528 - RdW 2007,528).

Direktlink (RIS-Volltext): [AZ: 6 Ob 6/06k](#) (RIS-neu, Format PDF)

---

## 2. LG ZRS Wien, Urteil und Beschluss vom 31. 3. 2008, GZ: 55 Cg 63107z-13

**Datenanwendung einer Wirtschaftsauskunftei zur Erteilung von Bonitätsauskünften ist „öffentlich zugängliche Datei“ iSv § 28 Abs. 2 DSG 2000, Daten eines Betroffenen sind nach Widerspruch zu löschen, DSK zur Nebenintervention berechtigt** (Stattgebung, Zulassung der NI) Die DSK hatte am 27. April 2007 zu GZ: K211.797/0004-DSK/2007 beschlossen, als Nebenintervenientin (§ 32 Abs. 6 DSG 2000) einem bereits anhängigen Rechtsstreit (Löschungsklage) vor dem Landesgericht für Zivilrechtssachen Wien (LG ZRS Wien) auf Seiten des Klägers beizutreten. Der Kläger hatte gegenüber dem Inhaber einer Wirtschaftsauskunftei (§ 151 GewO 1994) gemäß § 28 Abs. 2 DSG 2000 Widerspruch gegen die Verwendung seiner Daten erhoben. Der Widerspruch war vom Beklagten abgelehnt worden war. Der Beklagte bestritt u.a. die Zulässigkeit der Nebenintervention der DSK, die Wirksamkeit des behaupteten Widerspruchs sowie die öffentliche Zugänglichkeit der von ihm verarbeiteten Klägerdaten und regte u.a. an, verschiedene Fragen durch ein Vorabentscheidungsverfahren des EuGH (Artikel 234 EGV) klären zu lassen. Im Verlauf des Prozesses nahm er jedoch die Löschung der strittigen Daten vor, worauf das Klagebegehren auf die Kosten des Verfahrens eingeschränkt wurde. Durch die rechtskräftig gewordenen Entscheidung des LG ZRS Wien wurde der Klage stattgegeben und die Nebenintervention der DSK zugelassen. Gegen eine nicht gesetzlich angeordnete Aufnahme in eine öffentlich zugängliche Datei könne der Betroffene je-derzeit auch ohne Begründung seines Begehrens Widerspruch erheben. Auch wenn der Zugang zu den Daten nur gegen Entrichtung eines Entgeltes möglich ist, so stehe dieser doch einem unbeschränkten Personenkreis zur Verfügung und sei damit ein öffentlicher (Hinweis auf die Empfehlung der DSK vom 29. November 2005, [GZ: K211.593/OO11-DSK/2005](#)) Der Beklagte führe in seiner öffentlich zugänglichen Datei die Exekutions- und Insolvenzdaten des Klägers, deren Aufnahme in diese nicht aufgrund einer gesetzlichen Anordnung erfolgt sei. Da der Kläger einen Widerspruch nach § 28 DSG 2000 erhoben habe, hätte der Beklagte innerhalb von acht Wochen die den Kläger betreffenden Daten löschen müssen. Für die Wirksamkeit des Widerspruchs sei nach § 28 Abs. 2 DSG 2000 weder eine Begründung noch die Legitimation durch einen Personalausweis erforderlich. Der den Widerspruch Erhebende hat nur durch Angaben zu seiner Identität ausreichend darzulegen, der Betroffene zu sein. Durch die Angabe von Name, Adresse, Geburtsdatum und seiner Unterschrift im erfolgten Widerspruch bzw. in der Vollmachtserklärung sei eine ausreichende Identifikation des Klägers erfolgt.

**Letzte Meldung:** In einer sachverhältnismäßig sehr ähnlichen Zivilprozesssache hat das Oberlandesgericht Wien (OLG Wien) laut einer [Pressemitteilung des Bundesministers für Soziales und Konsumentenschutz](#) und weiteren Medienberichten inzwi-

schen ein Berufungsurteil gefällt, das die dargestellte Auslegung von § 28 Abs. 2 DSG 2000 bestätigen dürfte (OLG Wien, AZ: 13 R 44/08y).

Direktlink (RIS-Volltext DSK): [Zl:K211.797](#) (Dokumentation der NI, RIS-alt)

---

### **3. Deutsches Bundesverfassungsgericht Urteil AZ: 1 BvR 2074/05 u.a. vom 11. März 2008**

#### **Hessische und schleswig-holsteinische Vorschriften zur automatisierten Erfassung von Kfz-Kennzeichen nichtig**

1. Eine automatisierte Erfassung von Kraftfahrzeugkennzeichen zwecks Abgleichs mit dem Fahndungsbestand greift dann, wenn der Abgleich nicht unverzüglich erfolgt und das Kennzeichen nicht ohne weitere Auswertung sofort und spurlos gelöscht wird, in den Schutzbereich des Grundrechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) ein.
2. Die verfassungsrechtlichen Anforderungen an die Ermächtigungsgrundlage richten sich nach dem Gewicht der Beeinträchtigung, das insbesondere von der Art der erfassten Informationen, dem Anlass und den Umständen ihrer Erhebung, dem betroffenen Personenkreis und der Art der Verwertung der Daten beeinflusst wird.
3. Die bloße Benennung des Zwecks, das Kraftfahrzeugkennzeichen mit einem gesetzlich nicht näher definierten Fahndungsbestand abzugleichen, genügt den Anforderungen an die Normenbestimmtheit nicht.
4. Die automatisierte Erfassung von Kraftfahrzeugkennzeichen darf nicht anlasslos erfolgen oder flächendeckend durchgeführt werden. Der Grundsatz der Verhältnismäßigkeit im engeren Sinne ist im Übrigen nicht gewahrt, wenn die gesetzliche Ermächtigung die automatisierte Erfassung und Auswertung von Kraftfahrzeugkennzeichen ermöglicht, ohne dass konkrete Gefahrenlagen oder allgemein gesteigerte Risiken von Rechtsgutgefährdungen oder -verletzungen einen Anlass zur Einrichtung der Kennzeichenerfassung geben. Die stichprobenhafte Durchführung einer solchen Maßnahme kann gegebenenfalls zu Eingriffen von lediglich geringerer Intensität zulässig sein.

Quelle: Deutsches Bundesverfassungsgericht, Leitsätze

Direktlink (BVerfG-Website, Volltext + Leitsätze): [1 BvR 2074/05](#)

---

### **4. Deutsches Bundesverfassungsgericht Beschluss AZ: 1 BvR 256/08 vom 11. März 2008**

**Eilantrag in Sachen "Vorratsdatenspeicherung" teilweise erfolgreich** Der Antrag der Beschwerdeführer, §§ 113a, 113b TKG im Wege der einstweiligen Anordnung bis zur Entscheidung über die Verfassungsbeschwerde außer Kraft zu setzen, hatte teilweise Erfolg. Der Erste Senat des Bundesverfassungsgerichts ließ die Anwendung von § 113b TKG, soweit er die Verwendung der gespeicherten Daten zum Zweck der Strafverfolgung regelt, bis zur Entscheidung in der Hauptsache nur modifiziert zu. Aufgrund eines Abrufersuchens einer Strafverfolgungsbehörde hat der Anbieter von

Telekommunikationsdiensten die verlangten Daten zwar zu erheben und zu speichern. Sie sind jedoch nur dann an die Strafverfolgungsbehörde zu übermitteln, wenn Gegenstand des Ermittlungsverfahrens eine schwere Straftat im Sinne des § 100a Abs. 2 StPO ist, die auch im Einzelfall schwer wiegt, der Verdacht durch bestimmte Tatsachen begründet ist und die Erforschung des Sachverhalts auf andere Weise wesentlich erschwert oder aussichtslos wäre (§ 100a Abs. 1 StPO). In den übrigen Fällen ist von einer Übermittlung der Daten einstweilen abzusehen. Zugleich wurde der Bundesregierung aufgegeben, dem Bundesverfassungsgericht zum 1. September 2008 über die praktischen Auswirkungen der Datenspeicherungen und der vorliegenden einstweiligen Anordnung zu berichten. Im Übrigen lehnte der Erste Senat den Antrag auf Erlass einer einstweiligen Anordnung ab; insbesondere lehnte er die Aussetzung des Vollzugs von § 113a TKG, der allein die Speicherungspflicht für Daten regelt, ab.

Quelle: Deutsches Bundesverfassungsgericht - [Pressemitteilung Nr. 37/2008](#) vom 19. März 2008 (Auszüge)

Direktlink (BVerfG-Website, Volltext): [1 BvR 256/08](#)

---

## C – Sonstiges

### 1. Relaunch des Internet-Auftritts der DSK

Wer ab und zu einen Blick auf die Website der DSK wirft, wird die entsprechende „[Baustellenankündigung](#)“ kaum übersehen haben: Derzeit wird an einer Erneuerung der DSK-Websites gearbeitet. Die bewährten Inhalte bleiben, dennoch wird es einige Neuerungen geben. Die drei gesetzlichen Aufgabenbereiche der Datenschutzkommission, Rechtsschutz (Beschwerde-, Genehmigungs- und Kontrollinstanz), Datenverarbeitungsregister (DVR-Meldeverfahren) und Stammzahlenregister (E-Government) werden der Gliederung des Webauftritts zu Grunde gelegt und erhalten eigene, farblich akzentuierte Websites. Allgemeine Einstiegseite für Datenschutzkommission und Datenverarbeitungsregister und damit Homepage bleibt die URL <http://www.dsk.gv.at/>. Einen Vorgeschmack auf die zukünftige optische Gestaltung (Layout) gibt der Auftritt der DSK als Stammzahlenregisterbehörde <http://www.stammzahlenregister.gv.at/>. Die Websites werden in Zukunft mit Hilfe eines neuen Content-Management-Systems (CMS) inhaltlich gestaltet.

### 2. DSK im Rechtsinformationssystem des Bundes

Inzwischen ist es gelungen, die meisten Probleme der Entscheidungsdokumentation der DSK im Rechtsinformationssystem des Bundes zu beheben. Seit Ende Mai 2008 sollten auch die Datenbestände (gezählt nach Volltexten und Rechtssätzen) von RIS-alt und RIS-neu identisch sein und die Updates synchron verlaufen. Dementsprechend wurde in dieser Ausgabe der DSK-Datenpost vermehrt mit dem Setzen von Direktlinks auf PDF-Volltextdokumente des RIS-neu begonnen.

DSK-Entscheidungsdokumentation: <http://www.ris2.bka.gv.at/Dsk/> (RIS-neu)  
<http://ris.bka.gv.at/dsk/> (RIS-alt)

---

### 3. Stellungnahme der DSK zum Entwurf einer Novelle des DSG 2000

Im am 21. Mai 2008 offiziell beendeten vorparlamentarischen Begutachtungsverfahren hat die DSK am 16. Mai 2008 zum derzeit vorliegenden Ministerialentwurf eine umfassende Stellungnahme abgegeben. Insgesamt sind rund achtzig Stellungnahmen öffentlicher und privater Personen und Institutionen zu diesem Entwurf bekannt geworden.

Direktlink (DSK-Website): [GZ: K054.016/0002-DSK/2008](#) (Format PDF)

Direktlink (Parlamentswebsite): [182/ME \(XXIII. GP\) Datenschutzgesetz-Novelle 2008](#)

---

Impressum: Medieninhaber, Herausgeber und Redaktion: Datenschutzkommission (DSK, Bundesbehörde gemäß §§ 35ff DSG 2000), Ballhausplatz 1, 1014 Wien.

Kontakt: [dsk@dsk.gv.at](mailto:dsk@dsk.gv.at)

Website: <http://www.dsk.gv.at>

RIS-Entscheidungsdokumentation der DSK: [DSK im RIS-neu](#)  
<http://ris.bka.gv.at/dsk/> (RIS-alt)

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](mailto: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.