



- Datenpost

Newsletter der österreichischen Datenschutzkommission (DSK)

Nr. 4/Juli 2007 (Versand: 23. Juli 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: K121.259/0013-DSK/2007 vom 23.5.2007

Auskunftsrecht, EDV-Personalverwaltung, E-Mail- und Internet-Log-Files, Zutrittskontrollsysteme (Stattgebung, teilweise Zurück- und Abweisung) Der Beschwerdeführer arbeitet in einem öffentlich-rechtlichen Dienstverhältnis für eine Dienststelle des Bundesministeriums für Finanzen (BMF, Beschwerdegegner). Er richtete ein umfangreiches Auskunftsbegehren an das BMF als datenschutzrechtlichen Auftraggeber. Ihm wurde teilweise schriftliche Auskunft erteilt, teilweise Einsichtnahme gewährt und Ausdrücke (Screenshots) übergeben. Die Beschwerde rügte die Auskünfte als inhaltlich mangelhaft, insbesondere unvollständig.

Die DSK wies auf Leistungsaufträge bzw. faktisches Tätigwerden der DSK sowie auf die Feststellung bereits beseitigter Rechtsverletzungen gerichtete Anträge als unzulässig zurück. Sie stellte fest, dass Log-Files von Internet-Verbindungen (Webzugang) hier personenbezogene Daten sind, da der Auftraggeber parallel zur Aufzeichnung der Verkehrsdaten pro Endgerät (Log-Files) auch Aufzeichnungen führte, welches Gerät wann von welchem User benutzt wurde (Log-in-Files). Den Einwand des Beschwerdegegners, es handle sich hier um sequenziell gespeicherte Protokolldaten gemäß § 14 DSGVO 2000, die nicht dem Auskunftsrecht unterlägen, verwarf die DSK. Zum einen handle es sich hier nicht um Protokolldaten mit dem Zweck, unberechtigte Zugriffe auf Datenanwendungen des Beschwerdegegners zu vermeiden, da im Beschwerdefall Zugriffe auf nicht dem Auftraggeber zuzurechnenden Datenanwendungen (Websites) protokolliert würden. Zum anderen wäre ein kategorischer Ausschluss des Auskunftsrechts bei Protokolldaten grundrechtswidrig. Der Gesetzgeber habe mit der Bezugnahme auf sequenziell gespeicherte Protokolldaten nur das Vermeiden unverhältnismäßigen Suchaufwands beim Auftraggeber beabsichtigt. Der Beschwerdegegner müsse daher – vorbehaltlich von Ausschlussgründen nach § 26 Abs 2 DSGVO 2000 - in derselben Weise und unter Nutzung derselben (technischen) Suchinstrumente über Protokolldaten Auskunft erteilen, in der er selbst eine Suche zu den von angestrebten Zwecken (z.B. Überprüfung auf strafrechtswidrige Internetnutzung) durchführen würde. Dies gelte neben dem Internetzugang auch für das beim Beschwerdegegner betriebene Zutrittskontrollsystem.

Hinsichtlich jenes Teils des Auskunftsbegehrens, das auf Auskunft über den eigenen E-Mail-Account auf EDV-Anlagen des Dienstgebers (gespeicherte E-Mails,

gesendete wie empfangene) abzielte, befand die DSK, dass, unter Berücksichtigung des Rechtsschutzinteresses des Betroffenen, eine Auskunft über Inhalte, die der Betroffene (dem hier überdies eine auftraggeberähnliche Stellung zu komme) selbst einsehen könne, den Auftraggeber unverhältnismäßig beansprucht und durch § 26 Abs 8 DSGVO 2000 begrenzt ist. Dies gelte aber nicht für Fragen danach, wer auf Daten des (dienstlichen) E-Mail-Accounts zugegriffen hat. Die Verweigerung dieser Auskunft hat daher das Auskunftsrecht des Beschwerdeführers verletzt.

Hinsichtlich der Daten einer organisationsinternen Terminverwaltung war von Einsehbarkeit für den Betroffenen und dienstlicher „Quasi-Öffentlichkeit“ der Daten auszugehen. Daher können bei dieser Form der Datenverwendung Mitarbeiter und Vorgesetzte nicht als „Übermittlungsempfänger“ gelten. Eine Auskunft über die Terminverwaltungsdaten wurde daher zu Recht abgelehnt.

Hinsichtlich des automationsunterstützten Personalverwaltungssystems bestritt der Beschwerdeführer, einer Einschaunahme samt mündlicher Erläuterung an Stelle der schriftlichen Auskunftserteilung zugestimmt zu haben. Für die DSK stand allerdings fest, dass der Beschwerdeführer die ihm gebotene Möglichkeit der Einschaunahme und Erläuterung (sowie der Entgegennahme ausgedruckter Screenshots mit den aufgefundenen Daten) genützt und erst wieder im Beschwerdeverfahren vor der DSK auf schriftlicher Auskunftserteilung bestanden hat. In ersterem liege eine konkludente Zustimmung, sodass der Beschwerdegegner schon mit Gewährung der Einsichtnahme der Auskunftspflicht grundsätzlich nachgekommen ist. Der Auftraggeber ist aber diesfalls zu nachträglichen Erklärungen bei nach objektivem Verständnis erkennbaren Unklarheiten verpflichtet. Dies sei hier nicht vollständig erfolgt, der Beschwerdegegner hätte auch Felder einer Datenbank, bei denen ein personenbezogener Informationsgehalt nicht ausgeschlossen werden kann (Eintrag „0“) entsprechend beauskunften müssen.

Direktlink (RIS-Volltext): [GZ: K121.259/0013-DSK/2007](#)

2. Empfehlung GZ: K211.773/0009-DSK/2007 vom 4. Mai 2007

Datenaustausch Inkassoinstitut - Kreditauskunftei (Empfehlung) Der Adressat der Empfehlung, ein Inkassoinstitut, hatte die Daten (insbesondere die volle Höhe der einzubringenden Forderung) eines säumigen Zahlers (Einschreiter) an eine Kreditauskunftei übermittelt, obwohl der Einschreiter nach Mahnung die Forderung ohne Einschränkung anerkannt und sofort eine Teilzahlung geleistet hatte. Das Inkassoinstitut hatte in seinem Mahnschreiben – entgegen § 118 Abs 2 GewO (Verbot der Inkassoession) – behauptet, der Mandant habe ihm die Forderung abgetreten. Das Ermittlungsverfahren hatte überdies ergeben, dass das Inkassoinstitut, eine Gesellschaft m.b.H., die DVR-Nummer einer mit ihm in keinem gesellschaftsrechtlichen Verhältnis stehenden Einzelperson für eine bereits 1980 gemeldet und nie aktualisierte Datenanwendung „Rechnungswesen (Buchführung, Bilanz)“ führte.

Die DSK hielt fest, dass eine Gewerbeberechtigung nach § 152 GewO (Auskunftei über Kreditverhältnisse) grundsätzlich ein in bestimmten Fallkategorien die Betroffeneninteressen überwiegendes berechtigtes Interesse am Verwenden von einschlägigen Daten begründet. Dies gelte sowohl für den Gewerbetreibenden als auch für seine Kunden und die „Datenlieferanten“. Da aber Datenanwendungen, die der Auskunftserteilung über die Kreditwürdigkeit dienen, gemäß § 18 Abs 2 Z 3 DSGVO 2000 zu den vorabkontrollpflichtigen Datenanwendungen zählen, sind allen beteiligten Auftraggebern bei Verwendung dieser Daten besondere Sorgfaltspflichten aufer-

legt. Schon vor Übermittlung von Daten an eine Kreditauskunftei bzw. vor Verarbeitung der Daten durch eine solche, muss die Aussagekraft der Daten im Hinblick auf die Bonität des Betroffenen überprüft werden. So muss überprüft werden, ob der Schuldner nicht doch zahlungsfähig oder zahlungswillig ist und war, etwa weil der Einziehungsauftrag an das Inkassoinstitut auf einen Fehler beim Mandanten zurückgeht (Mahnungen an die falsche Adresse u.dgl.m.). Werden gegenüber dem Inkassoinstitut keine nennenswerten Zahlungsschwierigkeiten offenbar, so ist die bloße Tatsache der „Übergabe ins Inkasso“ im Hinblick auf deren beschränkte Aussagekraft nicht genug, um eine überwiegendes berechtigtes Interesse an der Übermittlung von Daten an eine Kreditauskunftei zu begründen. Überdies hätte nur der im Übermittlungszeitpunkt noch offene Betrag übermittelt werden dürfen. Der Einschreiter wurde daher in seinem Recht auf Geheimhaltung verletzt.

Aus § 24 DSGVO 2000 folgt überdies, dass sich das Inkassobüro in Mahnschreiben nicht auf eine nach § 118 GewO unzulässige Inkassoession berufen darf, und der Betroffene über die Voraussetzungen einer Datenweitergabe an Dritte zu informieren ist. Neben der Unterlassung gleichartiger Übermittlungen und der Verbesserung der Mahn- und Informationsschreiben, empfahl die DSK auch eine schleunige Behebung der festgestellten Verletzungen der Meldepflicht.

Direktlink (RIS-Volltext): [GZ: K211.773/0009-DSK/2007](#)

Direktlink (RIS-Rechtssatz): [GZ: K211.773/0009-DSK/2007 – RS1](#)

Direktlink (RIS-Rechtssatz): [GZ: K211.773/0009-DSK/2007 – RS2](#)

Direktlink (RIS-Rechtssatz): [GZ: K211.773/0009-DSK/2007 – RS3](#)

Direktlink (RIS-Rechtssatz): [GZ: K211.773/0009-DSK/2007 – RS4](#)

Direktlink (RIS-Rechtssatz): [GZ: K211.773/0009-DSK/2007 – RS5](#)

B – sonstige 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. VfGH Erkenntnis Zlen G 147, 148/06 u.a. vom 15. Juni 2007

Zulässigkeit der straßenpolizeilichen Geschwindigkeitsüberwachung durch „Section Control“ (Nicht-Aufhebung von § 100 Abs. 5b StVO in einem amtswegig eingeleiteten Gesetzesprüfungsverfahren) „Section Control“ als Überwachung der Einhaltung straßenpolizeilicher Geschwindigkeitsbeschränkungen durch automationsunterstützte Datenverarbeitung (Messung der Zeit, in der ein Kraftfahrzeug eine bestimmte Wegstrecke zurücklegt, Errechnung der Durchschnittsgeschwindigkeit und Verarbeitung von Bilddaten [Kfz-Kennzeichen] aller Kraftfahrzeuge, die die Messstrecke passieren) wurde vom VfGH grundsätzlich als mit dem Grundrecht auf Datenschutz für vereinbar befunden.

Die gesetzlichen Grundlagen sind nicht verfassungswidrig aber im Lichte des Grundrechts auf Datenschutz verfassungskonform, d.h. einschränkend zu interpretieren. Entgegen den Annahmen des VfGH in seinem Prüfungsbeschluss vom 26. Juni 2006 bedarf es dazu keiner spezialgesetzlichen Regelung. Die einfachgesetzlichen Regelungen des DSGVO 2000 (insbesondere §§ 6 Abs.1 Z.2 und 5, 7 Abs.1 und 27 Abs.1 Z.1) sind im Zusammenhang mit der StVO ausreichend, um die näheren Gren-

zen der rechtlichen Ermächtigung zur Ermittlung und Verwendung (sowie die Verpflichtung zur Löschung) von mittels eines automationsunterstützten Geschwindigkeitsmesssystems gewonnenen Daten zu ziehen.

Geboten ist insbesondere die Herstellung der notwendigen Publizität der Überwachung. Dazu ist die überwachte Strecke (auf Autobahnen) durch Verordnung des für Verkehr zuständigen Bundesministers (gestützt auf § 94 Z.2 StVO) genau festzulegen. Eine solche Verordnung hat sich auf eine „aktenmäßig gehörig belegte Feststellung“ für die Notwendigkeit des Grundrechtseingriffs (z.B. wegen einer Gefahrenstelle [Tunnel, Baustelle] oder einer Unfallhäufungsstrecke) zu stützen. Die Datenerhebung ist weiters auch an Ort und Stelle entsprechend anzukündigen.

Bei Durchführung der „Section Control“ ermittelte Daten sind streng nach dem Grundsatz der Notwendigkeit und der Zweckbindung zu verwenden. Bild- und Messdaten, die zu keinem Verdacht einer Verwaltungsübertretung führen, sind unverzüglich zu löschen, andere Daten dürfen nur für den Zweck eines einzuleitenden Verwaltungsstrafverfahrens verwendet werden. Die Vorsorge für entsprechende Vorkehrungen zur Datenlöschung sind dem Auftraggeber bereits bei der Gestaltung des Systems zur Pflicht gemacht.

Als ausdrücklich unzulässig auf Grundlage der angewendeten Gesetzesbestimmungen (insbesondere § 100 Abs.5b StVO) bezeichnet der VfGH „eine durchgehende Überwachung sämtlicher Wegstrecken im Bundesgebiet“ (Unterstreichung nicht im Originalzitat). Da die bisherigen Überwachungsstrecken (Anlassfall: Wien, A 22, Kaisermühltunnel) diesen Anforderungen nicht entsprechen (Fehlen entsprechender Verordnungen), wurden in den parallelen Bescheidbeschwerdeverfahren die Straferkenntnisse in den Anlassfällen aufgehoben.

Direktlink (PDF-Dokument von VfGH-Website): [G 147/06](#)

2. VwGH Erkenntnis, Zlen. 2001/12/0004, 0008-16 vom 6. Juni 2007

DSK-Beschwerde wegen Löschung ohne vorheriges Löschungsbegehren an Auftraggeber unzulässig (teilweise Stattgebung, teilweise Ab- bzw. Zurückweisung)
Der VwGH hat mit diesem Erkenntnis den Bescheid der DSK vom 9. März 2000, GZ: 120.672/28-DSK/00, im Spruchpunkt 1. aufgehoben.

Der Beschwerdeführer hatte im Jahr 1999 ein Auskunftsbegehren an das Bundesministerium für Inneres (BMI) gestellt. Er behauptete darin, im Zuge der Ermittlungen nach dem Urheber der berüchtigten Serie von Brief- und Rohrbombenanschlägen, wiewohl völlig unschuldig, ins Visier der „Staatspolizei“ (damalige Gruppe II/C im BMI) geraten zu sein. Er sei Ziel von Lausch- und Spähangriffen sowie Hausdurchsuchungen geworden. Er verlangte nun Auskunft über die dabei ermittelten und verarbeiteten, ihn betreffenden Daten. Die erteilte Auskunft des BMI betrachtete er als unzureichend und erhob Beschwerde an die DSK.

Während des Verfahrens erhob er ergänzend Beschwerde wegen Verletzung des Rechts auf Löschung seiner Daten, ohne jedoch ein entsprechendes Löschungsbegehren nachzuweisen. Die DSK wies die Beschwerde in beiden Punkten (1. Auskunft, 2. Löschung) ab.

Das Höchstgericht gab der dagegen erhobenen VwGH-Beschwerde hinsichtlich der möglichen Verletzung des Auskunftsrechts statt, da die DSK wegen unrichtiger Auslegung des Gesetzes eine nähere Überprüfung der Richtigkeit (Vollständigkeit) der Auskunft des BMI unterlassen habe („sekundärer Verfahrensmangel“ des DSK-Verfahrens).

Hinsichtlich der abweisenden Entscheidung über das geltend gemachte Lösungsrecht bestätigte der VwGH jedoch den DSK-Bescheid. Er führte aus, dass eine Verletzung im subjektiven Recht auf Löschung erst eintreten kann, wenn der Betroffene sich mit einem Lösungsbegehren an den datenschutzrechtlichen Auftraggeber gewandt hat, und dieses abgelehnt worden ist (§ 27 Abs.1 Z.2 und Abs.4 DSGVO 2000). Eine nicht erfolgte amtswegige Löschung (§ 27 Abs.1 Z.1 DSGVO 2000) stelle dagegen bloß eine Pflichtenverletzung des Auftraggebers dar. Eine Beschwerde an die DSK wegen Verletzung im Recht auf Löschung ohne Nachweis eines vorherigen Lösungsbegehrens ist damit formal unzulässig und kann von der DSK zurückgewiesen werden.

Direktlink (RIS-Volltext): [Zl. 2001/12/0004](#) (RIS-Auswertung in Arbeit!)

C – Sonstiges

1. Stellungnahme der Artikel 29-Arbeitsgruppe zur Frage des gemeinschaftsrechtlichen Begriffs der personenbezogenen Daten Das Organ der europäischen Datenschutzbehörden hat eine gemeinsame Auslegung des Datenbegriffs der Richtlinie 95/46/EG beschlossen und veröffentlicht („Opinion 4/2007 on the concept of personal data“ vom 20. Juni 2007). Diese ist nicht bindend, bietet aber in einer sorgfältigen und umfassenden Analyse wichtige Hinweise zur Bedeutung dieses für die Anwendung des Datenschutzrechts grundlegenden Begriffs. Derzeit liegt das Dokument nur in englischer Sprache vor; Übersetzungen in andere Sprachen werden vorbereitet.

Direktlink (PDF-Dokument von Website der Artikel 29-Arbeitsgruppe): [Opinion 4/2007](#)

2. Corrigendum: In DSK-Datenpost 3/2007, B 1., war in der Überschrift durch ein Redaktionsversehen vom „Widerruf“ die Rede. Richtig müsste es entsprechend § 28 DSGVO 2000 wie auch im Text der Meldung „Widerspruch“ heißen.

Impressum: Medieninhaber, Herausgeber und Redaktion: Datenschutzkommission (DSK, Bundesbehörde gemäß §§ 35ff DSGVO 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 DSGVO 2000), sonstige Tätigkeit der DSK und datenschutzrechtliche Fragen.

Der Bezug ist kostenlos.

An-/Abmeldung: E-Mail an dsk@dsk.gv.at

Information gemäß § 24 DSGVO 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.