Datenpanne in der Justiz – Schlaglicht auf den Sonderdatenschutz in der Gerichtsbarkeit*

Ein jüngst vom Höchstgericht[1] entschiedener Fall um die „unfreiwillige" Veröffentlichung von hunderten Verfahrensdaten aus sog. Anlegerschadensprozessen beim LG Wiener Neustadt rückt den Sonderdatenschutz für die Gerichtsbarkeit nach den §§ 83 ff GOG in den juristischen Fokus. Der folgende Beitrag erläutert die Entwicklung dieses Rechtsbereiches und nimmt eine erste Standortbestimmung vor.

Deskriptoren: Grundrecht auf Datenschutz, Geheimhaltung, Veröffentlichung, Gerichtsbarkeit, Bestimmtheitsgebot.
Normen: § 1 DSG 2000, § 8 Abs 1 Z 3 DSG 2000, § 24 Abs 2a DSG 2000, § 33 DSG 2000, § 24 StPO, § 83 GOG, § 85 GOG.

Von Clemens Thiele

1. Die Datenpanne

Anfang März 2013 passierte eine Datenpanne am LG Wiener Neustadt. Zum damaligen Zeitpunkt klagten mehrere hundert geschädigte Anleger die Unternehmen der Auer von Welspach (AvW)-Gruppe auf Schadenersatz wegen der seinerzeit erworbenen Genussscheine. Der spätere Zweitantragsteller, Anlegeranwalt Dr. Michael Bauer, vertrat mit seinem Kollegen RA Dr. Erich Holzinger rund 900 Geschädigte mit etwa 32 Sammelklagen gegen die Ex-AvW-Wirtschaftsprüfer Moore Stephens Ehrenböck mit Sitz in Gloggnitz. Die spätere Erstantragstellerin, eine Klientin der Anlegeranwälte, rief beim Zweitantragsteller an und fragte, warum sie, wenn sie im Internet ihren Namen in die Google-Suchmaschine eintippte, in einer Klage am Gericht in Wiener Neustadt – ohne jegliche Anonymisierung – aufschien.
Nach ersten Recherchen handelte es sich um eine „private Schatten-Website" des Gerichts: „Willkommen beim Aktenverwaltungssystem für die Massenverfahren AvW vs. Wirtschaftsprüfer", hieß es auf der Seite „MSE Akten Verwaltung", die unter http://www.****5n0w.net zur besseren justiziellen Bewältigung der Massen-Anlegerschadensfälle eingerichtet worden war. Dort ersichtlich waren auf insgesamt fünf Seiten mehr als hundert Namen von Klägern aus den zu konkret genannten Geschäftszahlen beim LG Wiener Neustadt anhängigen „Sammelklagen" gelistet. Eine Google-Suchabfrage nach dem Namen der Erstantragstellerin und „******" ergab noch am 14.3.2012 ein Suchergebnis, nämlich einen Verweis auf *http://www.****5n0w.net*. Aus der Vorschau waren ihr Name und der Streitwert ihres Verfahrens von 6.189,91 EUR ersichtlich.
Am 6.3.2012 war ein mit 6.3.2012 datierter, nicht mit dem Namen eines Entscheidungsorgans versehener Beschlussentwurf des LG Wr Neustadt zum Verfahren der Antragsteller ebenfalls unter *http://www.****5n0w.net* abrufbar, wonach diverse Verfahren zur gemeinsamen Verhandlung und Entscheidung verbunden wurden. In Punkt 3. des Beschlusstenors ist der Zweitantragsteller namentlich unter Bezugnahme auf die von ihm vertretene Antragstellerin als Klägerin mit jeweiligen Streitwerten und bezughabenden Geschäftszahlen genannt.
Über Anfrage der Wiener Zeitung[2] wurde mitgeteilt, dass das Gericht unbeabsichtigt die Namen der Parteien, der Parteienvertreter, die Streitwerte und die Aktenzahl im Internet veröffentlicht hatte. Die medial breit getretene Datenpanne war auch Gegenstand einer parlamentarischen Anfrage[3] am 18.5.2012 an das Innenministerium. Das BMI wies die Anfrage jedoch mangels Zuständigkeit zurück, da es sich um eine Justizangelegenheit handelte.[4]
Die Antragsteller erhoben nach den §§ 83 ff GOG Beschwerde an das OLG Wien wegen Verletzung von durch § 1 Abs 1 DSG geschützten Geheimhaltungsinteressen durch Organe der Rechtspflege. Im durchgeführten Verfahren stellte sich folgendes heraus:

---

* Hon.-Prof. RA Dr. *Clemens Thiele*, LL.M. Tax (GGU), Anwalt. Thiele@eurolawyer.at; Näheres unter http://www.eurolawyer.at.

1 OGH 28.11.2013, 6 Ob 165/13b – *MSE Akten-Verwaltung*, EvBl-LS 2014, 322 = Jus-Extra OGH-Z 5508 = jusIT 2014/37, 73 (*Bauer*) = RdW 2014/229, 197 = JBl 2014, 401 = ZIR 2014, 317.

2 Abrufbar unter http://www.wienerzeitung.at/nachrichten/wirtschaft/oesterreich/443292_Datenleck-am-Landesgericht-Wr.-Neustadt.html (21.05.2014).

3 „Datenleck" beim Landesgericht Wiener Neustadt (11729/J), abrufbar unter http://www.parlament.gv.at/PAKT/VHG/XXIV/J/J_11729/imfname_253604.pdf (21.05.2014)

4 Abrufbar unter http://www.parlament.gv.at/PAKT/VHG/XXIV/AB/AB_11530/fnameorig_261150.html (21.5.2014).

„Ende Jänner 2012 wurde von Organen des Landesgerichts Wiener Neustadt zur Verwaltung von Verfahrens- und Sachverhaltsdaten, die über 1000 bei diesem Gericht seit Ende 2011 in mehreren Gerichtsabteilungen anhängige Klagen von 2.200 ehemaligen AvW-Genussscheininhabern betreffen, ein virtueller Server eingerichtet, der mit einem kryptografisch geschützten System (public key authentification, 1024 Bit Schlüssellänge), einem verschlüsselten Zugang und einer passwortgesicherten Weboberfläche versehen wurde. Dieses System lief zusätzlich unter einer dynamisch zugeteilten, nicht veröffentlichten IP-Adresse ohne Domainzuweisung, sodass diese Datensammlung „MSE Akten-Verwaltung" (vorerst) auch nicht von Suchmaschinen gefunden werden konnte.

*Im August 2011 war aber von Unbekannten in Denver (USA) für ein Jahr die Domain ***** registriert worden. Diese Domain verwies auf die nicht veröffentlichte IP-Adresse des Landesgerichts Wiener Neustadt, auch noch nachdem der Server zur Domain ***** außer Betrieb genommen worden war. Warum diese Domain auf die IP-Adresse des Landesgerichts Wiener Neustadt verwiesen hatte, ist nicht bekannt. Der Zugriff auf die Datensammlung des Landesgerichts Wiener Neustadt war trotz dieses fehlerhaften Verweises vorerst nicht möglich, weil die Informationen durch die getroffenen Sicherheitsmaßnahmen geschützt waren.*

*Ende Feber 2012 wurde am Server jedoch durch das Landesgericht Wiener Neustadt der Passwortschutz zeitweise zu Debuggingzwecken ausgeschaltet, um verschiedene Tests durchzuführen. Jedenfalls innerhalb dieses Zeitraums von 24. bis 27. 2. 2012 erfolgte über den Verweis der Domain ***** auf die IP-Adresse des Landesgerichts Wiener Neustadt ein erfolgreicher Zugriff auf die am Server abgelegten Informationen. Dadurch wurden die über die Domain ***** abgerufenen Informationen von der Suchmaschine Google erfasst und im Google-Cache gespeichert. Bei Eingabe der entsprechenden Parameter bzw Suchworte ab diesem Zeitpunkt waren daher - bis zur Löschung aus dem Google-Cache etwa Ende März 2012 – Informationen aus der Datensammlung über Google abrufbar. Konkret waren über die Suchmaschine Google überwiegend die Namen von Klägern und der Streitwert ihrer Klagen abrufbar. In ca 20 % der Fälle war auch die Adresse der Kläger sichtbar, bei einem kleineren Teil alternativ das Geburtsdatum.*

*Den Organen des Landesgerichts Wiener Neustadt war bei Errichtung des Servers nicht bekannt, dass die Domain ***** auf die IP-Adresse des Landesgerichts Wiener Neustadt verwies und aufgrund der genannten Umstände diese Informationen über Google abrufbar waren. Nach dem Bekanntwerden der Verbreitung von Informationen aus der Datensammlung über Google am Vormittag des 13.3.2012 haben die Organe des Landesgerichts Wiener Neustadt den Server, auf dem diese Daten gespeichert waren, abgeschaltet; gleichzeitig wurden Anträge auf Löschung der Suchergebnisse aus dem Google-Cache übermittelt. Google entsprach diesen Anträgen und löschte die Daten ca 14 Tage später aus seinem Cache."*

Die Antragsgegnerin, die Republik Österreich, wandte ein fehlendes Geheimhaltungsinteresse der Beschwerdeführer ein. Die Datensammlung und Verwendung wäre rechtmäßig, weil die Verfahrensdaten ohnehin „aufgrund der gebotenen Öffentlichkeit in Gerichtsverfahren grundsätzlich jedermann zugänglich" wären.

Das OLG Wien gab der Beschwerde statt und qualifizierte die von Organen des LG Wr Neustadt angelegte „MSE Akten-Verwaltung" als eine iS des § 5 DSG öffentliche Datenanwendung nach § 4 Z 7 DSG, die schutzwürdige Geheimhaltungsinteressen der Antragsteller verletzt hätte. Ein Verschulden wäre nicht Voraussetzung für eine Verletzung im Grundrecht auf Datenschutz.

Aufgrund des Rekurses der Antragsgegnerin hatte der OGH über diesen Sachverhalt gem § 85 GOG zu entscheiden, letztlich darüber ob die Feststellung der Datenschutzverletzung durch ein Organ der Gerichtsbarkeit in Ausübung dessen Tätigkeit nach § 83 GOG erfolgt war oder nicht.

2. Die Entscheidung des Gerichts[5]

Der OGH gab dem Rekurs nicht statt und sprach aus, dass die versehentliche Übermittlung der Daten an Google und die dadurch bestehende Möglichkeit diese Daten für einen bestimmten Zeitpunkt im Internet abzurufen, einen Eingriff in das Grundrecht der Antragsteller auf Geheimhaltung der sie betreffenden personenbezogenen Daten darstellte. Die Höchstrichter vertraten zwar die Auffassung, dass es sich zum Zeitpunkt, als die Daten vom LG Wr. Neustadt versehentlich an Google übermittelt und im Internet abrufbar gemacht wurden, bereits um faktisch allgemein verfügbare Daten gehandelt hätte. Allein durch den bis dahin möglicherweise erfolgten Aufruf der Sache und allenfalls das Aufliegen eines Verhandlungsspiegels wären die von der Beschwerde betroffenen Daten keineswegs einer Allgemeinheit in dem von § 8 Abs 2 DSG geforderten Umfang verfügbar gewesen. Die betreffenden Daten wären somit nicht allgemein verfüg-

5 OGH 28.11.2013, 6 Ob 165/13b – *MSE Akten-Verwaltung*, EvBl-LS 2014, 322 = Jus-Extra OGH-Z 5508 = jusIT 2014/37, 73 (*Bauer*) = RdW 2014/229, 197 = JBl 2014, 401 = ZIR 2014, 317.

bar gewesen, weshalb der Eingriff in das Datenschutzgrundrecht auf Geheimhaltung der die Antragsteller betreffenden personenbezogenen Daten zu bejahen war.

3. Beschwerdezuständigkeit und anwendbares Datenschutzrecht

Die vorliegende Entscheidung ist sowohl von ihrem Sachverhalt als auch in ihrer rechtlichen Begründung höchst bemerkenswert. Sie erlaubt einen – soweit ersichtlich – erstmals tiefergehenden Einblick in den Datenschutz der österreichischen Justiz.

3.1. Zuständigkeit für die Grundrechtsbeschwerde

Das **Grundrecht auf Datenschutz** (Geheimhaltung) personenbezogener Daten bezieht sich in Österreich sowohl auf die automationsunterstützt verarbeiteten, als auch auf nicht automationsunterstützten Daten.[6] Im konkreten Fall haben die Beschwerdeführer eine Verletzung des Grundrechts auf Datenschutz geltend gemacht. Die sachliche Zuständigkeit richtet sich demgemäß nach dem Auftraggeber der beanstandeten Datenverarbeitung. Die ehemalige „*Rechtswegklausel*"[7] des § 1 Abs 5 DSG[8] hatte eine Entscheidungsbefugnis der DSK zur Durchsetzung des Grundrechts in seinen durch § 1 Abs 1 und 3 DSG gewährleisteten Teilrechten vorgesehen. Ausgenommen waren aber stets solche Datenverarbeitungen, die Akte der Gerichtsbarkeit betroffen haben.

> Zur datenschutzrechtlichen Prüfung von Handlungen oder Unterlassungen, die im Dienste der Gerichtsbarkeit erfolgen (hier: versehentliche Veröffentlichung von personenbezogenen Daten auf Gerichtsservern im Internet) sind ausschließlich die ordentlichen Gerichte nach §§ 83 ff GOG zuständig.

Der **Umgang mit personenbezogenen Daten durch Österreichs Gerichte** hat bereits mehrfach Anlass zu Beschwerden gegeben:

- durch eine unvollständig anonymisierte Entscheidung des OGH und deren Veröffentlichung im RIS verletzt erachtet.[9]
- Keine Zuständigkeit der DSK zur Entscheidung über eine Beschwerde wegen mangelnder Anonymisierung einer OGH-Entscheidung im RIS; keine Auftraggebereigenschaft des Bundeskanzlers und des Justizministers.[10]
- In Zusammenhalt mit § 24 StPO ist davon auszugehen, dass das Fotografieren für den festgestellten Zweck, nämlich die Überprüfung, ob die gegen den Bf bestehende Verdachtslage, weitere Straftaten (hier: Weitergabe von Suchtgift an Jugendliche) begangen zu haben, erhärtet werden kann, zulässig gewesen ist.[11]
- Abweisung der Beschwerde mangels Betroffenheneigenschaft, weil auf dem USB-Stick, auf den sich der Beschwerdeführer in seiner Beschwerde bezieht, keine Daten des Beschwerdeführers enthalten waren.[12]
- Abweisung der Beschwerde mangels Betroffeneneigenschaft, weil auf dem USB-Stick, der Gegenstand des Strafverfahrens über den Datendiebstahl war, auf den sich der Beschwerdeführer in seiner Beschwerde bezieht, keine Daten des Beschwerdeführers enthalten waren.[13]
- Keine Gewährung eines einstweiligen Rechtsschutzes nach § 31 Abs 3 DSG 2000 gegen mögliche zukünftige Datenübermittlungen durch die Justizanstalt an ein Inkassobüro.[14]
- Keine Zuständigkeit der DSK zur Prüfung von Handlungen, die im Dienste der Gerichtsbarkeit erfolgten. Kein Verstoß gegen das Übermaßverbot durch eine Datenermittlung im Anschluss an eine Durchsuchung und Sicherstellung.[15]

Sämtliche dieser Beschwerden wurden unter Hinweis darauf, dass die DSK nach § 1 Abs 5 letzter Satz DSG aF nicht zur Überprüfung von behaupteten Datenschutzverletzungen durch Akte der ordentlichen bzw Strafgerichtsbarkeit zuständig ist, erledigt.[16]

Um die aus verfassungsrechtlichen Gründen als empfindlich wahrgenommene Rechtsschutzlücke zu schließen, hat die Zivilverfahrensnovelle 2004[17] für die Gerichtsbarkeit eine eigene justizinterne Beschwerdemöglichkeit eröffnet. Die §§ 83 ff GOG regeln den **Datenschutz in Angelegenheiten der Gerichtsbarkeit**. Als „lex

6 So bereits VfGH 2.10.1989, G 238-241/88, V 209-212/88, infas 1990/A, 116.
7 *Pollirer/Weiss/Knyrim*, DSG (2010) § 1 Anm 22.
8 Aufgehoben durch BGBl I 51/2012.
9 Vgl DSK 22.5.2001, K120.742/005-DSK/2001, nv: Das unvollständig anonymisierte Dokument war im Zeitpunkt der Beschwerdeerhebung bereits durch den OGH aus dem RIS-Inhalt entfernt worden
10 DSK 28.5.2004, K120.917/0008-DSK/2004, RIDA-Nummer: 0150991.
11 DSK 21.6.2005, K120.942/0008-DSK/2005, RIDA-Nummer: 0154320.
12 DSK 20.3.2009, K121.424/0005-DSK/2009, RIDA-Nummer: 0219912.
13 DSK 18.9.2009, K121.543/0006-DSK/2009, RIDA-Nummer: 0219431.
14 DSK 14.4.2010, K121.566/006-DSK/2010, RIDA-Nummer: 0224202.
15 DSK 7.11.2012, K121.862/0012-DSK/2012, RIDA-Nummer: 0268537.
16 Zutreffend *Jahnel*, Handbuch Datenschutzrecht (2010) Rz 2/78 mwN.
17 BGBl I 2004/128 mit Wirkung vom 1.1.2005.

fugitiva" finden sich einschlägige Rechtsschutzbestimmungen seither in den §§ 84, 85 GOG.[18]

3.2. Anwendbares Datenschutzrecht

Der justizielle „**Sonderdatenschutz**" betrifft aber lediglich die formelle Geltendmachung der Betroffenenrechte nach den §§ 27 ff DSG. Sämtliche übrigen (materiellen) Bestimmungen des DSG gelten auch für die Organe der Gerichtsbarkeit. Demnach sind die Anträge auf Auskunft, Richtigstellung oder Löschung bei jenem übergeordnetem Gericht zu stellen, das für die Datenverwendung zuständig ist bzw war; im Anlassfall also beim OLG Wien. Das Verfahren richtet sich in Zivilsachen nach dem Außerstreitgesetz. Die Entscheidung erfolgt in Beschlussform und ist durch ein ordentliches Rechtsmittel nicht anfechtbar. Eine Überprüfung ist nur im Wege des Antrags nach § 85 GOG, und dies einmalig an den OGH, möglich.[19]

> Aus § 85 Abs 1 und 2 GOG folgt, dass das Gericht nicht von Amts wegen, sondern nur aufgrund einer Beschwerde, die auf Feststellung der Rechtsverletzung gerichtet ist, zu entscheiden hat. Die Beschwerde ist in bürgerlichen Rechtssachen grundsätzlich an das im Instanzenzug übergeordnete Gericht zu richten. Prüfungsmaßstab bildet primär das Grundrecht auf Datenschutz nach § 1 Abs 1 DSG.

Für den aufmerksamen Rechtsanwender bedeutet die im Übrigen uneingeschränkte Anwendbarkeit des DSG 2000 auch im Justizbereich, dass das LG Wr Neustadt die gesetzliche Verpflichtung zur sog. „*Data Breach Notification*" nach § 24 Abs 2a DSG getroffen hat. Dadurch wurde bereits mit Wirksamkeit vom 1.1.2010[20] eine besondere Informationsverpflichtung jener Auftraggeber geschaffen, die Kenntnis von einer systematischen und schwerwiegenden unrechtmäßigen Verwendung, maW einem Datenmissbrauch, ihrer Datenbestände erlangen. Ob eine derartige Information der Betroffenen, allenfalls auch über offensive Medienarbeit, von den Justizbehörden im Anlassfall erfolgt ist, entzieht sich der Kenntnis des Verfassers. Dass ein Fall des § 24 Abs 2a DSG vorgelegen ist, liegt aber mE auf der Hand.[21]

4. Verletzung des Grundrechts auf Geheimhaltung personenbezogener Daten in der Justiz (§ 85 GOG)

4.1. Akt der Gerichtsbarkeit

Wer durch ein Organ der Gerichtsbarkeit in Ausübung dessen Tätigkeit in seinen in § 83 GOG bezeichneten Rechten verletzt wurde, kann dem Bund gegenüber die Feststellung dieser Verletzung begehren. § 83 GOG verweist wiederum auf die im DSG 2000 geregelten Betroffenenrechte. Dazu gehört ua auch das Grundrecht auf Datenschutz gem § 1 DSG, welches aus mehreren, unterschiedlichen (Grund-)Rechten besteht:

- das „zentrale" Grundrecht auf Geheimhaltung personenbezogener Daten (§ 1 Abs 1 DSG);
- das Recht auf Auskunft (§ 1 Abs 3 Z 1 DSG);
- das Recht auf Richtigstellung unrichtiger Daten (§ 1 Abs 3 Z 2 erster Fall DSG);
- das Recht auf Löschung unzulässiger Weise verarbeiteter Daten (§ 1 Abs 3 Z 2 zweiter Fall DSG).

Rückgrat des Datenschutzrechts in der Justiz bildet das Grundrecht auf Datenschutz, das einen verantwortungsvollen Umgang mit den personenbezogenen Angaben der Betroffenen, maW der Privatheit der Menschen, einfordert. Staatliche Stellen, so auch Gerichte, dürfen in dieses Grundrecht allein aufgrund einer gesetzlichen Grundlage eingreifen.

§ 85 Abs 1 GOG erfordert einen Akt der Gerichtsbarkeit, dh ein Gericht im funktionellen Sinn. Notwendig, aber auch ausreichend ist nach der bisherigen Spruchpraxis[22] der DSK, dass die Verantwortung für eine bestimmte Datenanwendung grundsätzlich einem gerichtlichen Organ zugewiesen wird. Gemäß den Gesetzesmaterialien[23] umfasst der Begriff „Gerichtsbarkeit" auch angelagerte Hilfstätigkeiten einschließlich der Führung von Geschäftsregistern. Demnach kommt weniger der Abgrenzung zwischen der Ausübung von Hoheitsgewalt und der Privatwirtschaftsverwaltung Bedeutung zu als vielmehr der organisatorischen Zuweisung von bestimmten Agenden an ein gerichtliches (Hilfs-)Organ.

Zu beachten ist, dass zB für die Führung der öffentlichen Register wie Firmen- oder Grundbuch, eigene Datenschutzregime gelten.[24] Im Anlassfall hat ein Richter des LG Wiener Neustadt das Aktenverwaltungssystem

---

18 Dazu *Weiss/Knyrim*, Datenschutz in der Justiz, ecolex 2006, 74, 75; *Spenling*, Zivilverfahren und Datenschutz – Eine erste Orientierung zu den neuen §§ 83 bis 85 GOG, in: BMJ (Hrsg), Vorarlberger Tage (2005), 135; *Fercher*, Gerichtsbarkeit, in *Bauer/Reimer* (Hrsg), Handbuch Datenschutzrecht (2009) 181, 182 ff.

19 Vgl zu einem Anonymisierungsfall bereits *Thiele*, Entscheidungsanmerkung, jusIT 2012, 72, 73.

20 Eingefügt durch BGBl I 133/2009.

21 Statt vieler *Knyrim*, Die neue „Data Breach Notification Duty" im DSG, in Jahnel (Hrsg), Datenschutzrecht. Jahrbuch 2010 (2010), 59.

22 DSK 28.5.2004, K120.917/0008-DSK/2004, RIDA-Nummer: 0150991; 14.4.2010, K121.566/006-DSK/2010, RIDA-Nummer: 0224202; K121.862/0012-DSK/2012, RIDA-Nummer: 0268537.

23 AB zu BGBl I 165/1999

24 Vgl zum Grundbuch OGH 16.7.2013, 5 Ob 40/13p, *Grundbuchsumstellung II*, jusIT 2013/107, 225 (*Thiele*) = Zak 2013/765, 419; zum Firmenbuch OGH 20.3.2013, 6 Ob 181/12d, GES 2013, 250 (*Fantur*) = jusIT 2013/51, 107 (*Thiele*) = AnwBl 2013, 474 = wbl 2013/170, 471 = RdW 2013/399, 387 = ecolex 2013/443, 1084.

zu dienstlichen Zwecken für sich und seine mit den Massenverfahren betrauten Kollegen auf Servern des Gerichts installiert. Ein der Gerichtsbarkeit zurechenbares Organhandeln ist damit gegeben.

4.2. Verletzung des Grundrechts auf Datenschutz

4.2.1. Unzulässiger Eingriff

Der Eingriff in die grundrechtlich geschützte Position der Beschwerdeführer besteht in der Verarbeitung ihrer personenbezogenen Daten auf Webservern und deren Zurverfügungstellung im Internet,[25] wo Google sie indiziert und auffindbar gemacht hat.[26]

Damit aus einem Eingriff eine Datenschutzgrundrechtsverletzung wird, muss der Eingriff unzulässig gewesen sein. MaW die Voraussetzungen für die Zulässigkeit eines Eingriffs in das Grundrecht auf Datenschutz durch eine staatliche Behörde sind:[27]

- (1) Er muss zur Wahrung überwiegender berechtigter Interessen eines anderen erfolgen (Interessenabwägung).
- (2) Er darf nur auf Grund von Gesetzen erfolgen, die aus den m Art 8 Abs 2 EMRK genannten Gründen notwendig sind (materieller Gesetzesvorbehalt).
- (3) Der Eingriff in das Grundrecht darf jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden (gelindestes Mittel).[28]
- (4) Nach der stRsp[29] des VfGH muss ein Eingriffsgesetz zudem dem Bestimmtheitsgebot entsprechen.

Bei Eingriffen in sensible Daten müssen darüber hinaus (5) die Wichtigkeit des Eingriffstatbestandes (nur zur Wahrung wichtiger öffentlicher Interessen) nachgewiesen und (6) angemessene Garantien für den Geheimnisschutz vorgesehen werden.[30] Im Anlassfall sind – soweit ersichtlich – keine sensiblen Daten iS des § 4 Z 2 DSG veröffentlicht worden, sodass sich die folgende Prüfung auf die Zulässigkeitsgründe (1) bis (4) beschränkt.

4.2.2. Wahrung überwiegender berechtigter Interessen eines anderen

Ein Eingriff in das Grundrecht auf Datenschutz kann nach der gebotenen Interessenabwägung gerechtfertigt sein. Bei dieser sind die von der Rsp[31] zu anderen Interessenkollisionen, wie zB beim Recht auf Meinungsfreiheit nach Art 10 MRK gegenüber dem Recht auf Ehre nach § 1330 ABGB entwickelten Grundsätze anwendbar. Demzufolge kann aus der Beeinträchtigung eines absoluten Rechtes allein noch nicht auf die Rechtswidrigkeit der Handlung geschlossen werden, wenngleich in der Handlung selbst ein gewisses Indiz für das Vorliegen der Rechtswidrigkeit gelegen sein mag. Die Rechtfertigung des Grundrechtseingriffs kann nur aufgrund einer umfassenden Interessenabwägung beurteilt werden; dem Interesse am gefährdeten Gut (hier: der Privatheit des Betroffenen) müssen stets auch die Interessen des Handelnden (hier: Organ in Erfüllung dienstlicher Verpflichtungen) und die der Allgemeinheit (hier: an einer funktionierenden Justiz, die in schicklicher Frist auch in Massenverfahren Entscheidungen trifft) gegenübergestellt werden. Bei der Interessenabwägung kommt es auf folgende Zurechnungsmomente an:

- die Art des eingeschränkten Rechtes
- die Schwere des Eingriffes
- die Verhältnismäßigkeit zum verfolgten Zweck und
- den Grad der Schutzwürdigkeit dieses Interesses.

Jeder Weitergabe von nicht-sensiblen Daten (nach § 8 Abs 1 Z 3 DSG) muss eine Interessenabwägung vorangehen zwischen einem schutzwürdigen Interesse des Betroffenen und dem berechtigten Interesse eines Dritten, wobei im Zweifel die Vermutung für die Schutzwürdigkeit spricht. Als berechtigte Interessen Dritter sind dabei unter anderem auch subjektive, auf gesetzlicher oder vertraglich vereinbarter Grundlage beruhende Ansprüche anerkannt. Im konkreten Fall hat der 6. Senat zutreffend ein Überwiegen des schutzwürdiges Interesses der Betroffenen nach § 1 Abs 1 DSG bejaht.

> Das Grundrecht auf Geheimhaltung personenbezogener Daten wird dann verletzt, wenn Daten zu bei Zivilgerichten anhängigen Verfahren (hier: Anlegerschadenersatzprozesse) und deren Inhalte von Justizmitarbeitern auf einem von diesen eingerichteten virtuellen Server gespeichert werden und dem Zugriff der Internet-Suchmaschine Google ausgesetzt, in deren Cache gespeichert und über diese aus dem öffentlich zugänglichen Internet abrufbar waren.

---

25 EuGH 6.11.2003, C-101/01 – *Lindqvist*, Rz 25, EuGRZ 2003, 714 = MR 2004, 83 (*Kronegger*) = ÖJZ 2004/45, 741 (*Hörlsberger*) = ZER 2004/330, 93.

26 Vgl deutlich EuGH 13.5.2014, C-131/12 – *Google Spain ./. AEPD*, Rz 28, ZIR 2014, 204.

27 Deutlich *Jahnel*, Verfassungsrechtliche Fragen der elektronischen Gesundheitsakte (ELGA) in FS Stolzlechner (2014), 309, 313 mwN.

28 Vgl VfGH 1.10.2013, G 2/2013 – *Beweisverwertungsverbot*, jusIT 2013/106, 224 (*Jahnel*) = AnwBl 2014/8373, 134 (*Schrott*).

29 Vgl VfGH 14.3.2013, B 1326/12 – *Jugendfürsorge*, jusIT 2013/70, 152 (*Jahnel*) = JUS Vf/4879 = ZfVB 2013/1337 und VfGH 5.3.2008, B 1840/07 – *Section Control*, ZfVB 2008/1640/1674 = VfSlg 18.387;

30 Vgl *Jahnel*, Verfassungsrechtliche Fragen, 309, 313.

31 Vgl OGH 10.4.1991, 1 Ob 36/89 – *Altöl-Skandal*, JBl 1991, 796 = ÖBl 1991, 161 = SZ 64/36.

4.2.3. Allgemeine Verfügbarkeit der Daten?

§ 1 Abs 1 Satz 2 DSG schließt die Verletzung eines schutzwürdigen Geheimhaltungsinteressse der Betroffenen bei „allgemein verfügbaren Daten" ausdrücklich aus. Diese in der hL[32] bereits kritisierte Ausnahme greift der OGH auch für den justiziellen Datenschutz auf. Wohltuend deutlich erscheint höchstrichterliche Interpretation des § 1 Abs 1 zweiter Satz DSG. Dass die beiden darin genannten Fälle (allgemeine Verfügbarkeit und mangelnde Rückführbarkeit), welche nach dem Gesetz ein schutzwürdiges Interesse nach dem ersten Satz leg.cit. ausdrücklich ausschließen, die einzigen sein sollen, die ein schutzwürdiges Geheimhaltungsinteresse an personenbezogenen Daten verhindern – wie der OGH klar zum Ausdruck bringt –, erscheint im Lichte der Formulierung des Gesetzestextes zweifelhaft.
Die betreffenden Daten waren im Anlassfall nicht allgemein verfügbar. Die Tatsache, dass diese personenbezogenen Daten bereits zum Teil öffentlich zugänglich sind, bedeutet nicht, dass das Datenschutzregime dafür nicht gelten würde; im Gegenteil, die europäische Rsp[33] hat klargestellt, dass sich der Datenschutz für bereits veröffentlichte Daten grundsätzlich nicht vom Schutzumfang für sonstige personenbezogene Daten unterscheidet. Die hL[34] plädiert daher für eine richtlinienkonforme Interpretation des § 8 Abs 2 DSG, der schutzwürdige Geheimhaltungsinteressen als nicht verletzt ansieht, wenn zulässiger Weise veröffentlichte Daten verwendet werden. Im Lichte des EuGH-Urteils im *Satamedia*-Fall hat diese einfach gesetzliche Anordnung zurückzutreten. Demnach sind auch veröffentlichte personenbezogene Daten in den Anwendungsbereich der Datenschutzrichtlinie einzubeziehen. Die verfassungsrechtliche Ausnahme für veröffentlichte Daten in § 1 Abs 1 DSG hat zu entfallen.[35] Für den vorliegend zu beurteilenden Fall bedeutet dies eine uneingeschränkte Anwendung der Datenschutzrichtlinien im Wege des § 85 GOG.[36]

4.2.4. Bestimmtheitsgebot der gesetzlichen Eingriffsgrundlage

Die einen Eingriff rechtfertigende Gesetzesgrundlage muss nach st Rsp[37] des VfGH als Ermächtigungsnorm iS des § 1 Abs 2 DSG 2000 ausreichend präzise sein, also für jedermann vorhersehbar bezeichnen, unter welchen Voraussetzungen die Ermittlung bzw die Verwendung der Daten für die Wahrnehmung konkreter Verwaltungsaufgaben zulässig ist. Der jeweilige Gesetzgeber muss somit iSd § 1 Abs 2 DSG eine materienspezifische Regelung in dem Sinn vorsehen, dass die Fälle zulässiger Eingriffe in das Grundrecht auf Datenschutz konkretisiert und begrenzt werden.
Die im DSG 2000 enthaltenen einfachgesetzlichen Ausführungsvorschriften bezüglich der allgemeinen Grundsätze für die Verwendung von Daten (vgl den 2. Abschnitt des DSG 2000) reichen nach der Auffassung der Verfassungshüter für die Beschränkung des Grundrechts auf Datenschutz iS des § 1 Abs 2 DSG nicht aus.

> Allein durch den Aufruf der Sache und das Aufliegen eines „Verhandlungsspiegels" werden die Daten keineswegs einer Allgemeinheit im erforderlichen Umfang verfügbar. Zum Zeitpunkt, als die Daten versehentlich an Google übermittelt und im Internet abrufbar gemacht wurden, handelte es sich somit nicht um allgemein verfügbare Daten iS des § 1 Abs 1 DSG.

Insoweit bewegt sich auch der 6. Senat des OGH mit der vorliegenden Entscheidung auf sicherem Grundrechtsterrain: Dass die ZPO zwar die „Volksöffentlichkeit" zum Verfahrensgrundsatz hat, im Übrigen aber die Verpflichtung, künftige öffentliche Verhandlungen (etwa in Form eines „Verhandlungsspiegels") öffentlich anzukündigen, nicht kennt,[38] macht einmal mehr deutlich, dass es sich bei Verfahrensdaten weder um „bereits veröffentlichte" noch um „allgemein verfügbare Daten"

---

32 Statt vieler *Jahnel*, Dreifacher Datenschutz? Das Verhältnis von Europarecht, Verfassungsrecht und einfachgesetzlichen Bestimmungen in der jüngsten Judikatur von EuGH und VfGH zum Datenschutzrecht, in: Bergauer/Staudegger (Hrsg), Recht und IT (2009), 33, 37 ff.

33 EuGH 16.12.2008, C-73/07 – *Satakunnan Markkinapörssi ./. Satamedia*, jusIT 2009/13, 28 = RdW 2009/170, 207 = ARD 5936/4/2009 = EuGRZ 2009, 23 = MR-Int 2009, 14 (*Wittmann*) = ecolex 2009, 547.

34 *Jahnel*, Datenschutzrecht Rz 1/47; *derselbe*, Dreifacher Datenschutz? Das Verhältnis von Europarecht, Verfassungsrecht und einfachgesetzlichen Bestimmungen in der jüngsten Judikatur von EuGH und VfGH zum Datenschutzrecht in *Bergauer/Staudegger* (Hg), Recht und IT, 33.

35 *Jahnel*, Datenschutzrecht Rz 1/52; aA *Kotschy*, Das Grundrecht auf Geheimhaltung personenbezogener Daten. Rückblick und Ausblick (Teil I: § 1 Abs1 DSG (1978) bzw DSG 2000), in: Jahnel (Hrsg), Datenschutzrecht und E-Government. Jahrbuch 2012 (2012), 27, 45 f.

36 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutzrichtlinie – DSRL), ABl L 281 vom 23.11.1995, 31 ff; Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation – EDSRL), ABl L 201 vom 31.7.2002, 37 ff, geändert durch RL 2006/24/EG des Europäischen Parlaments und des Rates vom 15.3.2006, ABl L 105 vom 13.4.2006, 54, und RL 2009/136/EG des Europäischen Parlaments und des Rates vom 25.11.2009, ABl L 337 vom 18.12.2009, 11.

37 VfGH 15.6.2007, G 147/06 – *Section Control*, VfSlg 18146; 28.11.2001, B 2271/00 – *TK-Wirtschaftsdatenabfrage*, VfSlg 16.369.

38 *Schragel* in *Fasching/Konecny*, ZPO2, § 171 Rz 7.

handelt. Gemäß § 415 letzter Satz ZPO wird ein bei Schluss der mündlichen Verhandlung der schriftlichen Ausfertigung vorbehaltenes Urteil nicht verkündet, was erfahrungsgemäß der Regelfall ist.[39] Dass die mündliche Verkündung eines Urteils grundsätzlich möglich ist, entkleidet die im Richterspruch enthaltenen personenbezogenen Daten nicht ihres privaten Charakters.

4.3. Rechtsfolgen

4.3.1. Verletzung von schutzwürdigen Geheimhaltungsinteressen

Gegenstand des Ausgangsverfahrens bildet die Feststellung, dass die Beschwerdeführer in ihrem jeweiligen Grundrecht auf Geheimhaltung der sie betreffenden personenbezogenen Daten von Justizorganen verletzt worden sind. Der durch das Grundrecht auf Datenschutz unmittelbar eingeräumte subjektiv-öffentliche Anspruch auf Geheimhaltung personenbezogener Daten schützt sowohl vor ungerechtfertigter Ermittlung als auch Übermittlung von Daten. Damit steht nunmehr rechtskräftig fest, dass der Akt der Gerichtsbarkeit gegenüber den Betroffenen rechtswidrig ist und das Organ schuldhaft gehandelt hat.

Der nunmehr naheliegende Anspruch auf Schadenersatz gehört aber nicht zu den aus dem Grundrecht auf Datenschutz gemäß § 1 Abs 1 DSG ableitbaren Ansprüchen (Geheimhaltung, Löschung, Richtigstellung, Auskunft), sodass eine unmittelbare Geltendmachung zunächst ausscheidet.[40]

4.3.2. Schadenersatz

Durch eine Deaktivierung des Passwortschutzes lagen die Daten für jedermann auf der Welt offen. Physisch „lagen" die Namen und Schadensbeträge hunderter Anleger auf einem gespiegelten Server in Denver, USA, schreibt der OGH in seinem Beschluss. Suchroboter von Google stießen auf diese Daten, eine Anlegerin googelte ihren Namen, fand ihn bei Google und die Affäre flog auf. Google hat alle Daten gelöscht – wirklich alle? Aufmerksame Rechtsanwender wissen, dass das Internet nicht vergisst,[41] aber nunmehr vergessen soll.[42]

Gemäß § 33 Abs 1 DSG hat der Betroffene gegen den Auftraggeber oder Dienstleister Anspruch auf Schadenersatz nach den allgemeinen Bestimmungen des bürgerlichen Rechts. In einem Fall hat sich das zivile Höchstgericht[43] bereits mit dem Anspruch auf angemessene Entschädigung wegen erlittener Kränkung nach § 33 Abs 1 DSG befasst und deutlich gemacht, dass es sich dabei um den Ersatz immateriellen Schadens handelt.[44] Werden durch die öffentlich zugängliche Verwendung der in § 18 Abs 2 Z 1 bis 3 DSG genannten Datenarten schutzwürdige Geheimhaltungsinteressen eines Betroffenen in einer Weise verletzt, die einer Eignung zur Bloßstellung gemäß § 7 Abs 1 MedienG gleichkommt, so gilt diese Bestimmung auch in Fällen, in welchen die öffentlich zugängliche Verwendung nicht in Form der Veröffentlichung in einem Medium geschieht.

Der Anspruch auf angemessene Entschädigung für die erlittene Kränkung ist gegen den Auftraggeber der Datenverwendung geltend zu machen. Von den in § 18 Abs 2 Z 1 bis 3 DSG genannten Datenarten kommen als schadenersatzbegründend lediglich „die Kreditwürdigkeit betreffende Daten" in Betracht. Dass die rechtswidrige Aufnahme in die von Google suchbar gemachten Gerichtsserver geeignet war, die Betroffenen in der Öffentlichkeit bloß zustellen, weicht von der Rsp[45] nicht ab. Jemanden bloßstellen bedeutet im Fall des § 33 Abs 1 zweiter Satz DSG, Tatsachen (nämlich die in § 18 Abs 2 Z 1 bis 3 DSG genannten Datenarten) zu enthüllen, die ihn aus Sicht Dritter herabsetzen und sein Ansehen untergraben.[46] Nach der klaren Fassung des § 33 Abs 2 DSG geht es um bestimmte Datenarten und nicht um den „höchstpersönlichen Lebensbereich", mögen auch die Datenarten dem höchstpersönlichen Lebensbereich eines Menschen zugehören. Selbst wenn Daten der in § 18 Abs 2 Z 1 bis 3 DSG genannten Art für eine begrenzte Öffentlichkeit sichtbar oder einem begrenzten Kreis von Personen, zB im Gerichtsbetrieb, bekannt waren, schließt dies nicht aus, dass durch die öffentlich zu-

---

39 Vgl *Schragel* aaO Rz 8.

40 Vgl DSK 5.4.2002, K120.766/004-DSK/2002, RIDA-Nummer: 0154201.

41 Vgl die Website „Datenleck – Chronik der Datenpannen", abrufbar unter http://datenleck.net/?&fverursacher=330 (21.5.2014).

42 Vgl deutlich EuGH 13.5.2014, C-131/12 – *Google Spain ./. AEPD*, Rz 98 f, ZIR 2014, 204.

43 OGH 15.12.2005, 6 Ob 275/05t, RdW 2006/207, 212 = Zak 2006/201, 117 = ÖJZ-LSK 2006/84 = EvBl 2006/66, 373 = ecolex 2006/211, 486 = lex:itec 2006 H 3, 29 (*Thiele*) = ÖBA 2006/1356, 530 = MR 2006, 83 (*Knyrim*) = RZ 2006, 130 = ZIK 2006/82, 68 = JUS Z/4124 = SZ 2005/18.

44 Ebenso *Jahnel*, Handbuch Rz 9/63 FN 187 unter Bezugnahme auf Art 23 DSRL.

45 OGH 17.12.2009, 6 Ob 247/08d – *Kreditauskunftei*, ZFR 2010/82, 141 = jusIT 2010/49, 117 (*Kastelitz/Leiter*) = RdW 2010/306, 288 = ZIK 2010/168, 116 = ÖBA 2010/1623, 326 = KRES 10/261.

46 OGH 15.12.2005, 6 Ob 275/05t, RdW 2006/207, 212 = Zak 2006/201, 117 = ÖJZ-LSK 2006/84 = EvBl 2006/66, 373 = ecolex 2006/211, 486 = lex:itec 2006 H 3, 29 (*Thiele*) = ÖBA 2006/1356, 530 = MR 2006, 83 (*Knyrim*) = RZ 2006, 130 = ZIK 2006/82, 68 = JUS Z/4124 = SZ 2005/18.

gängliche Verwendung dieser Daten schutzwürdige Geheimhaltungsinteressen in einer Weise verletzt werden, die einer Bloßstellung in der Öffentlichkeit gleichkommt.[47]

Ausblick: Als rechtliche Herausforderung dürfte sich allerdings die Durchsetzung des Schadenersatzanspruchs gegenüber der Republik als Rechtsträger der Justiz erweisen. Dass es sich dabei um einen Amtshaftungsanspruch nach dem AHG handelt, weil Ansprüche aus der Behauptung eines rechtswidrigen Verhaltens von für den Bund handelnden Organen abgeleitet werden, liegt auf der Hand. Damit wäre die Zuständigkeit der ordentlichen Gerichte nach § 1 AHG eröffnet. Allein es verbleibt ein gewisses Spannungsverhältnis zur Verweisungsnorm des § 83 GOG. Nach dieser richtet sich „die Durchsetzung der im DSG 2000 geregelten Rechte des Betroffenen", wozu auch der Anspruch nach § 33 DSG zählt, nach den Vorschriften des GOG. Allein in § 84 GOG findet der Schadenersatzanspruch keine Erwähnung, sodass es im Umkehrschluss wohl bei der Zuständigkeit der allgemeinen Zivil- als Amtshaftungsgerichte verbleibt.

Weit kostengünstiger, aber offenbar realiter nicht machbar, käme eine rechtzeitige Entschuldigung bzw ein „Datenpannen-Management", welches rasch das enttäuschte Vertrauen der Betroffenen in ein chronisch unterdotiertes, aber grosso modo sehr gut funktionierendes Justizsystem wiederhergestellt hätte.[48]

5. Zusammenfassung

Nach Ansicht des OGH findet eine Verletzung des Grundrechts auf Datenschutz nach § 1 Abs 1 DSG durch die (versehentliche) Veröffentlichung von gerichtlichen Verfahrensdaten immer dann statt, wenn die Namen der Parteien, der Parteienvertreter, die Streitwerte und die Aktenzahl an Google gelangen, und dadurch die Möglichkeit besteht, diese Daten für einen bestimmten Zeitpunkt im Internet abzurufen. Die Feststellung der Verletzung schutzwürdiger Geheimhaltungsinteressen der Betroffenen sind nach den sonderdatenschutzrechtlichen Vorschriften der §§ 83 ff GOG bei den ordentlichen Gerichten geltend zu machen. Allfällige Schadenersatzansprüche bleiben einem Amtshaftungsverfahren vorbehalten.

47 Vgl OGH 17.12.2009, 6 Ob 247/08d – *Kreditauskunftei*, ZFR 2010/82, 141, unter Zitierung von *Berka* in *Berka/Höhne/Noll/Polley*, Mediengesetz² § 7 Rz 20.

48 Vgl *Bauer*, Entscheidungsanmerkung, jusIT 2014, 73: „... anstelle des Versuchs einer nicht aussichtsreichen Rechtfertigung ...".