Clemens THIELE

Widerspruchslose Bonitätsdatenbanken – Die Datenschutzjudikatur des OGH im Jahr 2010

Inhaltsübersicht

I. Einleitung

Die folgende Untersuchung beschränkt sich auf eine **überblicksmäßige Erörterung der im Jahr 2010 ergangenen zivilgerichtlichen Judikatur zum Datenschutzrecht**. Dabei wird zunächst versucht, die oberstgerichtlichen Lösungen kritisch zu hinterfragen und die Entscheidungen insgesamt in den methodisch-dogmatischen Zusammenhang des DSG und des Richtlinienrechts einzuordnen.

In chronologischer Reihenfolge wird z.T. in wesentlich unterschiedlicher Tiefe auf folgende Judikate eingegangen:[1]

Ger.	Datum	GZ	Kurzbezeichnung	Fundstelle
OGH	15.04.2010	6 Ob 40/10s	*Datenformat*	jusIT 2010/61, 136 (*Staudegger/Thiele*) = RdW 2010/530, 517
OGH	15.04.2010	6 Ob 41/10p	*Datenlöschung*	ecolex 2010/315, 858 = jusIT 2010/69, 146 (*Kastelitz/Leiter*) = RdW 2010/528, 516 = RZ-EÜ 2010/144, 237 = ZIK 2010/374, 238
OGH	22.04.2010	2 Ob 1/09z	*Klauselprüfung Leasingvertrag*	jusIT 2010/90, 188 (*Thiele*) = ÖBA 2010/1658, 686 m Anm *Kellner*, ÖBA 2010, 674
OGH	19.05.2010	6 Ob 2/10b	*Widerspruch beim Informationsverbundsystem*	jusIT 2010/70, 148 (*Kastelitz/Leitner*) = ZFR 2010/143, 226
KOG	22.06.2010	16 Ok 3/10	*Aufzugskartell III*	EvBl-LS 2010/141 = ÖBl-LS 2010/189 (*Hoffer*) = ÖZK 2010, 140 = wbl 2010/180, 480
OGH	11.10.2010	6 Ob 112/10d	*Widerspruch gegen Warnliste der Kreditinstitute*	jusIT 2010/12, 26 (*Thiele*) = JBl 2011, 113 = ÖBA 2011/1697 = ZFR 2011/10 (*Ennöckl*)
OGH	21.12.2010	6 Ob A 1/10f	*Öffentlicher Auftraggeber*	nv

II. Datenformat (Dienstleister; Datenherausgabe; Datenübergabe; fehlende Vereinbarung)

2.1. Der Dienstleister hatte die Personalverrechnung eines Unternehmens zu übernehmen, wobei es auch dessen Aufgabe war die Mitarbeiterdaten des Auftraggebers anhand der zur Verfügung gestellten Papierakte zu digitalisieren. Zudem musste er die Zeitwirtschaft und die Personalverrechnung sowie auch das Personalcontrolling, die Personalentwicklung und das Bewerbermanagement der Belegschaft anhand einer adaptieren Standardsoftware durchführen. Es wurde die gesamte Hard- und Softwareplattform des Dienstleisters genutzt,

1 Stichtag für die folgende Entscheidungsübersicht der Zivilsenate des OGH ist der 31.12.2010. Sämtliche Judikate sind im Volltext unter *http://www.eurolawyer.at* abrufbar.

der einen Web-Zugriff für den Auftraggeber einrichtete und sich zu Datenschutz und Datensicherheit auf höchstem Standard verpflichtete.

Der Auftraggeber löste den Vertrag vorzeitig auf. Der Dienstleister überstellte per Spedition die Papierakte und einen USB-Stick mit den Daten im .pdf-Format und .txt-Format. Daraufhin klagte der Auftraggeber, die Daten in einer Form zu übergeben, die für diesen in seiner Datenverarbeitung automatisch (ohne weitere Konvertierung oder Bearbeitung) verarbeitungstauglich sind.

Die Unterinstanzen wiesen die Klage ab. Das Höchstgericht hatte letztlich zu klären, ob der Auftraggeber nach § 11 Abs 1 Z 5 DSG einen Anspruch darauf hat, dass ihm sein Dienstleister die Daten in einem bestimmten, lesbaren (d.h. automatisch verwertbaren) Format übergibt?

2.2. Der OGH bestätigte die Klagsabweisung der Vorinstanzen und verneinte eine derartige Herausgabeverpflichtung des datenschutzrechtlichen Dienstleisters.

Aus der Bestimmung des § 11 Abs 1 Z 5 DSG könnte keine Verpflichtung abgeleitet werden, die vorhandenen Daten in einem ganz bestimmten, für den Auftraggeber am besten zu handhabenden Format zu übergeben. Eine diesbezügliche Vereinbarung hatten die Streitteile nicht getroffen. Nach den Feststellungen der Vorinstanzen bestand auch keine diesbezügliche Verkehrssitte. Dazu kam, dass für das dpw-Programm eine eigene Lizenz erforderlich war. Auch aus dieser zusätzlichen Erwägung konnte keine Verpflichtung der Übergabe von Daten in Form von dpw-Dateien abgeleitet werden. Ebenso wenig bot § 1009 ABGB eine Grundlage für das von der klagenden Partei erhobene Begehren.

2.3. Diese noch zur alten, aber durch die DSG-Novelle 2010[2] insoweit unverändert gebliebenen Datenschutzrechtslage ergangene Entscheidung bedeutet einigen Beratungsaufwand, insbesondere im Bereich des IT-Outsourcings.

Bedient sich ein Unternehmen Dritter als gewissermaßen outgesourcte IT-Partner oder wie im Ausgangsfall einer externen Personalverrechnung,[3] ist in diesen Fällen ein Dienstleister- oder Datenverarbeitervertrag iS des § 10 DSG (zumindest mündlich) abzuschließen, um die Zulässigkeit der Überlassung von Daten zu gewährleisten. § 11 Abs 2 DSG empfiehlt die Schriftlichkeit derartiger Verträge.

Es handelt sich also um eine Vereinbarung zwischen dem **Auftraggeber**[4] iS des § 4 Z 4 DSG einerseits und dem **Dienstleister**[5] iS des § 4 Z 5 DSG andererseits, die gemäß § 11 Abs 1 DSG einen zwingenden gesetzlichen Inhalt sowie nach der nunmehr vorliegenden Entscheidung auch einen u.U. ratsamen Inhalt aufweisen muss. Die datenschutzrechtliche Besonderheit besteht darin, dass ein Überlassen der personenbezogenen Daten vom Auftraggeber an den Dienstleister als interne Handlung eingestuft wird, die keine Zweckbindung, sondern lediglich die vertragliche Grundlage, insbesondere die Auftragsbindung, erfordert.[6]

---

2 BGBl I 2009/133 in Kraft seit 1.1.2010.

3 Vgl. zur Dienstleistereigenschaft DSK 20.05.2005, K120.862/0011-DSK/2005, RIDA0195281.

4 Grundlegend *Jahnel*, Handbuch Datenschutzrecht (2010), Rz 3/29 ff mwN.

5 Art 2 lit e Datenschutz-Richtlinie (DSRL), 95/46/EG, ABl L 281, 31 bezeichnet ihn als „Auftragsverarbeiter".

6 Vgl. das ausführliche Prüfungsschema von *Knyrim*, Datenschutzrecht (2003), 201 ff.

§ 11 Abs 1 Z 5 DSG verpflichtet den Dienstleister *„nach Beendigung der Dienstleistung alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben oder in dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten."* Ein Teil der Lehre[7] hat bereits zutreffend herausgearbeitet, dass eine Rückgabeverpflichtung der Daten selbst besteht, weil sich diese von den ausdrücklich genannten Verarbeitungsergebnissen nicht mehr trennen lassen. Über die Art und Weise der Herausgabe bestimmt das Gesetz nichts, sodass es sich empfiehlt, „im Dienstleitervertrag festzulegen, was mit den Daten nach Beendigung des Auftrags zu geschehen hat".[8]

Nach Auffassung der Höchstrichter verpflichtet diese Gesetzesbestimmung den Dienstleister nicht dazu, die Daten an den Auftraggeber in einer bestimmten, zur Weiterverarbeitung in der eigenen EDV geeigneten Form zu übergeben. Sofern im Vertrag keine ausdrückliche Regelung dazu vorhanden ist, stellt dies auch keine vertragliche Nebenpflicht des Dienstleisters dar. Auch aus der – insoweit von der Erstinstanz nicht feststellbaren – „Verkehrssitte" ist eine derartige Verpflichtung nicht ableitbar.

Schließlich verneinen die Höchstrichter auch eine Herausgabeverpflichtung nach den im Auftragsverhältnis geltenden zivilrechtlichen Bestimmungen. Nach § 1009 ABGB ist der Gewalthaber (Auftragnehmer oder hier Dienstleister) nur verpflichtet, alles vom Auftraggeber Stammende herauszugeben, das er nicht mehr benötigt. Nachdem im konkreten Anlassfall alle Originalunterlagen sowie die Lohnkonten in digitalisiert Form (.pdf / .txt) an den Auftraggeber übergeben worden sind, hat der Dienstleister damit seine (zivilrechtliche) Verpflichtung erfüllt. Aufgrund der Tatsache, dass die Formate .pdf und .txt *„durchaus übliche und gängige Dateiformate"* sind, kann sich der Auftraggeber auch nicht auf das Schikaneverbot nach § 1295 Abs 2 ABGB berufen. Die behaupteten Werknutzungsrechte iS der §§ 24, 26 Urheberrechtsgesetz an den dpw-Dateien lassen die Höchstrichter schon mangels Werkqualität der Lohnverrechnungsdaten[9] zu Recht scheitern.

In jedem Fall sind bei Abschluss eines Dienstleistungsvertrages nach § 11 Abs 2 DSG besondere Vorkehrungen zu treffen, um den zukünftigen Zugriff auf die eigenen Daten rechtlich und tatsächlich abzusichern sowie klare Regelungen für die Rückgabe der Daten zu treffen, die es dem Auftraggeber ermöglichen, die (rückgestellten) Daten in der weiteren Folge in seinen Datenverarbeitungssystemen weiter zu verarbeiten. Fehlt diese Regelung, dann reicht die Rückgabe der Originalunterlagen sowie der Daten in üblichen Dateiformaten aus. Dies führt zu erheblichen Mehrkosten beim Wechsel des Dienstleisters.

2.4. Nach Ansicht der Gerichte hat der Auftraggeber weder nach dem DSG noch nach ergänzender Vertragsauslegung einen Anspruch darauf, dass ihm ein Dienstleister die Daten in einem für den Auftraggeber lesbaren (hier: automatisch verwertbaren) Format übergibt. Klare Regelungen im Datenverarbeitungsvertrag sind daher in der Praxis dringend zu empfehlen.

---

7 *Jahnel*, Datenschutzrecht, Rz 3/65; *Andréewitch/Steiner*, Outsourcing – Herausgabe der Daten bei Vertragsbeendigung? ecolex 2005, 358, 359.

8 *Jahnel*, Datenschutzrecht Rz 3/65.

9 Vgl. OGH 9.11.1999, 4 Ob 282/99w – *Ranking*, MR 1999, 346 = ÖBl-LS 2000/26, 58.

III. Datenlöschung (Widerspruch; Löschung; physisches Vernichten; keine Datensperrung)

3.1. Der beklagte KSV 1870 ist Betreiber von Informationsverbundsystemen unter der Bezeichnung „Konsumenten-Kredit-Evidenz" (KKE) und „Warnliste" sowie einer über seine Website zugänglichen Bonitätsdatenbank. Bereits 1996 ermittelte der beklagte Kreditschutzverband Daten des (im Jahr 1998 insolvent gewordenen) Klägers ohne dessen Zustimmung zur Verarbeitung.

Der spätere Kläger erhob zunächst mit Schreiben an die beklagte Partei vom 17.7.2008 Widerspruch nach § 28 DSG gegen die Verwendung seiner Daten. Ab diesem Datum waren in der Datenbank der beklagten Partei die Daten des Klägers nicht mehr im Wege einer Onlineabfrage zugänglich, sondern wurde lediglich die Auskunft *„keinen Treffer gefunden"*. Ungeachtet dessen waren die Daten des Klägers weiterhin einem nicht von vornherein abgegrenzten Personenkreis zugänglich unter der Voraussetzung einer persönlichen Überprüfung des rechtlichen Interesses des Anfragenden durch den Leiter der Wirtschaftsinformation der beklagten Partei bzw. dessen Stellvertreter. Ab 16.1.2009 richtete die beklagte Partei eine vollständige Sperre ein, sodass Daten über den Kläger seither nur mehr einem bestimmten Kreis zugänglich sind, nämlich dem Leiter der Wirtschaftsinformation und dessen Stellvertreter. Eine unternehmensinterne Übermittlung von bonitätsbezogenen Daten des Klägers fand nicht statt. Eine Löschung der Daten erfolgte nicht. Die Daten des Klägers wurden von der beklagten Partei ungeachtet des eingeschränkten Zugriffs weiterhin verarbeitet.

Der Kläger begehrte die Löschung der gegenständlichen Daten aufgrund des seinerzeit erhobenen Widerspruchs nach § 28 Abs 2 DSG, der mit einem Antrag auf Löschung gemäß § 28 Abs 1 DSG verbunden worden war.

Die beklagte Partei wendete ein, die Daten nicht mehr zu verwenden, ein physisches Löschen nicht notwendig und eine Sperre des Zugangs zu diesen Daten völlig ausreichend wäre.

Die ersten beiden Instanzen gaben dem Löschungsbegehren statt und verfügten ein „physisches Vernichten" der personenbezogenen Daten.

Das Höchstgericht hatte letztlich zu klären, ob die „Löschung" von Daten nach einem Widerspruch gemäß § 28 Abs 2 DSG durch „physisches Löschen" (Vernichten) oder durch „logisches Löschen" (Sperren) von Daten erfüllt würde?

3.2. Der OGH bestätigte die Entscheidungen der Vorinstanzen und sprach aus, dass die Daten unwiederbringlich zu vernichten waren. Um das datenschutzrechtliche Löschungsgebot zu erfüllen, genügte es nach Ansicht der Höchstrichter nicht, die Datenorganisation so zu verändern, dass bloß ein „gezielter Zugriff" auf die betreffenden Daten ausgeschlossen wäre. Es bedürfte einer physischen Beseitigung. Schon der vom Betroffenen rechtmäßig erhobene Widerspruch nach § 28 DSG löste die Verpflichtung zur Vernichtung der Daten beim Auftraggeber aus.

3.3. Die vorliegende Entscheidung klärt die nicht nur in der Lehre z.T. umstrittenen Anforderungen an die „Datenlöschung", sondern klärt auch eine in der Praxis häufig gestellte Herausforderung zumindest aus juristischer Sicht ab.

Anhand der konkreten Fragestellung, ob ein Auftraggeber (hier: der Betreiber einer Datenbank als derjenige, der für die Datenverarbeitung verantwortlich ist) die Verpflichtung hat, nach einem Widerspruch gemäß § 28 DSG die Daten (zur

Gänze, unwiederbringlich) aus der Datenbank zu entfernen, m.a.W physisch zu löschen, zu vernichten, oder ob insoweit eine bloße Sperre (auch als „logisches Löschen" bezeichnet) des Zugangs zu diesen Daten ausreicht?

Das Datenschutzgesetz unterscheidet in § 4 Z 9 DSG selbst praxisnah zwischen dem „*Löschen und Vernichten von Daten*" einerseits und dem „*Sperren von Daten*" andererseits. Es kann nämlich in der modernen elektronisch-gestützten Datenverarbeitung durchaus den Anwenderwunsch geben, gelöschte Daten so lange wie möglich zu erhalten, da sie (möglicherweise) irrtümlich gelöscht sein können und dies erst nach einiger Zeit auffällt. Die Praxis spricht von aufwandslos rekonstruierbaren Daten und einem sog. logischen Löschen.

Unter dem „*Löschen*" versteht ein Teil der Lehre[10] eine Maßnahme mit der Wirkung, dass der Auftraggeber nicht mehr über die Daten verfügt. Der OGH schließt sich der hL[11] ausdrücklich an, wonach zur Erfüllung des Löschungsgebotes es nicht genügt, die Datenorganisation bloß so zu verändern, dass ein „gezielter" Zugriff" auf die Daten ausgeschlossen ist. Vielmehr bedarf es eines physischen Löschens, d.h. einer unumkehrbaren Beseitigung. Die Höchstrichter verweisen auch auf § 3 Abs 4 Z 4 (deutsches) BDSG, das insoweit eine Legaldefinition der Begriffe „Löschung" und „Sperre" nach den vorgenannten Kriterien enthält.[12] Diese Differenzierung entspricht mE auch der DSRL.[13]

Die von den Gerichten klar statuierte Löschungsverpflichtung löst bei Nichtbeachtung in den Fällen der §§ 27, 28 DSG, d.h. bei verspäteter Löschung oder Nichtlöschung, nach § 52 Abs 2a DSG[14] eine Verwaltungsstrafe in Höhe von bis Euro 500,-- aus. Es liegt daher im wirtschaftlichen Interesse von Unternehmen, aber auch öffentlich-rechtlichen Auftraggebern, einer Löschung bzw. Richtigstellung nach § 27 DSG oder einem Widerspruch nach § 28 DSG umgehend – jedenfalls innerhalb der Maximalfrist von acht Wochen – durch effektives und nachhaltiges Löschen nachzukommen.

3.4. Nach Auffassung der österreichischen Gerichte führt ein datenschutzrechtlicher Widerspruch nach § 28 DSG nicht nur zu einem Verwendungsverbot der personenbezogenen Daten des Betroffenen, sondern zugleich zur gerichtlich durchsetzbaren Verpflichtung des Auftraggebers, die (allenfalls) vorhandenen Daten zur Gänze, unwiederbringlich aus der Datenbank zu entfernen, d.h. physisch zu löschen, zu vernichten bzw. nachhaltig löschen zu lassen.

---

10 *Jahnel*, Datenschutzrecht Rz 3/112.

11 *Jahnel*, Datenschutzrecht Rz 3/112 und 7/74 mwN; ebenso *Drobesch/Grosinger*, Datenschutzgesetz (2000), Anm 4 zu § 27 Abs 6; aA *Dohr/Pollirer/Weiss/Knyrim*, DSG² § 27 Anm 18 ohne Begründung.

12 Vgl. *Jahnel*, Datenschutzrecht Rz 3/112; *Simitis*, Kommentar zum Bundesdatenschutzgesetz[6] § 3 Rz 180 ff.

13 Vgl. *Dammann/Simitis*, EU-Datenschutzrichtlinie (1997), Anm 16 und 17 zu Art 12, 198.

14 IdF DSG-Nov 2010 für eine Säumnis seit dem 01.01.2010.

IV. Klauselprüfung Leasingvertrag (Datenverarbeitungsklausel, Zustimmung in AGB; Transparenzgebot)

4.1. In dem vom Verein für Konsumenteninformation (VKI) geführten Rechtsstreit handelte es sich um eine Verbandsklage gegen ein Leasingunternehmen, die O-GmbH, wegen der massenhaften Verwendung von Formularverträgen bei Kfz-Leasinggeschäften. Mit Schreiben vom 21. 3. 2007 beanstandete die klagende Partei insgesamt 43 Klauseln der Allgemeinen Geschäftsbedingungen der beklagten Partei als gesetz- bzw. sittenwidrig und forderte die beklagte Partei auf, binnen bestimmter Frist eine vorformulierte „Unterlassungserklärung mit Vertragsstrafevereinbarung" abzugeben. Danach sollte sich die beklagte Partei verpflichten, eine Vertragsstrafe von 726 EUR pro Klausel und pro Zuwiderhandlung an die klagende Partei zu bezahlen. Aus der Perspektive des Datenschutzrechts war folgende Klausel strittig: *„Der LN ist ausdrücklich damit einverstanden, dass die personen- und wirtschaftsbezogenen Daten aus gegenständlichem Leasingvertrag automationsunterstützt verarbeitet und zur Durchführung dieser Geschäftsverbindung herangezogen werden. Diese Daten werden auf Anfrage O*****-Abteilungen und O*****-Geschäftsstellen zur Beurteilung von Finanzierungen und zur Abwicklung des Zahlungsverkehrs zur Verfügung gestellt ebenso Gläubigerschutzverbänden. Auf Widerruf des LN werden hinkünftig keine Daten an Dritte übermittelt."*

Nach Auffassung der klagenden Partei verstieß die Klausel gegen § 4 Z 14 DSG und, weil sie die Tragweite der Einwilligung nicht erkennen ließ, gegen das verbraucherschutzrechtliche Transparenzgebot des § 6 Abs 3 KSchG. Die beklagte Partei hielt dem entgegen, dass der Personenkreis der Datenempfänger ebenso wie deren Aufgabenbereich und der Zweck der Weitergabe klar angegeben wäre. Die Zustimmung des Leasingnehmers wäre ohnedies widerrufbar. Das Erstgericht wies das Unterlassungsbegehren ab. Das Berufungsgericht schloss sich hingegen der Ansicht des VKI an.

4.2. Der OGH bestätigte diese Auffassung und erläuterte die Voraussetzungen einer wirksamen datenschutzrechtlichen Zustimmungserklärung.[15] Unter Bezugnahme auf einschlägige Vorjudikatur in den Fällen Mobilpoints,[16] Creditanstalt,[17] Friends of Merkur,[18] BA-CA,[19] oder GE-Money-Bank[20] betont das Höchstgericht, dass eine in Allgemeinen Geschäftsbedingungen enthaltene, wirksame Zustim-

---

15 Dazu *Knyrim*, Datenschutzrechtliche Zustimmungserklärungen richtig formulieren und platzieren in *Knyrim/Leitner/Perner/Riss*, Aktuelles AGB-Recht (2008), 133 ff mwN.

16 OGH 13.9.2001, 6 Ob 16/01y, JBl 2002, 178 = RdW 2002/67, 79 = ecolex 2002/35, 86 (*Leitner*) = KRES 1h/32.

17 OGH 22.3.2001, 4 Ob 28/01y, ÖBA 2001/977, 645 (*Koziol*) = ecolex 2001/147, 438 (*Rabl*) = RdW 2001/557, 531 = SZ 74/52 = ÖBA 2004, 737 (*Apathy*) = KRES 1h/31.

18 OGH 27.1.1999, 7 Ob 170/98w, ecolex 1999/182 = RdW 1999, 458 = ARD 5023/25/99 = JUS Z/2765-2767 = SZ 72/12.

19 OGH 19.11.2002, 4 Ob 179/02f, RdW 2003/50, 66 (*Iro*) = ÖBA 2003/1090, 141 = ÖBA 2003, 129 (*Iro/Koziol*) = ÖBA 2003, 177 (*Apathy*) = wbl 2004, 213 (*Krassnig/Stotter*) = ÖBA 2004, 737 (*Apathy*) = SZ 2002/153 = KRES 3/113 = ÖBA 2008, 329 (*Gerhartinger*).

20 Vgl. OGH 20.3.2007, 4 Ob 221/06p, ecolex 2007/252, 601 (*Wilhelm*) = ÖBA 2007/1450, 981 (*Rummel*) = RZ 2007/EÜ 340/341/342/343/344/345/346, 226 = KRES 1d/95 = RdW 2008/10, 53 (*Gehringer*).

mung im Sinne des § 4 Z 14 DSG nur dann vorliegen kann, wenn der Betroffene weiß, welche seiner nicht sensiblen Daten zu welchem Zweck verarbeitet werden sollen; nur dann kann davon gesprochen werden, dass er der Verwendung seiner Daten „in Kenntnis der Sachlage für den konkreten Fall" zustimmt. Dies bedeutet, dass sowohl der Personenkreis der Datenempfänger, als auch deren Aufgabenbereich und der Zweck der Weitergabe klar angegeben sein müssen. Es besteht selbstverständlich eine jederzeitige Möglichkeit die Zustimmung zu widerrufen, auch ohne Angabe von Gründen. Ein derartiger Hinweis darauf hat lediglich deklarativen Charakter.

4.3. Gefordert wird demzufolge die **informierte Zustimmung**. Personenbezogene Daten dürfen immer dann verwendet werden, wenn die Geheimhaltungsinteressen der Betroffenen nicht verletzt sind. Dies ist nach den §§ 8, 9 DSG u.a. dann gegeben bei **Zustimmung des Betroffenen** iS des § 4 Z 14 DSG: Maßgebend ist die gültige, insbesondere *ohne Zwang* abgegebene *Willenserklärung* nach §§ 861, 869 ABGB des Betroffenen, sodass er in *Kenntnis der Sachlage* für den *konkreten* Fall in die *Verwendung* seiner Daten einwilligt. Diese Definition schließt für die Zukunft abgegebene allgemeine Zustimmungserklärungen aus.

Für die Praxis empfiehlt sich folgende **Checkliste**:

Anforderungen an eine Zustimmungserklärung

- grundsätzlich gilt **Formfreiheit**: auch mündlich (Beweisproblem), konkludent (schlüssig iSv § 863 ABGB) oder als Teil der AGB möglich[21]
- **Willenserklärung**: im zivilrechtlichen Sinn (§§ 861, 869 ABGB); Art hängt vom Adressaten ab, d.h. bei Konsumenten höhere Anforderungen als bei Geschäftsleuten. Klare Abgrenzung von zustimmungspflichtigen Datenübermittlungen von anderen.

Empfehlung: ausdrückliche Unterschrift, getrennt von sonstigen Vereinbarungen, deutlich hervorgehoben und erhöhte Informationspflichten.[22]

- **Kenntnis** der Sachlage: Aufklärung über Umfang der Datenarten, Inhalt der Daten, Zweck der Datenweitergabe, Empfänger der Daten (so detailliert, dass der Betroffene die konkreten Empfänger erkennen kann), insbesondere bei der Zustimmung zu Werbezwecken.[23]
- für den **konkreten** Fall: bestimmter Zweck und exakte Bedingungen; Pauschalzustimmungen, ohne besonderen Zweck sind unzulässig.[24]

21 OGH 2.8.2005, 1 Ob 104/05h: Zustimmung in Allgemeinen Geschäftsbedingungen möglich.

22 Vgl. OGH 20.3.2007, 4 Ob 221/06p, ecolex 2007/252, 601 (*Wilhelm*) = ÖBA 2007/1450, 981 (*Rummel*) = RZ 2007/EÜ 340/341/342/343/344/345/346, 226 = KRES 1d/95 = RdW 2008/10, 53 (*Gehringer*).

23 Vgl. OGH 20.3.2007, 4 Ob 221/06p, ecolex 2007/252, 601 (*Wilhelm*) = ÖBA 2007/1450, 981 (*Rummel*) = RZ 2007/EÜ 340/341/342/343/344/345/346, 226 = KRES 1d/95 = RdW 2008/10, 53 (*Gehringer*).

24 OGH 27.1.1999,7 Ob 326/98m – *In alle Welt*, ecolex 1999/183 = KRES 15/24 = RdW 1999, 457.

- **Widerrufshinweis**: gesetzlich nicht vorgeschrieben, aber Rsp[25] tendiert zur Widerrufsmöglichkeit in derselben Klausel wie Zustimmung, ansonsten besteht eine Irreführungsmöglichkeit.

V. Widerspruch gegen Informationsverbund (Auftraggebereigenschaft; Informationsverbund; Bonitätsauskunft)

5.1. Der Kläger begehrte gemäß § 28 Abs 2 DSG die Löschung des ihn betreffenden Datensatzes aus der Kleinkreditevidenz (KKE) der beklagten Parteien, die eine Auskunftei über Kreditverhältnisse iS von § 152 GewO betrieben, wobei sie bonitätsrelevante Informationen verarbeiteten. Die gespeicherten Daten stellten sie ihren Kunden mit rechtlichem oder wirtschaftlichem Interesse zur Verfügung. Bei der Konsumentenkreditevidenz handelte es sich um ein Informationsverbundsystem, in das die Bonitätsdaten des Klägers von der P-AG eingemeldet worden waren. Nichtsdestotrotz erklärte die zweitbeklagte Partei über schriftliche Aufforderung des Klägers vom 16.6.2009, dessen Datensatz würde erst im Juni 2014 gelöscht werden.

Im Sicherungsverfahren begehrte der Kläger daraufhin, die Übermittlung des ihn betreffenden Datensatzes zu unterlassen. Das Erstgericht gab dem Sicherungsbegehren gegenüber beiden beklagten Parteien statt, das Rekursgericht lediglich hinsichtlich der zweitbeklagten Partei.

Der OGH hatte sich daher u.a. mit der Frage auseinanderzusetzen, wer datenschutzrechtlicher Auftraggeber iS des § 4 Z 4 DSG und damit ob die beklagten Parteien konkret für den erhobenen Widerspruch des Betroffenen nach § 28 Abs 2 DSG passiv legitimiert war?

5.2. Das Höchstgericht wies den Antrag auf Erlassung einer Einstweiligen Verfügung gegen die beklagten Parteien ab, weil der Betreiber eines Informationsverbundsystems eben nicht Auftraggeber der Datenverarbeitung wäre, die ein anderer Teilnehmer in dieses eingemeldet hatte, auch wenn er (der Betreiber) selbst einer der teilnehmenden Auftraggeber des Inormationsverbundsystems war. Die Erledigung eines Löschungsanspruchs des Betroffenen setzte nämlich die Verfügungsgewalt des Auftraggebers über die davon betroffenen Daten voraus. Im vorliegenden Fall war die Unmöglichkeit, die Daten zu löschen, nicht faktischer, sondern rechtlicher Natur, sodass nur an die P-AG ein Löschungsbegehren zu richten wäre und allein diese für eine klagsweise Durchsetzung passiv legitimiert wäre. Der Betreiber eines Informationsverbundsystems war „nur" dafür verantwortlich, dass der Betroffene auch in Erfahrung bringen konnte, an wen er sich deshalb wenden könnte.

---

25 Vgl. OGH 20.3.2007, 4 Ob 221/06p, ecolex 2007/252, 601 (*Wilhelm*) = ÖBA 2007/1450, 981 (*Rummel*) = RZ 2007/EÜ 340/341/342/343/344/345/346, 226 = KRES 1d/95 = RdW 2008/10, 53 (*Gehringer*); 20.3.2007, 4 Ob 221/06p, ecolex 2007/252, 601 (*Wilhelm*) = ÖBA 2007/1450, 981 (*Rummel*) = RZ 2007/EÜ 340/341/342/343/344/345/346, 226 = KRES 1d/95 = RdW 2008/10, 53 (*Gehringer*).

5.3. Die vorliegende Entscheidung folgt der datenschutzrechtlichen Spruchpraxis[26] und der hL,[27] wonach für Informationsverbundsysteme § 28 Abs 2 DSG stets iVm § 50 Abs 1 DSG gelesen werden muss. Demzufolge hat zunächst der zwingend vorgesehene Betreiber als „erster Ansprechpartner des Betroffenen"[28] *„auf Antrag binnen zwölf Wochen alle Auskünfte zu geben, die notwendig sind, um den für die Verarbeitung seiner Daten im System verantwortlichen Auftraggeber festzustellen."* Das Widerspruchsrecht nach § 28 DSG, aber auch das in § 50 Abs 1 DSG ausdrücklich genannte Auskunftsrecht haben sich – wie sonst auch – gegen den datenschutzrechtlichen Auftraggeber zu richten.[29] Diese Auffassung findet seine Stütze gleichfalls in der Definition des Informationsverbundsystems nach § 4 Z 13 DSG, die von einer gemeinsamen Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber ausgeht, wobei *„jeder Auftraggeber auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden"*. Die Zuordnung der Daten zu den einzelnen Auftraggebern bleibt daher grundsätzlich aufrecht.[30]

5.4. Die Betroffenenrechte nach §§ 26 ff DSG sind auch bei Vorliegen eines Informationsverbundsystems nach § 4 Z 13 DSG ausschließlich gegen den (jeweiligen) datenschutzrechtlichen Auftraggeber zu richten. Der nach § 50 Abs 1 DSG einzusetzende Betreiber ist selbst dann nicht passiv legitimiert, wenn er selbst teilnehmender Auftraggeber ist, aber den konkreten Datensatz, gegen den Widerspruch erhoben worden ist, nicht geliefert hat.

VI. Aufzugskartell III (Datenschutz im Kartellverfahren; eingeschränkter Schutz von Geschäftsgeheimnissen; Auskunft)

6.1. In einem gegen mehrere Beschuldigte wegen Betrugs und wettbewerbsbeschränkender Absprachen bei Vergabeverfahren nach den §§ 146 ff, 168b StGB geführten Ermittlungsverfahren im Rahmen des sog. „Aufzugskartells" schaffte die Staatsanwaltschaft Wien den zugehörigen Kartellakt von der Bundeswettbewerbsbehörde bei. Den Beschuldigten und Privatbeteiligten wurde daraufhin im strafrechtlichen Vorverfahren (eingeschränkte) Akteneinsicht auch auf die Vernehmungsprotokolle und eidesstättigen Erklärungen des Kartellverfahrens gewährt.

Über Antrag des Vertreters eines der beteiligten Unternehmen forderte das OLG Wien als Kartellgericht den Akt zurück, weil Akteneinsicht mangels Zustimmung der betroffenen Verfahrensparteien nach § 39 Abs 2 KartG nicht gewährt

---

26 DSK 12.12.2007, K600.033-018/0002-DVR/2007, RIDA-Nummer: 0191051, zu den Auflagen für die Teilnahme einer Bank als Auftraggeber an der in Form eines Informationsverbundsystems vom KSV geführten Datenanwendung „Kleinkreditevidenz (Konsumentenkreditevidenz)" zum Zweck des Gläubigerschutzes und der Risikominimierung.

27 *Jahnel*, Datenschutzrecht Rz 8/85 mwN.

28 *Jahnel*, Datenschutzrecht Rz 8/84.

29 *Lettner*, Informationsverbundsysteme. Rechtliche Einführung und Grundlagen, lex:itec 2008 H 4, 17, 18.

30 Vgl. *Jahnel*, Datenschutzrecht Rz 8/89.

werden könnte. Mit dem Abhilfeantrag nach § 76 Abs 2a StPO an das übergeordnete Kartellobergericht (KOG) begehrte die Staatsanwaltschaft vom so zuständigen OGH, er möge feststellen, dass die durch § 39 KartG verfügte Beschränkung der Akteneinsicht unrechtmäßig wäre.

6.2. Das Höchstgericht nahm zunächst seine Kompetenz wahr und entschied, dass bei erstinstanzlicher Zuständigkeit des OLG Wien in analoger Schließung der planwidrigen Lücke des § 76 Abs 2a StPO der OGH zur Entscheidung berufen war. Inhaltlich gab das Höchstgericht dem Antrag statt und trug dem Kartellgericht (OLG Wien) auf, dem staatsanwaltschaftlichen Übersendungsersuchen in dem bestimmt bezeichneten Ermittlungsverfahren ohne Rücksicht auf die in § 39 Abs 2 KartG normierten besonderen Parteirechte nachzukommen. Eine spezifische behördliche Geheimhaltungspflicht, wie z.B. das nach § 38 BWG zu beachtende Bankgeheimnis, normierte § 39 Abs 2 KartG nämlich keineswegs. Geschäftsgeheimnisse iS des § 39 Abs 2 KartG wären auch keine (sensiblen) Daten gemäß § 4 Z 2 DSG. Die genannten Geschäftsgeheimnisse waren lediglich durch § 54 StPO geschützt, wonach untersagt ist, ua durch Akteneinsicht erlangte, personenbezogene, nicht öffentlich bekannt gewordene Daten einer breiten Öffentlichkeit zugänglich zu machen.

6.3. Die vorliegende Entscheidung gibt Anlass, sich mit dem Verhältnis von Geschäftsgeheimnissen und dem Datenschutz näher zu befassen. In Österreich fehlt eine allgemein gültige Definition des „*Geschäftsgeheimnisses*", wenngleich der Gesetzgeber den Begriff häufig verwendet, ihn aber stets voraussetzt.[31] „**Geschäftsgeheimnisse**" betreffen nach hA[32] Tatsachen und Erkenntnisse von wirtschaftlicher und kaufmännischer Bedeutung, wie zB Kalkulationsgrundlagen, Präferenzverträge mit Kunden und Lieferanten, eine Kundenkartei,[33] Quellen kaufmännischer Auskünfte, Höhe der Gehälter; Einzelheiten aus dem Finanzierungsbereich, wie Kreditumfang, Bankverbindung, Geldgeber, Umsatzhöhe und Reingewinn, steuerliche Verhältnisse, Tatsachen des Bankgeheimnisses, Informationsquellen des Redakteurs, aber auch die Deklarierung der Haltbarkeit von Lebensmitteln in einem Betrieb.[34] Die in Frage kommenden Tatsachen und Vorgänge müssen in einer Beziehung zum Betrieb stehen. Sie können auch Bedeutung für seine Wettbewerbsfähigkeit haben. Die Umstände sind idR nur einem eng begrenzten, im Wesentlichen geschlossenen Personenkreis bekannt, dem diese Kenntnis entsprechend der Natur des Betriebes nicht verwehrt werden kann. Nach dem Willen des Betriebsinhabers sollen sie geheim gehalten, somit vertraulich behandelt werden, und es muss ein berechtigtes Interesse an der Geheimhaltung bestehen.[35]

---

31 Vgl. z.B. §§ 122, 123, 124 StGB; §§ 11, 26 UWG; §§ 39, 47, 74 KartG; § 119 PatG; § 125 TKG 2003; §§ 305, 321 ZPO.

32 *Lewisch*, WK² § 122 Rz 9; *Leukauf/Steiniger*, StGB³ § 122 Rz 4; *Thiele* in SbgK, § 122 Rz 40; *derselbe* in *Wiebe/Kodek*, UWG § 11 Rz 34 jeweils mwN zur Rsp.

33 Vgl *Schmölzer*, Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr – Entscheidungsanmerkung zu OGH 6.12.1995, 13 Os 161/95, JBl 1997, 212.

34 OLG Linz 12.4.1989, 9 Bs 84/89, zitiert nach *Mayerhofer/Rieder* StGB⁵ § 123 ENr 3; siehe zum Ganzen *Schumacher*, Zeugnisverweigerung wegen eines Geschäftsgeheimnisses (§ 321 Abs 1 Z 5 ZPO), ÖJZ 1987, 673, 675.

35 Näher *Thiele* in SbgK § 122 Rz 33 ff.

Nach hL[36] handelt es sich bei Geschäftsgeheimnissen um *„Angaben"* iS des § 4 Abs 1 DSG, da das österreichische DSG auch die Daten juristischer Personen erfasst.

Nach der **uneinheitlichen Rsp**[37] entspricht die Zusammenstellung eines Verzeichnisses von Firmen und Telefonnummern von Kunden und Lieferanten unter Einbeziehung von Ansprechpersonen als solches nicht dem Erfordernis eines Geschäftsgeheimnisses; das Kopieren diesbezüglicher Daten aus dem Datenbestand des Arbeitgebers auf eine eigene Diskette des ausscheidenden Arbeitnehmers stellt kein strafbares Auskundschaften von Betriebsgeheimnissen dar, ist aber seit 1. 1. 2000 dem Straftatbestand des **§ 51 DSG** zu unterstellen. Demgegenüber verletzt nach einer anderen, höchst fragwürdigen E ein ehemaliger Mitarbeiter, der Unternehmensdaten (hier: Kunden- und Produktlisten) für eigene gewerbliche Zwecke weiterverwendet, weder das Datenschutzgeheimnis nach § 15 DSG noch die Vorschrift des § 11 UWG, da die Verarbeitung eigener Daten nicht unter das DSG fiele.[38] Insb letztere Entscheidung ist in der Lehre[39] völlig zu Recht auf vehemente Kritik gestoßen, da sie die **datenschutzrechtliche Rolle** des Betroffenen verkannt hat.

Darüber hinaus erlangt die datenschutzrechtliche Beurteilung eines Geschäftsgeheimnisses in der Spruchpraxis bislang bei der Interessenabwägung nach § 26 Abs 2 DSG zur Beschränkung der Auskunftserteilung eine entscheidende Bedeutung.[40] IdR kann der Auskunftspflichtige sich nicht mit Erfolg auf das Vorliegen eines Geschäftsgeheimnisses berufen, um die begehrte Auskunft zu verweigern.[41] Das vom KOG gefundene Ergebnis ist daher letztlich zutreffend.

6.4. Geschäftsgeheimnisse iSd § 39 Abs 2 KartG sind zwar personenbezogene, aber keine sensiblen (und damit besonders schutzwürdigen) Daten nach § 4 Z 2 DSG. Es gilt für sie daher die Bestimmung des § 8 Abs 1 Z 4 DSG, wonach schutzwürdige Geheimhaltungsinteressen bei Verwendung nicht-sensibler Daten dann nicht verletzt sind, wenn überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern. Das ist gemäß § 3 Z 2 DSG dann der Fall, wenn die Verwendung der Daten durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung zur Amtshilfe nach Art 22 B-VG geschieht.

---

36 *Jahnel*, Datenschutzrecht Rz 3/72 aE.

37 LG Linz 7.12.1999, 27 EVr 591/99, 27 EHv 123/99 – *Wirtschaftsspionage*, ARD 5120/27/2000; vgl. demgegenüber OGH SSt 7/6; EvBl 1949/430; ÖBl 1972, 72; ÖBl 1988, 13 – *Tenniskartei*; HG Wien 23.10.1998, ARD 4993/14/99; LG f ZRS Graz ArbSlg 7.014.

38 OGH 4.5.2004, 4 Ob 50/04p – *Unternehmensdaten*, ecolex 2004/415, 873 (krit *Knyrim*) = RdW 2004/540, 596 m krit Anm *Jahnel*, RdW 2005/244, 200 = SZ 2004/68.

39 *Jahnel*, OGH: Kein Schutz von Unternehmensdaten nach dem DSG? RdW 2005, 200; *Knyrim*, Entscheidungsanmerkung, ecolex 2004, 873.

40 Zur Stufenprüfung instruktiv *Jahnel*, Datenschutzrecht Rz 7/57 mwN.

41 DSK 15.02.2005, K120.981/0002-DSK/2005, RIDA 0151025, bestätigt durch VwGH 19.12.2006, 2005/06/0111 – *Kreditauskunftei*, JBl 2007, 466 = JUS A/4686 = ZfVB 2007/2585 = VwSlg 17.090 A

VII. Widerspruch gegen Warnliste der Kreditinstitute (Datensammlung; keine bankrechtliche Grundlage; Datenlöschung)

A. Typischer Ausgangsfall

Die spätere Beklagte, die L-AG, veranlasste die Einmeldung der personenbezogenen Daten des späteren Klägers in die Warnliste der österreichischen Kreditinstitute. Nachdem er Ende August 2005 vollständig Zahlung geleistet hatte, veranlasste die Beklagte die Einmeldung des Vermerks „vollständige Tilgung per 13.9.2005" in die Warenliste. Mit Schreiben vom 9.4.2008 erhob der Kläger zunächst Widerspruch nach den §§ 27, 28 DSG und forderte schließlich die Löschung der eingemeldeten Daten. Die Beklagte antwortete, dass diese erst nach dem Ablauf einer Tilgungsfrist von 3 Jahren, sohin frühestens am 18.9.2008 gelöscht würden. Dies hätte zur Folge, dass die Kreditinstitute nicht mehr auf diese Daten zugreifen könnten. Die Daten würden allerdings archiviert, um später nachvollziehbar ziehen zu können, wann jemals Einmeldungen erfolgten. Auf die archivierten Daten könnten das Rechenzentrum des KSV sowie die BA-CA Administration und Services GmbH zugreifen.

Das Erstgericht wies das Löschungs- bzw. Unterlassungsbegehren des Klägers unter Hinweis auf § 39 Abs 2 BWG ab. Das Berufungsgericht bestätigte diese Entscheidung, führte aus, dass § 39 Abs 2 BWG keine ausreichende gesetzliche Grundlage im Sinne des § 28 Abs 2 DSG darstellte, jedoch die Gefahren, die von einer öffentlichen Zugänglichkeit der Datenanwendungen ausgehen würden, mit der Archivierung der Daten im Sinne eines Sperrens gegen unbefugte Zugriffe „gebannt" wäre.

Im Wege der außerordentlichen Revision hatte der Oberste Gerichtshof letztlich die Frage zu klären, ob § 39 Abs 2 BWG eine ausreichende gesetzliche Grundlage im Sinne des § 28 Abs 2 DSG zur Archivierung von Kreditdaten herangezogen werden könnte?

B. Entscheidung des Gerichts

Die Höchstrichter gaben dem außerordentlichen Rechtsmittel Folge und verpflichteten die Beklagte, die in der Datenanwendung „Warnliste der Banken" verarbeiteten personenbezogenen Daten des Klägers binnen 14 Tagen zu löschen und dem Klagevertreter davon Mitteilung zu erstatten. § 39 Abs 2 BWG stellte lediglich ein von der Rechtsordnung grundsätzlich gebilligtes überwiegendes berechtigtes Interesse an der Sammlung, Aufbewahrung und Weitergabe bonitätsrelevanter personenbezogener Daten im Sinne des § 8 Abs 1 Z 4 DSG dar. Durch diese Vorschrift könnte aber weder die Aufnahme bestimmter Daten in eine Datenanwendung noch der Betrieb eines kreditinstitutsübergreifenden-Informationsverbundsystems iS des § 4 Z 13 iVm § 50 DSG über bonitätsrelevante Daten verpflichtend vorgesehen werden. Aufgrund des rechtmäßig erhobenen Widerspruchs nach § 28 Abs 2 DSG war die beklagte Partei nicht nur zum Sperren der Daten verpflichtet, sondern zu ihrer physischen Vernichtung. Die nachträgliche Einschränkung des Zugriffs auf die Daten nach einem gestellten Löschungsbegehren entspricht nämlich dem Löschungsgebot keineswegs. Zu

bedenken war auch, dass die Daten deshalb archiviert wurden, um irgendwann später nachvollziehen zu können, wann jeweils Einmeldungen erfolgten.

C. Bisherige Rechtslage

1. Position der Gerichte

Die vorliegende Entscheidung setzt die bisherige Rechtsprechung des 6. Senats zum Widerspruch gegen Bonitätsdatenbanken fort und rundet sie gewissermaßen (zeitlich) ab.[42] Bemerkenswert ist zunächst daran, dass für ein Widerspruchsrecht nach § 28 Abs 2 DSG die „Auslagerung" des Rechenzentrums des KSV an eine dritte Gesellschaft keine andere Beurteilung nach sich gezogen hat. Diesem Rechenzentrum ist nach den Feststellungen weiterhin der Zugriff auf die Daten möglich, sodass mit einer bloßen „Verschiebung ins Archiv" dem Löschungsanspruch des Klägers nicht entsprochen worden ist.

2. Widerspruchsrecht nach § 28 Abs 2 DSG

Die materiellen Voraussetzungen des Widerspruchsrechts nach § 28 Abs 2 DSG bestehen lediglich in

(1) der nicht gesetzlich angeordneten Aufnahmen
(2) in eine öffentlich zugängliche
(3) Datei.

(1) Im gegenständlichen Fall war die Aufnahme der personenbezogenen Kreditdaten des Klägers in eine öffentlich zugängliche Datei im Sinne der Rechtsprechung nicht strittig. Zu prüfen ist lediglich, ob § 39 Abs 2 BWG eine ausreichende gesetzliche Grundlage im Sinne einer gesetzlichen Anordnung enthält. § 39 Abs 2 BWG in der auf den Sachverhalt anwendbaren Fassung[43] lautet: *„Die Kreditinstitute haben für die Erfassung, Beurteilung, Steuerung und Überwachung der bankgeschäftlichen und bankbetrieblichen Risiken über Verwaltungs-, Rechnungs- und Kontrollverfahren zu verfügen, die derart dem Umfang und der Komplexität der betriebenen Bankgeschäfte angemessen sind. Die Verwaltungs-, Rechnungs- und Kontrollverfahren haben weitest gehend auch bankgeschäftliche und bankbetriebliche Risiken zu erfassen, die sich möglicherweise ergeben können. Die Organisationsstruktur hat durch den Geschäftsbetrieb angemessene aufbau- und ablauforganisatorische Abgrenzungen Interessen- und Kompetenzkonflikte zu vermeiden. Die Zweckmäßigkeit dieser Verfahren und deren Anwendung ist von der internen Revision mindestens einmal jährlich zu prüfen."*

---

42 OGH 14.9.2006, 6 Ob 167/06m, JUS Z/4256; 1.10.2008, 6 Ob 195/08g, jusIT 2009/14, 28 (*Dörfler*) = ÖJZ EvBl-LS 2009/33, 233 = RdW 2009/172, 208 = ÖBA 2009/1549, 395 = ecolex 2009/84, 234 = ZIK 2010/55, 39; 12.11.2009, 6 Ob 156/09y, jusIT 2010/12, 25 (*Kastelitz/Leiter*) = ÖBA 2010/1618, 253 = RdW 2010/308, 289; 17.12.2009, 6 Ob 41/09m, jusIT 2010/48, 115 (*Kastelitz/Leiter*) = lex:itec 2010 H 3, 50; 17.12.2009, 6 Ob 247/08d, ZFR 2010/82, 141 = jusIT 2010/49, 117 (*Kastelitz/Leiter*) = RdW 2010/306, 288; 19.5.2010, 6 Ob 2/10b, jusIT 2010/70, 148 (*Kastelitz/Leiter*).

43 BGBl 532/1993 idF BGBl I 108/2007.

Gemäß § 39 Abs 2b BWG haben die Verfahren gemäß § 39 Abs 2 BWG insbesondere das Kreditrisiko zu berücksichtigen.

Nach Ansicht der Höchstrichter deckt diese gesetzliche Bestimmung lediglich einen Eingriff in die geschützte datenschutzrechtliche Position des Kunden bzw. Kreditnehmers ab, indem schutzwürdige Geheimhaltungsinteressen bei der Verwendung nicht-sensibler Daten demgemäß nach § 8 Abs 1 Z 4 DSG wegen überwiegender berechtigter Interessen des Auftraggebers (hier Kreditinstitut) nicht verletzt werden. Damit liegt ein Rechtfertigungsgrund in bestimmte bonitätsrelevante Datenverarbeitungen bzw. Datenanwendungen vor.

Keineswegs ermöglicht diese Bestimmung jetzt doch im Sinne einer gesetzlichen Anordnung die Aufnahme von bestimmten bonitätsrelevanten personenbezogenen Daten in ein Informationsverbundsystem im Sinne des § 4 Z 13 iVm § 50 DSG, wie es die Warnliste der österreichischen Kreditinstitute darstellt. Damit sind insoweit die Voraussetzungen für eine erfolgreiche Geltendmachung des Widerspruchsrechts durch den Betroffenen der bonitätsrelevanten personenbezogenen Daten im konkreten Fall gegeben.

(2) Das zivile Höchstgericht[44] definiert die „öffentlich zugängliche Datei" nach § 28 Abs 2 DSG als eine Datei,[45] die einem nicht von vornherein bestimmten, nicht nach außen hin begrenzten Personenkreis zugänglich gemacht wird und der Zugang zur Datei nur von der Entscheidung des Auftraggebers über das ausreichende „berechtigte Interesse" des Abfragenden abhängig ist. Damit folgen die Höchstrichter insoweit der bisherigen Spruchpraxis der Datenschutzkommission,[46] wonach allein das Bestehen einer Kostenpflicht für eine Abfrage sowie das Erfordernis, sich zum Nachweis der entrichteten Entgelte zu identifizieren, die öffentliche Zugänglichkeit einer Datei nicht aufzuheben vermag.

Bemerkenswerterweise bedeutet diese Auffassung, dass damit nahezu jede (elektronisch geführte) Wirtschaftsdatenbank eine öffentlich zugängliche Datei iS des § 4 Z 6 DSG ist. Dies zeigt schon der Umstand, dass auch die Abfrage aus dem Grundbuch, dem Musterbeispiel einer öffentlich zugänglichen Datei,[47] kostenpflichtig ist.[48] Für die Aufnahme in die Wirtschaftsdatenbank der beklagten Auskunftei existiert keine gesetzliche Anordnung, sodass der Anwendungsbereich des – ohne Begründung – wirksamen Widerspruchsrechts nach § 28 Abs 2 DSG eröffnet ist.

(3) Der in § 28 Abs 2 DSG idF vor der DSG-Novelle 2010[49] verwendete Begriff der „**Datei**" ist nicht nur unglücklich gewählt, sondern durch die Rechtsprechung aller drei Höchstgerichte[50] zu § 4 Z 6 DSG auf eine strukturierte Sammlung von

---

44 OGH 12.11.2009, 6 Ob 156/09y, jusIT 2010/12, 25 (*Kastelitz/Leiter*) = ÖBA 2010/1618, 253 = RdW 2010/308, 289.

45 Zu dem nicht unumstrittenen Begriff der „Datei" siehe gleich unten Pkt (3).

46 Deutlich niedergelegt in der Empfehlung DSK 29.11.2005, K211.593/0011-DSK/2005, RIDA0157384.

47 Vgl. § 7 GBG, § 6 Abs 1 GUG.

48 Vgl. TP 9 lit d GGG samt Anm 15.

49 BGBl I 2009/133 in Kraft seit 01.01.2010.

50 Jüngst VwGH 23.11.2009, 2008/05/0079; OGH 28.6.2000, 6 Ob 148/00, RdW 2000/727, 736 = EvBl 2001/1, 17 = ZVR 2001/31, 118 = JUS Z/3065 = KRSlg 2001/1775 = SZ 73/105; VfGH 15.12.2005, B 1590/03, ecolex 2006, 339 = ZfVB 2006/1816/1827 = VfSlg 17.745.

Daten in papierloser Form reduziert. Der Novellengesetzgeber hat den Begriff nunmehr durch den umfassenderen Begriff der „**Datenanwendung**" iS des § 4 Z 7 DSG in § 28 Abs 2 DSG ersetzt. Dies führt zu weitreichenden Änderungen des Anwendungsbereichs. Nach den Gesetzesmaterialien[51] soll *„durch die Verwendung des Begriffs „Datenanwendung" gewährleistet werden [...], dass auch etwa bei Internetanwendungen, bei denen über die Dateieigenschaft Unklarheit besteht, das Recht auf Widerspruch geltend gemacht werden kann."*

Dadurch wird die Möglichkeit eröffnet, Widerspruch gegen Inhalte in nicht gesetzlich angeordneten Onlinepublikationen jeglicher Art wie z.B. Internetforen,[52] Bewertungsplattformen, Onlinearchiven etc. zu erheben, sofern diese öffentlich zugänglich sind (was im Internet den Regelfall darstellt) und personenbezogene Daten des Betroffenen verwenden. Dadurch eröffnet sich in Zukunft noch verstärkter als bisher ein Feld der Interessenabwägung des in das Belieben des Betroffenen gestellten[53] Widerspruchsrechts des § 28 Abs 2 DSG mit dem Medienprivileg des § 48 DSG[54] einerseits sowie der verfassungsrechtlich verankerten Meinungsäußerungs- und Pressefreiheit andererseits.

Nach bislang gefestigter Rsp kann ein datenschutzrechtlicher Widerspruch nach § 28 Abs 2 DSG auch gegen die Aufnahme in eine „öffentliche zugängliche Datei" erhoben werden, in die lediglich Personen Einsicht nehmen können, die dafür an den Datenbankbetreiber bezahlt haben.

3. Verfeinerung der Rsp zum Widerspruchsrecht

In einem weiteren Urteil[55] hat das zivile Höchstgericht – entgegen mancher Stimmen[56] – keine Judikaturänderung zur Geltendmachung des Widerspruchsrechts nach § 28 Abs 2 DSG gegenüber Bonitätsdatenbankbetreibern,[57] sondern vielmehr eine **differenzierende Fortentwicklung** vorgenommen. Die Höchstrichter betonen darin ausdrücklich, dass nach „mittlerweile gefestigter Rechtsprechung" für die öffentliche Zugänglichkeit einer Datei nicht erforderlich ist, dass „jedermann" im wörtlichen Sinne Einsicht in eine bestimmte Datei nehmen kann; es reicht vielmehr aus, dass es einen entsprechend großen Kreis von Abfrageberechtigten gibt und das berechtigte Interesse an der Einsichtnahme im Einzelfall nicht überprüft wird.[58]

Bonitätsdatenbanken sind auch nach dem vorliegenden Urteil grundsätzlich

---

51 ErlRV 472 BlgNR 24. GP 11.

52 Vgl. dazu OLG Linz 16.7.2009, 3 R 101/09g – *www.parents.at*, jusIT 2010/13, 26 (krit *Jahnel*) = MR 2009, 306 (krit *Koukal*).

53 OGH 1.10.2008, 6 Ob 195/08g, jusIT 2009/14, 28 (*Dörfler*) = EvBl-LS 2009/33, 233 = RdW 2009/172, 208 = ÖBA 2009/1549, 395.

54 Ausführlich dazu auch im Lichte der EuGH-Rsp *Jahnel,* Publizistische Tätigkeit und Datenschutzrecht, in *Jahnel* (Hg), Jahrbuch Datenschutzrecht und E-Government 2009 (2009), 79 mwN.

55 OGH 17.12.2009, 6 Ob 41/09m, jusIT 2010/48, 115 (*Kastelitz/Leiter*); dazu *Thiele*, Eingeschränktes Widerspruchsrecht gegen Bonitätsdatenbanken, lex:itec 2010 H 3, 50.

56 Nachweise zum „Medienrummel" bietet die ARGE Daten unter http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=29161uph (08.02.2011).

57 Statt vieler dazu *Jahnel*, Datenschutzrecht Rz 7/82 ff.

58 OGH 1.10.2008, 6 Ob 195/08g, jusIT 2009/14, 28 (*Dörfler*) = EvBl-LS 2009/33, 233 = RdW 2009/172, 208 = ÖBA 2009/1549, 395 = ecolex 2009/84, 234; 12.11.2009, 6 Ob 156/09y, jusIT 2010/12, 25 (*Kastelitz/Leiter*).

„öffentlich zugänglich" iS der § 28 Abs 2 DSG. Jeder Betroffene kann daher Widerspruch gegen die Verwendung seiner Daten erheben. Dieser Widerspruch führt dazu, dass die Daten des Betroffenen aus den insbesondere via Internet oder sonst online zugänglichen Datenbanken zu löschen sind. Nicht zu löschen sind die Daten hingegen aus den **besonders zugangs- und auskunftsgeschützten Datenbanken** der Kreditauskunfteien. Die Übermittlung der Daten an identifizierte Kunden ist dann rechtmäßig, wenn vor Übermittlung im Einzelfall das berechtigte Interesse des Anfragers geprüft und zumindest bescheinigt worden ist, dass der behauptete Abfragezweck bzw. die Weitergabe einem berechtigten Interesse, z.B. auf Durchsetzung von Ansprüchen, der Identitätsprüfung oder sonstigen rechtlich geschützten Interessen dient.

Das vorliegende Urteil legitimiert bis zu einem gewissen Grad die gängige Praxis, dass Kreditauskunfteien sich von ihren (identifizierten) Kunden vertraglich zusichern lassen, dass diese nur bei Vorliegen eines berechtigten Interesses (typischerweise Verträge mit Kreditelementen) Daten abfragen und übermitteln. Darüber hinaus erfordert eine auch gegenüber dem Widerspruch nach § 28 Abs 2 DSG bestandskräftige Datenverwendung eine individuelle „Handprüfung" des Interesses im Einzelfall. Es bleibt abzuwarten, inwieweit sich die österreichischen Auskunfteien auf diese Judikaturentwicklung einstellen werden.

Der OGH[59] hat in Verfeinerung seiner bisherigen Rsp zum datenschutzrechtlichen Widerspruch gegen Eintragungen in Bonitätsdatenbanken entschieden, dass eine Auskunftei dann zulässigerweise Daten verarbeitet, wenn durch erhebliche Einschränkungen des Zugangs sichergestellt ist, dass Bonitätsinformationen nur identifizierten Kunden gegeben werden, die in jedem Einzelfall der Datenabfrage eine Glaubhaftmachung des Abfragezwecks und der weiteren Verwendung verlangt. Bei Nachweis des rechtlichen Interesse durch denjenigen, der eine Auskunft begehrt, dürfen damit Daten von Personen, die einer Aufnahme in die Bonitätsdatenbank gemäß § 28 DSG widersprochen haben, auch weiterhin gespeichert und bei entsprechendem Nachweis an Dritte weitergeben werden.

4. Löschung nach Widerspruch

In seiner Löschungsanordnung verfestigt der OGH seine bisherige Rsp[60], nach der es nicht genügt, die Datenorganisation so zu verändern, dass ein „gezielter Zugriff" auf die betreffenden Daten ausgeschlossen ist, um das Löschungsgebot nach dem DSG 2000 zu erfüllen.[61]

Abschließend ist an der vorliegenden Entscheidung pro futuro bemerkenswert, dass die Verletzung von höchstpersönlichen Rechten, einer Bewertung durch Geld unzugänglich ist. Demzufolge hat insoweit ein Bewertungsausspruch in der zweiten Instanz zu entfallen und eine bleibt die volle Anrufung des OGH bleibt bei Streitigkeiten nach dem DSG nach wie vor erhalten.[62]

---

59 OGH 17.12.2009, 6 Ob 41/09m, jusIT 2010/48, 115 (*Kastelitz/Leiter*); dazu *Thiele*, Eingeschränktes Widerspruchsrecht gegen Bonitätsdatenbanken, lex:itec 2010 H 3, 50.

60 OGH 15.4.2010, 6 Ob 41/10p – *Datenlöschung*, jusIT 2010/69, 146 (*Kastelitz/Leiter*).

61 Dazu *Thiele*, Löschen heißt Vernichten, lex:itec 2010/4, 20.

62 Ebenso OGH 20.4.2010 4 Ob 43/10t, EvBl-LS 2010/135 = ÖBl-LS 2010/161; **aA** noch OGH 14.1.2010, 6 Ob 2/10b, Zulassungsentscheidung zu OGH 15.4.2010, 6 Ob 41/10p – *Datenlöschung*, jusIT 2010/69, 146 (*Kastelitz/Leiter*).

§ 39 Abs 2 BWG stellt keine gesetzliche Anordnung im Sinne des § 28 Abs 2 DSG idF vor dem Verbraucherkreditgesetz, BGBl I 2010/28, dar. Nach nunmehr gültiger Rechtslage scheidet jedoch eine Anwendung des Widerspruchsrechtes nach § 28 Abs 2 DSG gegenüber den in die Warnliste der österreichischen Kreditinstitute eingemeldeten bonitätsrelevanten personenbezogenen Daten aus.

Im Falle einer wirksamen Widerspruchsverpflichtung ist eine Löschungsverpflichtung durch physische Löschung der Daten, nicht bloß durch eine Sperre zu vollziehen.

D. Geänderte Rechtslage ab dem 11.06.2010

Die Höchstrichter erwähnen ausdrücklich, dass auf den vorliegenden Fall die erst nach Schluss des Verfahrens erster Instanz in Kraft getretene Änderung der Gesetzeslage durch § 7 Abs 5 VerbrKG (Verbraucherkreditgesetz) nicht anzuwenden ist.

§ 7 Abs 5 VKrG lautet: *„§ 28 Abs 2 des Datenschutzgesetzes 2000 – DSG 2000, BGBl I Nr 165/1999 in der jeweils geltenden Fassung, ist auch bei der Datenschutzkommission registrierte Informationssysteme kreditgebende Institutionen zur Bonitätsbeurteilung, bei den die Verwendung auf § 8 Abs 1 Z 2 oder Z 4 DSG beruht, nicht anzuwenden."*[63] Nach dem eindeutigem Wortlaut dieser Bestimmung wäre also der vorliegende Unterlassungs- und Löschungsanspruch abzuweisen gewesen, da die Warnliste der österreichischen Kreditinstitute bei der Datenschutzkommission als Informationsverbundsystem registriert ist, und nach den klaren Worten des OGH die Datenverwendung auf § 8 Abs 1 Z 4 DSG beruht.[64]

VIII. Unzulässigkeit des Rechtsweges (Auftraggeber des öffentlichen Rechts; Gesundheitsdaten; Verletzung des Rechts auf Geheimhaltung)

8.1. Der Kläger stand in einem öffentlich-rechtlichen Dienstverhältnis zur erstbeklagten Partei, der Stadt Wien, und war aufgrund des Wiener ZuweisungsG[65] für Bedienstete der Wiener Stadtwerke der zweitbeklagten Partei, der Wiener Linien GmbH & Co KG, zugeteilt, die für den öffentlichen Personenverkehr verantwortlich ist. Er befand sich seit Februar 2008 im Krankenstand. Im Rahmen einer direktionsärztlichen Untersuchung zur Überprüfung seiner Dienstfähigkeit wurde die zuständige Direktionsärztin angewiesen, sämtliche Krankheitsdaten (insbesondere Diagnose und Medikation) der Personalabteilung der Zweitbeklagten mitzuteilen. Darüber hinaus wurden die Krankendaten des Klägers auch an seinen Vorgesetzten weitergegeben und der Krankenakt dem Personalakt des Klägers angeschlossen; auch das das Sekretariat des direktionsärztlichen Büros hatte von den sensible Gesundheitsdaten Kenntnis gehabt.

---

63 BGBl I 2010/28 in Kraft seit 11.6.2010.

64 Vgl. DSK 32.111.2001 K095.014/021 DSK 2001, RIDA-Nr. 0151021.

65 Gesetz über die Zuweisung von Bediensteten der Wiener Stadtwerke, Wr LGBl 17/1999 idgF.

Der Kläger begehrte unter Berufung auf die Verletzung seines Rechts auf Geheimhaltung von beiden Beklagte die Unterlassung, vom Direktionsarzt oder dessen Mitarbeitern erfasste Gesundheitsdaten an Dritte, insbesondere andere Mitarbeiter der Beklagten ohne Zustimmung des Klägers weiterzugeben, wenn die Weitergabe nicht zum Zweck der Koordination des Personaleinsatzes oder zur Beurteilung der Dienstfähigkeit erforderlich war und es sich um Angaben handelte, die über den Beginn, die Dauer und die Ursache der Arbeitsunfähigkeit hinausgingen. Bei der Zweitbeklagten handelte es sich um einen Auftraggeber des privaten Bereichs; die Erstbeklagte hätte dafür einzustehen, weil sich ja an deren Haftung und der dienstrechtlichen Stellung des Klägers durch die Zuweisung nichts geändert hätte. Die Beklagten erhoben die Einrede der Unzulässigkeit des Rechtswegs, aber auch der sachlichen Unzuständigkeit des Arbeits- und Sozialgerichts Wien.

Das Erstgericht wies die Klage wegen Unzulässigkeit des ordentlichen Rechtswegs zurück; das Berufungsgericht bestätigte diese Entscheidung lediglich für die erstbeklagte Partei und verwarf jedoch die Einrede der Unzulässigkeit des Rechtswegs hinsichtlich der zweitbeklagten Partei. Letztlich hatte sich der OGH – soweit ersichtlich erstmals – mit der Frage der Zulässigkeit des Rechtswegs im Zusammenhang mit zugewiesenen Beamten und deren auf das Datenschutzgesetz gestützten Ansprüchen zu befassen.

8.2. Die Höchstrichter bestätigten die Zurückweisung der Klage in vollem Umfang. Sie stellten das Ersturteil wieder her und führten aus, dass die Stadt Wien in Form des öffentlichen Rechts als Gebietskörperschaft eingerichtet war und damit kein privater Rechtsträger iS des § 1 Abs 5 DSG vorlag, für den der Rechtsweg zum Schutz von Rechten nach dem Datenschutzgesetz zulässig wäre.[66] Auch der klägerische Hinweis auf die Verletzung der Fürsorgepflicht des Arbeitgebers ginge fehl, da Streitigkeiten aus dem öffentlichen Dienstverhältnis grundsätzlich im Verwaltungsweg auszutragen waren. Das galt auch für die gegenüber der zweitbeklagten Partei erhobenen Ansprüche, da es sich insoweit ebenfalls um Streitigkeiten aus dem öffentlich-rechtlichen Dienstverhältnis von Beamten handelte.

8.3. Muss der Betroffene seine Rechte nach den §§ 27 ff DSG durchsetzen, so spielt es eine entscheidende Rolle, ob der Auftraggeber iS des § 4 Z 1 DSG dem **öffentlichen** oder dem **privaten Bereich** zuzurechnen ist. Auftraggeber des öffentlichen Bereichs sind nach § 5 Abs 1 und 2 DSG alle Auftraggeber, die in Formen des öffentlichen Rechts eingerichtet sind (zB eine Gemeinde, Bezirksverwaltungsbehörden, der Landeshauptmann, Minister, Sozialversicherungsträger oder die Kammern), alle anderen sind Auftraggeber des privaten Bereichs (zB natürliche Personen, OG, KG, GmbH, AG oder Vereine).[67] Nach der Spruchpraxis zählen aber auch die Österreichische Forschungsgesellschaft[68] oder eine KrankenanstaltengmbH als Betreiberin eines öffentlichen Landeskrankenhauses[69] zu den privaten Auftraggebern.

---

66 Zu Abgrenzungsfragen siehe *Jahnel*, Datenschutzrecht Rz 3/37 ff mwN.

67 Zu den weiteren Folgen der Unterscheidung siehe *Jahnel*, Datenschutzrecht Rz 3/154.

68 DSK 21.6.2005, K120.996/0006-DSK/2005, RIDA 0151411.

69 DSK 27.4.2007, K121.283/0005-DSK/2007, RIDA 0191031.

Für Verletzungen des **Rechts auf Auskunft** ist die DSK sowohl im öffentlichen als auch im privaten Bereich, d.h. nach § 1 Abs 5 DSG stets zuständig. Die Datenschutzkommission ist eine kollegiale Sonderbehörde, die nach den §§ 35 ff DSG in Form eines unabhängigen Tribunals eingerichtet ist, das auch über bestimmte Kontrollbefugnisse verfügt, wie z.B. Zutritts- und Nachschaurechte (vgl. § 30 DSG). Die DSK hat folgende wesentliche Befugnisse:

- **Empfehlungen** an Auftraggeber:[70] die Nichteinhaltung kann zur Überprüfung und Entzug der Registrierung oder Klage führen.[71]
- Anzeige strafbarer Datenmissbräuche nach §§ 51, 52 DSG
- im privaten Bereich selbst Klage beim zuständigen Gericht gegen rechtsverletzende Auftraggeber erheben
- **Vorabkontrolle**, d.h. vor Aufnahme einer Datenanwendung, nach den §§ 10, 18 Abs 2, 20, 21, 30 DSG: bestimmte Datenanwendungen, wie z.B. solche mit sensiblen Daten. Eine Prüfung ist auch ohne Verdachtsmomente möglich; Auflagen können erteilt werden, Dienstleister sind zu melden (z.B. Videoüberwachung).
- **Mandatsbescheid**: zur vorbeugenden Unterlassung einer Datenanwendung, z.B. Liste zahlungsunwilliger Konsumenten im Internet,[72] mit DSK-internem Rechtszug.

Für Verletzungen des **Rechts auf Geheimhaltung**[73] nach § 1 DSG, **Richtigstellung oder Löschung** ist die DSK dann zuständig, wenn es sich um Auftraggeber des öffentlichen Bereichs handelt. Handelt es sich um Auftraggeber des privaten Bereichs, ist die Verletzung mit Klage bei dem für den Betroffenen zuständigen Landesgericht nach § 32 Abs 4 DSG geltend zu machen. Nach § 32 Abs 3 DSG besteht die Möglichkeit der Erlassung einstweiliger Verfügungen ohne Gefahrenbescheinigung.

8.4. Nach zutreffender Rechtsansicht ist zur Entscheidung über die konkret behauptete Verletzungen der Rechte eines öffentlich-rechtlicher Bediensteten auf Geheimhaltung, Richtigstellung oder Löschung seiner medizinischen Daten durch die Stadt Wien, die ihn als Dienstgeber nach dem WrZuweisungsG an die privat organisierten Wiener Linien abgestellt hat, die DSK nach § 31 Abs 2 DSG berufen. Die ordentlichen Gerichte sind deshalb nicht zuständig, da insoweit die Gebietskörperschaft nach wie vor gemäß § 5 Abs 2 DSG als Auftraggeber des öffentlichen Rechts gilt. Mangels Zulässigkeit des Rechtswegs ist die Unterlassungsklage daher zurück zuweisen.

---

70 DSK 29.9.2006, K213.000/0005-DSK/2006, RIDA 0169644: Speicherung von Verkehrsdaten; dazu *Leitner*, Speicherung dynamisch vergebener IP-Adressen. Datenschutzrechtlich nur bedingt zulässig, lex:itec 2006 H 5, 23.

71 DSK 29.11.2005, K211.593/0011-DSK/2005, RIDA 0157384: Auskunftssperre einer Wirtschaftsdatenbank.

72 DSK 20.1.2004, K211.505/002-DSK/2004, RIDA 0199095.

73 Vgl. OGH 3.9.2002, 11 Os 109/01, EvBl 2003/14, 69 = JUS St/3245 = SSt 64/48: Amtsmissbrauch und Verletzung des Datenschutzes durch missbräuchliche Datenabfrage durch Revierinspektor; DSK 1.3.2005, K120.817/0005-DSK/2005, RIDA 0154202: Weitergabe von Einkommensdaten aus Nebentätigkeiten eines Universitätsangehörigen an Medien ist unzulässig, auch wenn Daten aus der beruflichen Tätigkeit eines öffentlich-rechtlichen Bediensteten nicht unter Datenschutz fallen (§ 8 Abs 3 Z 6 DSG).

IX. Zusammenfassung

Die ausdifferenzierte Judikatur des OGH zum Widerspruchsrecht gegenüber Bonitätsdatenbanken, die im 1. Oktober 2008 ihren Anfang nahm, hat im Jahr 2010 ihren (vorläufigen) Abschluss gefunden. Die für viele allzu großzügige Anwendung des begründungslosen Widerspruchs nach § 28 Abs 2 DSG verbunden mit einer physisch zu verstehenden Löschungsverpflichtung haben letztlich wohl zu einer bedeutsame Gesetzesänderung durch das Verbraucherkreditgesetz (VerbrKrG)[74] geführt. § 7 Abs 5 VerbrKrG nimmt mit Wirksamkeit vom 11. Juni 2010 bei der Datenschutzkommission registrierte Informationsverbundsysteme kreditgebender Institutionen zur Bonitätsbeurteilung, wie z.B. die Warnliste der Banken[75] aus dem Anwendungsbereich des Widerspruchs nach § 28 Abs 2 DSG generell aus.

Damit nimmt der Gesetzgeber in Kauf, dass manche Bonitätsdatenbanken „einen bevorzugten Status haben", was dem Nutzer und den Betroffenen den Überblick jedenfalls kaum erleichtern wird. In Wahrheit sind Informationsverbundsysteme öffentlicher zugänglich als Datenbanken nur eines Auftraggebers, jedenfalls wenn der Rechtsanwender die Ansicht des Höchstgerichtes teilt, dass nicht der Empfänger der Übermittlung die Entscheidung darüber treffen soll, ob ein berechtigtes Interesse an der Übermittlung besteht, sondern der Übermittelnde. Einen solchen vom Empfänger verschiedenen Auftraggeber gibt es nämlich beim Informationsverbundsystem nicht.

Die weitere Entwicklung bleibt abzuwarten, aber jedenfalls spannend.

74 BGBl I 2010/28 in Kraft seit 11.6.2010.

75 Vgl. DSK 23.11.2001, K095.014/021-DSK/2001, RIDA-Nr 0151021; 21.3.2007, K600.014-010/0002-DVR/2007, RIDA-Nr 0191034.