Datenschutz im Verfassungsrecht

Andreas Lehner / Konrad Lachmayer

Literatur: *Dohr/Pollierer/Weiss*, DSG[2] § 1; *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000) 97; *Duschanek*, § 1 DSG in Korinek/Holoubek (Hrsg), Bundesverfassungsrecht (2005); *Jahnel*, Das Grundrecht auf Datenschutz nach dem DSG 2000, in FS Schäffer (2006) 313; *Kunnert*, Der Ministerialentwurf für eine DSG Novelle 2010, jusIT 2009, 102; *Lehner*, Das Grundrecht auf Datenschutz, in Heißl (Hrsg), Handbuch Menschenrechte (2009) 211; *Rill*, Das Grundrecht auf Datenschutz, in Duschanek (Hrsg), Datenschutz in der Wirtschaft (1981) 15; *Wiederin*, Privatsphäre und Überwachungsstaat (2003) 57ff; *ders*, Schutz der Privatsphäre, in Merten/Papier (Hrsg), Handbuch der Grundrechte. Grundrechte in Österreich (2009) 175, 221.

Rechtsgrundlagen: Art 1, §§ 35, 37, 38, 61 Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000), BGBl I 1999/165 idgF.

Rechtsprechung: VfSlg 12.166/1989 (Datenübermittlung im Verwaltungsverfahren); 12.228/1989 (Statistik – Wirtschaftsdaten); 12.768/1991 (Richtigstellung und Löschung); 15.130/1998 (Ärztehonorare – Rechnungshof); 16.150/2001 (Interessenabwägung bei Löschung); 16.369/ 2001 (Telekom-Control); 16.467/2002 (Gebietskrankenkasse – Ärztekammer); 17.065/2003 (ORF-Bezüge); 16.986/2003 (Ausschluss des Auskunftsrechts im SPG); 17.745/2005 (Löschung von Daten im SPG); 17.940/2006 (Beitragseinhebung – Sozialversicherungsanstalt); 15.06.2007, G147/06 ua (Section Control); 2.10.2007, B227/05 (Herold Business Data); 7.3.2007, B1708/06 (Löschung – Papierakt).

DSK 13.6.1991, 195.007, ZfVB 1997, 289 (Private Lebensgestaltung); 19.3.1997, 120.512, ZfVB 1997, 565 (Direkte Befragung vor Ermittlung); 5.10.1999, 120.667/8-DSK/99 (Geisteskrankenevidenz); 18.5.2000, 120.686/3-DSK/00 (Waffenverbot); 10.11.2000, 120.707/7-DSK/00 (Löschung aus manueller Datei); 14.9.2001, K120.705/010-DSK/2001 (Wesentlichkeitsgrundsatz); 4.5.2002, K120.766/004-DSK/2002 (Führerschein); 21.1.2003, K120.757/001-DSK/2003 (Amtsarzt – AHS-Lehrer); 27.2.2004, K120.867/0001-DSK/2004 (Veröffentlichung im Internet).

OGH 26.8.1999, 2 Ob 244/99t (Kundendaten); 28.6.2000 6 Ob 162/00t (Offenlegungspflichten); 22.3.2001, 4 Ob 28/01y (Bank – AGB); 3.9.2002, 11 Os 109/01 (verdeckter Ermittler); 20.3.2007, 4 Ob 221/06p (Kreditvertragsformulare).

I. Einleitung

Die verfassungsrechtlichen Dimensionen des Datenschutzes liegen primär im Grundrecht auf Datenschutz (II.), durch das ein breiter Schutz des Einzelnen sowohl gegenüber dem Staat als auch Privaten gewährleistet wird. In diesem Sinne soll auch das Hauptaugenmerk dieser Ausführungen beim Grundrecht auf Datenschutz liegen.

Neben der Facette des Grundrechts auf Datenschutz stehen aber auch unterschiedliche andere Regelungen im Rahmen des DSG im Verfassungsrang. Dabei ist vor allem auf die kompetenzrechtlichen Tatbestände (III.) und die speziellen organisationsrechtlichen Bestimmungen zur DSK (IV.) einzugehen. Letztlich sollen aber auch alle sonstigen Verfassungsbestimmungen im datenschutzrechtlichen Kontext (V.) kurz beleuchtet werden.

II. Grundrecht auf Datenschutz

Dieses Kapitel wurde von *Andreas Lehner* bereits (nahezu wortgleich) publiziert. Vgl *Lehner*, Grundrecht auf Datenschutz, in *Heißl* (Hrsg), Handbuch Menschenrechte (2009) 211ff.

A. Einleitung

Durch die zunehmende Vereinfachung der Datenerfassung und -verarbeitung und der damit verbundenen zunehmenden Verbreitung von Datenverwendungen kommt dem Grundrecht auf Datenschutz eine stetig steigende Bedeutung zu. Dies findet auch in der Spruchtätigkeit des VfGH Niederschlag. Lag die Zahl der datenschutzrechtlichen Entscheidungen von 1983 bis 1999 noch bei knapp über zehn, so gab es seit dem Jahr 2000 bereits an die 40 Erkenntnisse und Beschlüsse zum Grundrecht auf Datenschutz. Dass es vor 1983 keine Entscheidungen gab, liegt daran, dass das Grundrecht auf Datenschutz gemeinsam mit dem DSG 1978 erst am 1.1.1980 in Kraft getreten ist. Verglichen mit den Garantien des Staatsgrundgesetzes von 1867 oder auch mit jenen der EMRK von 1958, handelt es sich also um ein sehr junges Grundrecht, zu dem es noch relativ wenig höchstgerichtliche Judikatur gibt.

Datenverwendungen können auch einen Eingriff in den Schutzbereich des **Rechts auf Privatleben** gemäß Art 8 EMRK darstellen, die beiden Rechte können aber keinesfalls gleichgestellt werden. Die Schutzbereiche haben zwar eine gemeinsame Schnittmenge, sind aber nicht deckungsgleich. So bezieht sich das Grundrecht auf Datenschutz nur auf den Schutz personenbezogener Daten, nicht aber auf andere Aspekte des Persönlichkeitsschutzes. Im Hinblick auf diese Daten besteht der Schutz jedoch auch für juristische Personen und unabhängig davon, ob die Verwendung der Daten einen besonders privaten Lebensbereich betrifft oder nicht.

Eine Besonderheit des Grundrechts auf Datenschutz ist seine **unmittelbare Drittwirkung**. Es ist das einzige verfassungsgesetzlich gewährleistete Recht, das seinen Schutz nicht nur gegenüber staatlichen Eingriffen entfaltet, sondern auch gegenüber Privatpersonen wirkt und diesbezüglich auch vor den ordentlichen Gerichten geltend gemacht werden kann.

Das Grundrecht auf Datenschutz umfasst vier Garantien: das Recht auf Geheimhaltung personenbezogener Daten, das Recht auf Auskunft über die Verwendung personenbezogener Daten, das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässig verarbeiteter Daten.

B. Recht auf Geheimhaltung

1. Struktur

Gemäß § 1 Abs 1 DSG hat jede oder jeder **Anspruch auf Geheimhaltung** der sie oder ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Abs 2 leg cit bestimmt, dass, soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse der

betroffenen Person oder mit ihrer Zustimmung erfolgt, Beschränkungen dieses Anspruchs nur zur Wahrung überwiegender berechtigter Interessen einer anderen Person zulässig sind. Eingriffe einer staatlichen Behörde sind nur aufgrund von Gesetzen statthaft, die aus den in Art 8 Abs 2 EMRK genannten Gründen notwendig sind. Die behördliche Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, darf nur aufgrund von Gesetzen zum Schutz wichtiger öffentlicher Interessen stattfinden, wobei diese Gesetze gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festzulegen haben. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten zum Ziel führenden Art vorgenommen werden.

Während § 1 Abs 1 DSG den Schutzbereich des Grundrechts umschreibt, legt Abs 2 fest, unter welchen Bedingungen Eingriffe in diesen Schutzbereich **gerechtfertigt** sind. Daraus ergeben sich unterschiedliche Anforderungen je nachdem, ob der Eingriff durch den Gesetzgeber, eine staatliche Behörde oder eine Privatperson erfolgt. Der Gesetzgeber darf nur Eingriffe vorsehen, wenn diese entweder mit Zustimmung der betroffenen Person, zum Schutz ihrer lebenswichtigen Interessen oder zum Schutz von überwiegenden berechtigten Interessen anderer erfolgt. Sieht das Gesetz Eingriffe durch Private vor, so reicht es, wenn einer dieser Rechtfertigungsgründe vorliegt und das Gesetz verhältnismäßig ist. Sieht das Gesetz aber Eingriffe durch eine Behörde vor, so muss dieses Gesetz der nationalen Sicherheit, der öffentlichen Ruhe und Ordnung, dem wirtschaftlichen Wohl des Landes, der Verteidigung der Ordnung und der Verhinderung von strafbaren Handlungen, dem Schutz der Gesundheit und der Moral oder dem Schutz der Rechte und Freiheiten anderer dienen. Sollen besonders schutzwürdige Daten verwendet werden, so muss das Gesetz einem wichtigen öffentlichen Interesse dienen und zusätzlich angemessene Garantien zum Schutz der Geheimhaltungsinteressen der Betroffenen vorsehen. Auch diese eingriffsermächtigenden Gesetze müssen dem Grundsatz der Verhältnismäßigkeit entsprechen.

Eine **staatliche Behörde** darf nur dann in das Grundrecht eingreifen, wenn der Eingriff mit Zustimmung des Betroffenen oder zum Schutz seiner lebenswichtigen Interessen erfolgt oder der Eingriff auf ein Gesetz gestützt werden kann. Auf ein Gesetz kann ein gerechtfertigter Eingriff nur gestützt werden, wenn dieses in denkmöglicher Weise angewendet wird und nicht verfassungswidrig ist. Die Behörde hat bei der Auswahl der eingreifenden Mittel darauf zu achten, jenes Mittel einzusetzen, das am gelindesten in die Rechtssphäre der betroffenen Person eingreift.

Privatpersonen dürfen in das Grundrecht eingreifen, wenn dies mit der Zustimmung der betroffenen Person bzw zum Schutz ihrer lebenswichtigen Interessen geschieht. Eingriffe sind aber auch dann zulässig, wenn Eingreifende zum Schutz überwiegender berechtigter Interessen handeln.

2. Schutzbereich

a) „Jedermann“

Jedermann hat Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten. Mit „jedermann“ ist jede **natürliche und juristische**

Person gemeint. Verstorbene sind vom Schutzbereich ebenso wenig erfasst wie Einheiten, denen keine Rechtspersönlichkeit zukommt. Auch juristische Personen des öffentlichen Rechts genießen Rechtsschutz.[1]

b) Geheimhaltung

Der Anspruch auf Geheimhaltung umfasst das Recht, dass keine Daten an Dritte **übermittelt**[2] werden und Daten nicht von Dritten **ermittelt**[3] werden. Auch die **strukturierte Evidenthaltung** von personenbezogenen Daten greift in den Schutzbereich des Grundrechts auf Geheimhaltung ein.[4] Unbedeutend ist die Art und Weise, auf die Daten ermittelt, übermittelt bzw aufbewahrt werden. Eingriffe sind also nicht nur durch elektronische Verarbeitung, sondern auch durch Niederschriften, gesprochene Mitteilungen oder andere konventionelle Formen der Datenverwendung möglich.

c) Personenbezogene Daten

Unter einem personenbezogenen Datum ist jede Information zu verstehen, die mit einer **bestimmten oder bestimmbaren Person** verknüpft ist. Dabei ist irrelevant, auf welche Weise die Information transportiert wird bzw auf welchem Datenträger sie liegt. Schall kann in Form des gesprochenen Wortes genauso Daten tragen wie elektromagnetische Felder auf Festplatten. Von Bedeutung ist einzig, ob die Information mit einer Person verknüpft bzw verknüpfbar ist. Dies ist dann der Fall, wenn der Personenbezug mit vernünftigen Mitteln hergestellt werden kann. Diese Einschränkung ist deshalb notwendig, da ansonsten jeder Gegenstand, auf dem ein Mensch eine Spur hinterlassen hat, zum Informationsträger und jede Aneignung oder Weitergabe dieses Gegenstandes zum Eingriff in das Grundrecht auf Datenschutz wird. Tatsächlich wird der Gegenstand aber erst dann zum Informationsträger, wenn die Spuren, die eine Person hinterlassen hat, **unter dem Einsatz von vernünftigen Mitteln** mit dieser Person **verknüpfbar** sind.[5]

d) Schutzwürdige Geheimhaltungsinteressen

Der Anspruch auf Geheimhaltung besteht nur insoweit, als die betroffene Person ein schutzwürdiges Geheimhaltungsinteresse hat. Ob dies der Fall ist, ist anhand der gesamten Rechtsordnung zu ermitteln, wobei es nicht notwendig ist, dass das Geheimhaltungsinteresse ausdrücklich durch eine positivrechtliche Bestimmung unter Schutz gestellt wurde.[6] Vielmehr ist davon auszugehen, dass jede natürliche Person grundsätzlich selbst darüber bestimmen darf, welche Informationen sie als Teil ihrer Privatsphäre betrachtet, sodass es für die Schutzwürdigkeit dieser Informationen ausreicht, wenn die betroffene Person die Information für schutzwürdig erachtet und dementsprechend mit dieser Information umgeht.[7] Dabei beschränkt sich der Schutzbereich nicht auf den innersten Kreis einer privaten, der Öffentlichkeit verborgenen Lebensgestaltung.[8] Werden Daten von der betroffenen Person selbst veröffentlicht, weil sie von dieser nicht als „privat" angesehen werden, so werden sie auch von der Rechtsordnung unter keinen besonderen Schutz gestellt. Juristische Personen verfügen über keine Privatsphäre, sodass ein diesbezügliches von der Rechtsordnung anerkanntes Schutzinteresse nicht in Frage kommt. Es gibt aber auch andere Interessen, die für natürliche wie für juristische Personen gleichermaßen schützenswert sind. So sieht die Rechtsordnung an verschiedenen Stellen einen Schutz von Geschäfts- und Betriebsgeheimnissen vor und anerkennt damit, dass marktwirtschaftlich agierende (juristische) Personen ein Interesse daran haben, dass Teile der Unternehmensinformation geheim bleiben.[9]

Gemäß § 1 Abs 1 DSG ist ein schutzwürdiges Geheimhaltungsinteresse jedenfalls dann ausgeschlossen, wenn Daten infolge ihrer **allgemeinen Verfügbarkeit** oder wegen ihrer mangelnden Rückführbarkeit auf die betroffene Person einem Geheimhaltungsanspruch nicht zugänglich sind. Allgemein verfügbar sind Daten nur dann, wenn sie aktuell für jede und jeden verfügbar sind, und nicht etwa schon, wenn sie zu einem früheren Zeitpunkt verfügbar waren, der Zugang zu den Daten aber inzwischen nicht mehr besteht[10] oder der Zugang nur für eine gewisse Gruppe von Personen gegeben ist.[11] Die allgemeine Verfügbarkeit ist als rechtlicher und nicht als faktischer Begriff zu verstehen. Es kommt also darauf an, dass die Allgemeinheit über die Daten verfügen darf,[12] und nicht darauf, dass sie über die Daten verfügen kann. In diesem Sinne sind zB Informationen, die unrechtmäßigerweise veröffentlicht wurden, nicht allgemein verfügbar, während Daten, die etwa die betroffene Person selbst veröffentlicht hat, sehr wohl allgemein verfügbar sind. Es würde dem Schutzgedanken des Grundrechts diametral widersprechen, wenn die Schutzwürdigkeit eines Datums von Dritten beseitigt werden könnte, indem man sie einem möglichst großen Publikum möglichst dauerhaft zur Verfügung stellt. Nur zulässigerweise veröffentlichte Daten können daher allgemein verfügbar sein.[13]

---

1 Organe von Gebietskörperschaften können aber nicht in subjektiven Rechten verletzt werden, weshalb eine Beschwerde nicht auf Art 144 B-VG gestützt werden kann. Siehe VfSlg 17.838/2006.

2 VfSlg 16.467/2002.

3 DSK 5.10.1999, 120.667/8-DSK/99; VfSlg 16.369/2001.

4 DSK 21.1.2003, K120.757/001-DSK/2003.

5 Dazu ausführlicher *Stelzer/Lehner*, Datenschutz in Biobanken, ZfV 2008, 241 (242).

6 So auch *Jahnel*, Das Grundrecht auf Datenschutz nach dem DSG 2000, in FS Schäffer (2006) 323 und *Wiederin*, Privatsphäre und Überwachungsstaat (2003) 60. *Duschanek* meint hingegen mit Verweis auf die Materialien, dass die Schutzwürdigkeit immer vorliegt, wenn nicht eine der beiden expliziten Ausnahmen einschlägig ist. Siehe *Duschanek*, § 1 DSG in Korinek/Holoubek (Hrsg), Bundesverfassungsrecht (2002) Rz 42.

7 Vgl Art 8 EMRK; *Wiederin*, Art 8 EMRK, in Korinek/Holoubek (Hrsg), Bundesverfassungsrecht (2002) Rz 35ff.

8 Vgl DSK 13.6.1991, 195.007, ZfVB 1997, 289.

9 VfSlg 12.228/1989; 16.369/2001.

10 Wenn etwa Daten aus einem öffentlichen Register gelöscht wurden.

11 OGH 3.9.2002, 11 Os 109/01.

12 Wie etwa Daten aus der Ärzteliste, die gemäß § 27 Abs 1 ÄrzteG zu veröffentlichen ist. Vgl auch VfSlg 16.467/2002.

13 So auch *Jahnel*, Das Grundrecht auf Datenschutz nach dem DSG 2000, in FS Schäffer (2006) 321.

Der zweite Fall, bei dem gemäß § 1 Abs 1 DSG die Schutzwürdigkeit fehlt, ist der, bei dem die Information **auf keine Person mehr zurückgeführt** werden kann. Solche Informationen sind jedoch schon nicht vom Datenbegriff umfasst, der ja nur Informationen meint, die mit einer Person verknüpft oder verknüpfbar sind.[14] Ein Anspruch auf Geheimhaltung ist also schon deshalb nicht ableitbar, weil es sich nicht um personenbezogene Daten handelt. Auch indirekt personenbezogene Daten sind vom Grundrecht grundsätzlich erfasst, da auch sie auf eine Person zurückgeführt werden können.[15] Eingriffe durch die Verwendung nur indirekt personenbezogener Daten werden aber leichter zu rechtfertigen sein.

Für die Schutzwürdigkeit des Geheimhaltungsinteresses und damit für die Frage, ob ein Datum vom Schutzbereich des Grundrechts erfasst ist, ist es nicht von Bedeutung, ob dieses Geheimhaltungsinteresse das konkrete Verwendungsinteresse auch überwiegt. Es reicht aus, wenn festgestellt werden kann, dass ein Geheimhaltungsinteresse besteht. Eine Abwägung zwischen verschiedenen Interessen findet auf dieser Ebene nicht statt. Solche überwiegenden Interessen an einer Datenverwendung können nämlich nicht den Schutzbereich des Grundrechts auf Datenschutz einschränken, sondern allenfalls einen Eingriff in diesen rechtfertigen.[16]

3. Eingriffe durch den Gesetzgeber

a) Eingriffe

Ein Eingriff durch den Gesetzgeber liegt dann vor, wenn ein einfaches Gesetz die **Verwendung**, also insb die Herausgabe,[17] Ermittlung[18] oder Übermittlung[19] von Daten vorschreibt, unabhängig davon, ob diese durch Private oder staatliche Behörden zu erfolgen hat. Ein solches Gesetz ist gerechtfertigt, wenn die darin vorgesehenen Eingriffe mit Zustimmung der betroffenen Person oder in deren lebenswichtigem Interesse erfolgen oder wenn sie zur

[14] Würde man unter „Rückführbarkeit“ nicht die faktische Möglichkeit zur Herstellung des Personenbezuges verstehen, sondern deren rechtliche Zulässigkeit, so würde das zum Ergebnis führen, dass auch indirekt personenbezogene Daten vom Schutzbereich des Grundrechts ausgenommen sind. Ein solches Verständnis kann aber weder der Spruchpraxis des VfGH noch der Literatur entnommen werden. Siehe etwa *Dohr/Pollierer/Weiss*, DSG[2] § 1 Anm 9; *Wiederin*, Privatsphäre und Überwachungsstaat (2003) 59.

[15] So auch *Jahnel*, Das Grundrecht auf Datenschutz nach dem DSG 2000, in FS Schäffer (2006) 323; Der VfGH deutet zwar in VfSlg 18.146/2007 in einem Halbsatz an, dass er „indirekt personenbezogene Daten“ nicht als „personenbezogen“ iSv § 1 Abs 1 DSG versteht, bleibt aber so vage, dass daraus kein Ausschluss der Schutzwürdigkeit indirekt personenbezogener Daten geschlossen werden darf.

[16] Eine solche Abwägung auf der Ebene des Schutzbereiches kann auch nicht aus VfSlg 12.880/1991 abgeleitet werden, weil der VfGH hier davon ausgeht, dass die Behörde richtigerweise eine rechtfertigende Abwägung vorgenommen hat. Diesbezüglich etwas missverständlich *Jahnel*, Das Grundrecht auf Datenschutz nach dem DSG 2000, in FS Schäffer (2006) 324.

[17] VfSlg 12.228/1989.

[18] VfGH 15.6.2007, G147/06 ua.

[19] VfSlg 17.940/2006.

Wahrung überwiegender berechtigter Interessen eines anderen notwendig sind. Ein Eingriff liegt etwa vor, wenn ein Gesetz Bürgerinnen und Bürger verpflichtet, zur Ermittlung ihrer Versicherungs- und Beitragspflicht ihren Einkommenssteuerbescheid einer Sozialversicherungsanstalt vorzuweisen.[20]

b) Zustimmung

Datenverwendungen dürfen gesetzlich jedenfalls dann vorgesehen werden, wenn sie sich auf die Zustimmung der betroffenen Person stützen. Dieser Rechtfertigungsgrund entspricht der Idee, dass jede Person grundsätzlich selbst darüber bestimmen können soll, wofür ihre Daten verwendet werden. Dabei wird dieser Idee der **informationellen Selbstbestimmung**[21] nur Rechnung getragen, wenn die betroffene Person weiß, worin sie einwilligt, und wenn diese Einwilligung freiwillig und ohne Zwang erfolgt. Dies bedeutet, dass die betroffene Person nur solchen Datenverwendungen zustimmen kann, bei denen feststeht, welche Daten zu welchem Zweck von wem ermittelt bzw an welche Empfänger übermittelt werden. Um von einer freiwilligen Zustimmung sprechen zu können, darf die betroffene Person nicht in einem maßgeblichen Abhängigkeitsverhältnis von der die Zustimmung erbittenden Person stehen,[22] und die Zustimmung darf nicht aufgrund einer Anordnung[23] erfolgen.

Damit sind der Rechtfertigungsmöglichkeit von gesetzlichen Eingriffen durch Zustimmung klare Grenzen gesetzt. Insbesondere bei komplexeren Datenverwendungen, bei denen zum Zeitpunkt der Ermittlung der Daten noch unklar ist, an wen zu einem späteren Zeitpunkt zur Erreichung des Verarbeitungszweckes Daten übermittelt werden müssen, ist die Zustimmung der betroffenen Person nur mit großem und manchmal unverhältnismäßigem Aufwand einholbar. Außerdem liegt keine gültige Zustimmung vor, wenn der Gesetzgeber diese anordnet.

c) Lebenswichtiges Interesse des Betroffenen

Gesetzliche Regelungen zur Ermittlung oder Übermittlung von Daten sind auch dann gerechtfertigt, wenn sie dem lebenswichtigen Interesse der betroffenen Person dienen. Dies ist dann der Fall, wenn die Nichtverwendung das körperliche Überleben gefährden würde.

d) Überwiegende berechtigte Interessen eines anderen

Der wichtigste Rechtfertigungsgrund für Eingriffe in das Recht auf Geheimhaltung ist die Wahrung überwiegender berechtigter Interessen anderer.

[20] VfSlg 17.940/2006.

[21] Die Idee eines Informationellen Selbstbestimmungsrechts stammt aus Deutschland, wo das Bundesverfassungsgericht sie 1983 im sog „Volkszählungsurteil“ (BVerfGE 65, 1) als Teil des allgemeinen Persönlichkeitsrechts gem Art 2 Abs 1 GG iVm Art 1 Abs 1 GG anerkannt hat.

[22] Wie etwa in einem Arbeits- oder Mietverhältnis.

[23] Etwa aufgrund einer Weisung oder einer gesetzlichen Anordnung.

Für den an eine mögliche Rechtfertigung anzulegenden Maßstab kommt es bei Eingriffen durch den Gesetzgeber darauf an, ob das eingreifende Gesetz die Datenverwendung durch Private oder durch eine staatliche Behörde vorsieht.

aa) Datenverwendung durch eine staatliche Behörde

Das DSG spricht von „Eingriffen einer **staatlichen Behörde**". Unter einer Behörde versteht man ein Organ einer Gebietskörperschaft, das durch den Gesetzgeber ermächtigt wurde, Hoheitsgewalt auszuüben. Dies kann bei Verwaltungsbehörden in Form von Bescheiden, von Verordnungen oder durch Ausübung unmittelbarer verwaltungsbehördlicher Befehls- oder Zwangsgewalt (AuvBZ), bei Gerichten in Form von Urteilen oder Beschlüssen erfolgen. Der Schutzbereich des Rechts auf Geheimhaltung zielt aber auf Tätigkeiten ab, die selten in hoheitlicher Form gesetzt werden. Die Verarbeitung von Daten erfolgt in der Regel ohne die Setzung eines Hoheitsaktes. Ein Eingriff einer staatlichen Behörde liegt also auch dann vor, wenn ein in einem bestimmten Verwaltungsbereich mit Hoheitsgewalt ausgestattetes Organ bei der Vollziehung von Verwaltungsaufgaben in diesem Bereich Daten verwendet[24] oder eine Verwendung anordnet. Akte im Rahmen der Privatwirtschaftsverwaltung sind hingegen keine Eingriffe einer staatlichen Behörde.

Soll die Datenermittlung oder -übermittlung durch eine staatliche Behörde vorgenommen werden, so ist dies nur zulässig, wenn das eingriffsermächtigende Gesetz der nationalen Sicherheit, der öffentlichen Ruhe und Ordnung, dem wirtschaftlichen Wohl des Landes, der Verteidigung der Ordnung und der Verhinderung von strafbaren Handlungen, dem Schutz der Gesundheit und der Moral oder dem Schutz der Rechte und Freiheiten anderer dient[25] und den Grundsatz der Verhältnismäßigkeit achtet. Dabei ist die Eingriffsermächtigung besonders präzise zu fassen, sodass für jede und jeden[26] vorhersehbar ist, unter welchen Voraussetzungen es für die Wahrnehmung einer Verwaltungsaufgabe notwendig ist, Daten zu verarbeiten.[27] **Verhältnismäßig** ist ein solches Gesetz dann, wenn die eingreifenden Mittel zur Erreichung des konkreten Zieles[28] geeignet und notwendig[29] sind und der Eingriff im Vergleich zum erreichten Ziel dabei nicht unverhältnismäßig schwer wiegt.[30]

[24] ZB die Datenverwendung durch einen Amtsarzt: DSK 4.5.2002, K120.766/004-DSK/2002 und DSK 21.1.2003, K120.757/001-DSK/2003.

[25] Siehe Art 8 Abs 2 EMRK.

[26] Vor allem aber für jene, die von dem Eingriff betroffen sein können. Vgl EGMR 20.5.1999, *Rekvényi*, 25.390/94, Rz 34.

[27] VfSlg 16.369/2001; VfGH 15.06.2007, G147/06 ua. In älteren Entscheidungen scheint der VfGH einen weniger strengen Maßstab für eine ausreichende Determinierung angelegt zu haben: VfSlg 12.166/1989; in VfSlg 15.130/1998 stützt der VfGH die Verwendungsbefugnis direkt auf eine Verfassungsbestimmung (Art 127a B-VG), die im gleichen Rang steht wie das Grundrecht auf Datenschutz.

[28] Das angestrebte Ziel stellt dabei eine Konkretisierung des öffentlichen Interesses dar.

[29] VfSlg 17.065/2003.

[30] VfSlg 17.940/2006.

Sind die Daten, die von der Behörde verarbeitet werden, ihrer Art nach besonders schutzwürdig, so hat das Gesetz, um einen Eingriff rechtfertigen zu können, außerdem einem **wichtigen öffentlichen Interesse** zu dienen und **angemessene Garantien zum Schutz der Geheimhaltungsinteressen** der Betroffenen vorzusehen. Mit Daten, die ihrer Art nach besonders schutzwürdig sind, sind Daten gemeint, deren Bekanntwerden für die betroffene Person zu von der Rechtsordnung besonders unerwünschten Benachteiligungen führen kann.[31] Eine solche Kategorie von Daten wird im einfachgesetzlichen Teil des DSG als „sensible Daten" definiert[32] und umfasst Daten über die rassische oder ethische Herkunft, die politische Meinung, die Gewerkschaftszugehörigkeit, die religiöse oder philosophische Überzeugung, die Gesundheit und das Sexualleben.[33]

Alle oben beschriebenen Interessen, zu deren Gunsten der Gesetzgeber das Grundrecht auf Geheimhaltung beschränken darf, sind wichtige Interessen. In der Literatur[34] findet man aber Stimmen, die meinen, dass der Schutz der Rechte und Freiheiten anderer kein **wichtiges öffentliches Interesse** darstellt und damit für sich genommen keinen Grund darstellt, der einen Eingriff rechtfertigen könnte. Dies ist uE deshalb nicht richtig, weil der Schutz der Rechte und Freiheiten anderer nicht nur im Interesse derjenigen gelegen ist, deren Rechte gerade betroffen sind. Vielmehr stellt der staatliche Schutz der Rechte und Freiheiten und insb der Grundrechte und -freiheiten in einem Rechtsstaat immer und grundsätzlich ein wichtiges öffentliches, dh dem Gemeinwohl dienendes Interesse dar, das einen entsprechenden Eingriff rechtfertigen kann. Liegt also eines der in Art 8 Abs 2 EMRK genannten Eingriffsinteressen vor, so erübrigt sich eine weitere Prüfung auch bei Eingriffen, die die Verwendung sensibler Daten betreffen.

Angemessene Garantien zum Schutz der Geheimhaltungsinteressen der Betroffenen können verschiedene Formen haben. Mögliche Maßnahmen sind etwa die Anordnung besonderer Verschwiegenheitspflichten,[35] besondere über das vom DSG geforderte Maß hinausgehende Datensicherheitsmaßnahmen oder Protokollierungspflichten, strenge Verwendungsbeschränkungen oder Löschungspflichten oder Maßnahmen, die auf einen erhöhten Rechtsschutz der Betroffenen abzielen. Je nach Art und Umfang der Datenverwendung wird es nötig sein, mehrere dieser Maßnahmen zu kombinieren.

bb) Datenverwendung durch Private

Sieht ein Gesetz die Datenverwendung oder Veröffentlichung[36] durch Private vor, so ist der Rechtfertigungsstandard ein anderer als bei Datenverwen-

[31] DSK 21.1.2003 K120.757/001-DSK/2003.

[32] Vgl § 4 Abs Z 2 DSG.

[33] DSK 5.10.1999, 120.667/8-DSK/99.

[34] *Dohr/Pollierer/Weiss*, DSG[2] § 1 Anm 18; mit Verweis auf diese Stelle auch *Jahnel*, Das Grundrecht auf Datenschutz nach dem DSG 2000, in FS Schäffer (2006) 313 (335).

[35] Vgl 17.940/2006.

[36] Etwa die Pflicht zur Veröffentlichung des Jahresabschlusses gemäß § 277 Abs 2 UGB.

dungen durch Behörden. Auch solche Gesetze müssen im öffentlichen Interesse gelegen sein. Diese Anforderung ergibt sich jedoch nicht aus dem Grundrecht auf Datenschutz, sondern aus dem Gleichheitssatz. Das Grundrecht auf Datenschutz fordert lediglich, dass die Datenverwendung durch Private im **überwiegenden berechtigten Interesse eines anderen** stattfinden muss, um gerechtfertigt zu sein. Dabei können diese überwiegenden berechtigten Interessen sowohl öffentliche Interessen als auch private Interessen sein. Maßstab für die Beurteilung, welche Interessen als überwiegend angesehen werden können, ist die Rechtsordnung selbst,[37] sodass sich für den Gesetzgeber keine besondere Bindung ableiten lässt.

Der Gesetzgeber darf jedoch nur die **gelindesten zum Ziel führenden Eingriffe** anordnen. Das bedeutet, dass der Gesetzgeber dem Interesse, das er als überwiegend betrachtet, nur mit jenen Mitteln zum Durchbruch verhelfen kann, die am wenigsten stark in die Rechtssphäre der betroffenen Person eingreifen. Im Ergebnis unterliegt also die Datenverwendung durch Private keinem Gesetzesvorbehalt. Entscheidet sich der Gesetzgeber aber zur Anordnung einer privaten Datenverwendung, so hat dieses Gesetz verhältnismäßig zu sein.

4. Eingriffe durch eine staatliche Behörde

a) Eingriffshandlungen

Ein Eingriff einer staatlichen Behörde liegt vor, wenn ein mit Hoheitsgewalt ausgestattetes staatliches Organ[38] (Gericht oder Verwaltungsbehörde) personenbezogene Daten **ermittelt, übermittelt**[39] oder **aufbewahrt**[40] bzw die Er- oder Übermittlung von Daten mit Bescheid anordnet.[41] Datenverwendungen im Rahmen der Privatwirtschaftsverwaltung stellen keine Eingriffe einer staatlichen Behörde dar. Gerechtfertigt können Eingriffe sein, wenn sie mit der Zustimmung der betroffenen Person, in deren lebenswichtigem Interesse oder aufgrund einer verfassungskonformen gesetzlichen Grundlage erfolgen. Stehen der Behörde mehrere zum Ziel führende Eingriffe zur Wahl, hat sie jenen auszuwählen, der den gelindesten Eingriff in das Recht der betroffenen Person darstellt.

b) Zustimmung

Eine Zustimmung ist nur gültig, wenn sie in Kenntnis der Sachlage freiwillig, ohne Zwang in Hinblick auf eine konkrete Datenverwendung abgegeben wurde. Dabei fordert § 1 Abs 2 DSG keine ausdrückliche Zustimmung,

37 Etwa Gläubigerschutz, siehe OGH 28.6.2000 6 Ob 162/00t.

38 ZB Amt der Kärntner Landesregierung, DSK, 27.2.2004, K120.867/0001-DSK/2004; Siehe dazu auch Kapitel Rz 11/20.

39 Darunter ist auch die Veröffentlichung im Internet zu verstehen. DSK, 27.2.2004, K120.867/0001-DSK/2004.

40 DSG 21.1.2003, K120.757/001-DSK/2003.

41 VfSlg 16.369/2001.

sodass grundsätzlich auch konkludente Willenserklärungen eine rechtfertigende Wirkung entfalten können. Die Zustimmung kann vor allem überall dort als tauglicher Rechtfertigungsgrund dienen, wo Behörden auf Antrag und damit im Interesse der betroffenen Person tätig werden. Stellt also etwa jemand einen Antrag auf Baubewilligung, so umfasst dieser Antrag auch eine Willenserklärung, dass er für das Baubewilligungsverfahren in die Datenverwendung durch die Behörde einwilligt.

c) Lebenswichtige Interessen des Betroffenen

Auch wenn es um lebenswichtige Interessen des Betroffenen geht, dürfen Behördenorgane Daten ohne gesetzliche Grundlage verwenden. Die Datenschutzkommission geht offenbar davon aus, dass dies auch dann zulässig ist, wenn eine solche Datenverwendung gegen den Willen des Betroffenen stattfindet.[42] Eine solche Interpretation entspricht jedenfalls nicht den Vorgaben der EG-Datenschutzrichtlinie,[43] die zumindest eine Verwendung von besonders schutzwürdigen Daten[44] im lebenswichtigen Interesse der betroffenen Person nur gestattet, wenn diese aus rechtlichen oder medizinischen Gründen außerstande ist, ihre Einwilligung zu geben. Diese Interpretation ist daher zu Recht in der Literatur auf Kritik gestoßen.[45]

d) Gesetzliche Grundlage

Den wichtigsten Fall für die Rechtfertigung eines behördlichen Grundrechtseingriffs stellt das Vorliegen einer gesetzlichen Rechtsgrundlage dar. Kann sich die Behörde also weder auf den Schutz lebenswichtiger Interessen der betroffenen Person noch auf deren Zustimmung stützen, so verletzt sie das Grundrecht auf Geheimhaltung personenbezogener Daten, wenn die Datenverwendung

– **gesetzlos**,
– in **denkunmöglicher** Anwendung eines Gesetzes oder
– aufgrund eines **verfassungswidrigen Gesetzes**

stattfindet.

Gesetzlos ist eine Datenverwendung dann, wenn überhaupt keine gesetzliche Grundlage zur Rechtfertigung herangezogen wird. Denkunmöglich wird ein Gesetz dann angewendet, wenn es bspw nur zum Schein herangezogen wird, dieses Gesetz jedoch tatsächlich keine Grundlage für die Verwendung darstellen kann, oder wenn einem Gesetz fälschlicherweise ein verfassungswidriger Inhalt unterstellt wird. Ein Fall der denkunmöglichen Anwendung

42 DSK 5.4.2002, K120.766/004-DSK/2002.

43 Art 8 Abs 2 lit c 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, ABl L 281 vom 23.11.1995, 31–50.

44 Siehe Rz 11/20.

45 *Jahnel*, Das Grundrecht auf Datenschutz nach dem DSG 2000, in FS Schäffer (2006) 313 (328).

eines Gesetzes liegt auch vor, wenn eine zu unpräzise Rechtsgrundlage, in der die Voraussetzungen für eine behördliche Datenverwendung zu unbestimmt sind, herangezogen wird.[46] Die Verfassungswidrigkeit eines Gesetzes kann etwa darin begründet sein, dass es gegen das Grundrecht auf Datenschutz verstößt, also bspw nicht in einem in Art 8 Abs 2 EMRK aufgezählten öffentlichen Interesse gelegen ist, oder dass es bei der Verwendung von besonders schutzwürdigen Daten keine angemessenen Garantien zum Schutz der Geheimhaltungsinteressen beinhaltet.

e) Verhältnismäßigkeit

Lässt das Gesetz der Behörde einen Spielraum bei der Auswahl der Mittel, um ein festgesetztes Ziel zu erreichen, so hat die Behörde jenes Mittel einzusetzen, das am wenigsten stark in die Rechtssphäre der betroffenen Person eingreift. Dies ergibt sich schon aus einer verfassungskonformen Interpretation des eingriffsermächtigenden Gesetzes. Da dieses Gesetz dem Verhältnismäßigkeitsprinzip entsprechen muss, das heißt nur den gelindesten Eingriff zur Erreichung eines Zieles vorsehen darf, würde eine Interpretation, bei der die Behörde unter mehreren möglichen Mittel das stärker eingreifende auszuwählen hätte, dem Gesetz fälschlicherweise einen verfassungswidrigen Inhalt unterstellen, was eine denkunmögliche Gesetzesanwendung und damit eine Grundrechtsverletzung darstellen würde.

Darüber hinaus legt aber auch der letzte Satz des § 1 Abs 2 DSG explizit fest, dass auch im Falle zulässiger Beschränkungen der Eingriff in das Grundrecht nur in der gelindesten zum Ziel führenden Art vorgenommen werden darf. Eine davon abweichende Vorgehensweise einer Behörde stellt eine Grundrechtsverletzung dar. Aus diesem Grund muss eine Behörde auch zuerst versuchen, Daten von der betroffenen Person selbst zu erhalten, bevor sie auf andere Informationsquellen zurückgreift.[47] Vom Verhältnismäßigkeitsprinzip ist auch der „Wesentlichkeitsgrundsatz“ umfasst. Dieser besagt, dass Daten nur so weit verwendet werden dürfen, als sie für den Zweck einer Datenverwendung wesentlich sind bzw über diesen Zweck nicht hinausgehen.[48]

5. Eingriffe durch Private

Eine Besonderheit des Grundrechts auf Datenschutz ist seine unmittelbare Drittwirkung, das heißt, dass es auch vor Eingriffen durch Private schützt.[49] Rechtfertigungsgründe sind auch hier die Zustimmung der betroffenen Person, die Wahrung der lebenswichtigen Interessen der betroffenen Personen und die Wahrung überwiegender berechtigter Interessen einer oder eines anderen.

Die Voraussetzungen einer gültigen **Zustimmung** für eine Datenverwendung durch Private entsprechen jenen einer Datenverwendung durch eine Behörde.[50] Beim Abschluss von Verträgen, die eine Datenverwendung notwendig machen, kann die Zustimmung angenommen werden.[51] Ist die Zustimmung aber kein notwendiger Vertragsbestandteil, so ist sie nur wirksam, wenn die betroffene Person weiß, welche ihrer Daten zu welchem Zweck verwendet werden. Diesem Erfordernis wird eine Vertragsbestimmung nicht gerecht, die nur eine allgemeine Umschreibung des Empfängers oder von Empfängerkreisen enthält.[52] Besondere Bedeutung haben diese Voraussetzungen für Zustimmungserklärungen, die in allgemeinen Geschäftsbedingungen enthalten sind.[53]

Akte Privater müssen im Gegensatz zu Akten staatlicher Organe nicht im öffentlichen Interesse gelegen sein. Für sie gilt die allgemeine Handlungsfreiheit, die in den Rechten anderer ihre Grenzen findet. Aus diesem Grund müssen die Eingriffe durch Private auch nicht auf Gesetze gestützt sein, die besonderen öffentlichen Interessen dienen, sondern es reicht, wenn der Eingriff einem **überwiegenden berechtigen (auch privaten) Interesse** dient. Der Schutz des Interesses der oder des einen endet also dort, wo es mit einem überwiegenden berechtigten Interesse anderer kollidiert. Maßstab für die Bewertung, welches Interesse als überwiegend zu betrachten ist, ist die gesamte Rechtsordnung. Dabei gelten als berechtigte Interessen Dritter auch subjektive, auf gesetzlicher oder vertraglich vereinbarter Grundlage beruhende Ansprüche.[54]

C. Recht auf Auskunft, Richtigstellung und Löschung

1. Schutzbereich

Gemäß § 1 Abs 3 DSG hat jede Person, soweit sie betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen das Recht auf Auskunft darüber, **wer welche Daten** über sie zu welchem Zweck verarbeitet, **woher sie stammen** und **an wen sie übermittelt** werden. Darüber hinaus hat jede Person das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten. Der Schutzbereich der Rechte auf Auskunft, Richtigstellung und Löschung ist gegenüber dem Schutzbereich des Rechts auf Geheimhaltung insofern wesentlich eingeschränkt, als er sich nur auf Daten bezieht, die dazu bestimmt sind, in automationsunterstützter Form oder in Form einer manuellen Datei verarbeitet zu werden. Daten in einer dieser Formen sind besonders leicht auffindbar, weil sie in eine Ordnung gebracht, also strukturiert wurden.

46 VfSlg 16.369/2001.
47 DSK 19.3.1997, 120.512, ZfVB 1997, 565.
48 DSK 14.9.2001, K120.705/010-DSK/2001.
49 OGH 26.8.1999, 2 Ob 244/99t.
50 Siehe Rz 11/16 und 11/28.
51 VfSlg 16.467/2002.
52 OGH 22.3.2001, 4 Ob 28/01y.
53 OGH 20.3.2007, 4 Ob 221/06p.
54 OGH 26.8.1999, 2 Ob 244/99t.

a) Auskunft

Das Recht einer betroffenen Person auf Auskunft umfasst alle Daten über diese Person, die von einem Dritten verarbeitet werden. Dabei reicht es nicht, wenn nur Datenarten oder Datenkategorien bekanntgegeben werden. Enthalten etwa auch Protokolldaten personenbezogene Informationen, so ist auch über diese Protokolldaten Auskunft zu erteilen. Besteht gemäß § 14 Abs 3 DSG keine Protokollierungspflicht bezüglich Übermittlungen, so erfasst das Auskunftsrecht im Hinblick auf die Empfänger nur eine Auskunft über die Empfängerkreise. Wurden jedoch die tatsächlichen Empfänger protokolliert, so sind diese bei einem Auskunftsersuchen auch anzugeben, weil grundsätzlich Auskunft über alle vorhandenen Daten zu geben ist.[55]

b) Richtigstellung

Das Recht auf **Richtigstellung** bezieht sich auf **unrichtige Daten**. Unrichtig sind Daten dann, wenn sie nicht mit der Wirklichkeit übereinstimmen. Da sich die Wirklichkeit ändert, ist auch von Bedeutung, auf welchen Zeitpunkt sich die Daten beziehen. Unrichtig gewordene Daten können nämlich tatsächlich richtig sein, wenn aus der Aufzeichnung hervorgeht, dass sich die Information auf einen Zeitpunkt bezieht, zu dem die Daten richtig waren. Werden jedoch Daten nicht richtiggestellt, die sich immer auf die aktuelle Situation beziehen, so stellt dies einen Eingriff in das Grundrecht dar.[56] Das Recht auf Richtigstellung setzt nicht voraus, dass die betroffene Person einen Antrag auf Richtigstellung stellt. Tatsächlich haben also Datenverarbeiter dafür zu sorgen, dass Daten stets richtig bleiben.

c) Löschung

Das Recht auf **Löschung** besteht hinsichtlich Daten, die **unzulässigerweise verarbeitet** werden. Eine Verarbeitung ist dann unzulässig, wenn sie die Voraussetzungen des DSG oder anderer gesetzlicher Verwendungsermächtigungen nicht erfüllt. Da die Zulässigkeit einer Verarbeitung nach dem DSG maßgeblich vom Zweck der Verarbeitung abhängt, umfasst das Recht auf Löschung auch eine Pflicht des Datenverarbeiters, die Daten nach Erreichung des Zweckes oder wenn sich die Daten als nicht notwendig für die Erreichung dieses Zweckes erweisen,[57] zu löschen.

d) Automationsunterstützte Verarbeitung

Um von einer automationsunterstützten Verarbeitung sprechen zu können, muss zumindest ein Vorgang im Rahmen der Datenanwendung automationsunterstützt ablaufen. Eine Datenanwendung wird abgegrenzt durch ihren Zweck. Jene Datenverwendungen, die zu demselben bestimmten Zweck durchgeführt werden, machen die Datenanwendung aus. Automationsunterstützt ist ein Datenverwendungsvorgang dann, wenn er **programmgesteuert**, dh unter Einsatz von elektronischen Datenverarbeitungsanlagen erfolgt. Dabei kommt es nicht darauf an, dass die Verarbeitung besonders komplex abläuft oder dass die personenbezogene Information besonders strukturiert in einer Datenbank abgelegt wird. Die Strukturierung erfolgt bei einer automationsunterstützten Verarbeitung bereits bei der Digitalisierung. Das Erstellen und Abspeichern einer Textverarbeitungsdatei ist also genauso eine automationsunterstützte Verarbeitung wie das Ausdrucken einer E-Mail.

55 VfGH 2.10.2007, B227/05.
56 VfSlg 16.150/2001.
57 VfGH 15.06.2007, G147/06 ua.

e) Manuelle Datei

Eine manuelle Datei zeichnet sich dadurch aus, dass in ihr Daten **strukturiert**, aber nicht digitalisiert sind. Dabei muss ein solcher Ordnungsgrad erreicht werden, dass eine gezielte Suche nach bestimmten personenbezogenen Daten möglich ist. Es reicht also nicht, dass die Information mit einer Ordnungsnummer oder Geschäftszahl versehen[58] wird oder Blätter innerhalb eines Aktes chronologisch abgelegt werden.[59] Werden allerdings eine Kartei oder Personalakte alphabetisch nach Namen oder den Geburtsdaten von Personen sortiert, so liegt eine manuelle Datei vor.

f) Gesetzesvorbehalt

Die Rechte auf Auskunft, Richtigstellung und Löschung bestehen gemäß § 1 Abs 3 DSG nach Maßgabe gesetzlicher Bestimmungen. Diese Einschränkung ist nicht als Ausgestaltungsvorbehalt zu verstehen, wie ihn etwa Art 12 StGG für das Versammlungs- und Vereinigungsrecht kennt. Nicht jede Verletzung der einfachgesetzlich ausgestalteten Modalitäten der Rechte auf Auskunft, Richtigstellung und Löschung stellt also eine Grundrechtsverletzung dar. Eine Feinprüfung findet daher durch den VfGH nicht statt.[60] Vielmehr verbleibt diese Prüfungskompetenz beim VwGH. Der einfache Gesetzgeber darf aber aufgrund dieser Bestimmung Verfahrensregelungen zur Geltendmachung der Rechte auf Auskunft, Richtigstellung und Löschung festlegen. Schränkt eine dieser Verfahrensregelungen die Ausübung eines der drei Rechte ein, so stellt diese Regelung aber einen Eingriff in das Grundrecht dar, der auch vom VfGH geprüft und im Falle einer Verletzung aufgehoben werden kann.[61]

2. Eingriffe

a) Arten von Eingriffen

Eingriffe in die Rechte auf Auskunft, Richtigstellung und Löschung passieren meist in Form von **Unterlassungen**. So stellt es etwa einen Eingriff in das

58 VfSlg 17.745/2005; VfGH 7.3.2007, B1708/06; DSK 10.11.2000, 120.707/7-DSK/00.
59 DSK 18.5.2000, 120.686/3-DSK/00.
60 VfSlg 12.768/1991.
61 Vgl VfSlg 16.986/2003.

Recht auf Auskunft dar, wenn einem Auskunftsersuchen nicht oder nicht vollständig nachgekommen wird. Die Auskunft muss auch in angemessener Zeit erfolgen. Die Achtung der Rechte auf Richtigstellung und Löschung hängen hingegen nicht von einem Antrag der betroffenen Person ab. Sie müssen also ständig beachtet werden und nicht wie beim Recht auf Auskunft nur im Falle eines Antrags der betroffenen Person. Eingriffe stellen die Verwendung von unrichtigen Daten und die Aufbewahrung von unzulässig verarbeiteten Daten dar. Während die unzulässige Erhebung von Daten einen Eingriff in das Recht auf Geheimhaltung darstellt, stellt die Aufbewahrung auf Vorrat, die nicht auf einen bestimmten legitimen Zweck abzielt, einen Eingriff in das Recht auf Löschung dar.[62]

b) Rechtfertigung

Eingriffe in das Recht auf Auskunft, Richtigstellung oder Löschung sind unter den gleichen Bedingungen gerechtfertigt wie solche in das Recht auf Geheimhaltung. Grundsätzlich sind also die Aussagen, die diesbezüglich getroffen wurden, [63] auch für die Rechte auf Auskunft, Richtigstellung und Löschung gültig. Insb gilt auch hier, dass Gesetze, die Eingriffe vorsehen, verhältnismäßig sein müssen.[64] Praktisch sind aber Eingriffe zur Wahrung lebenswichtiger Interessen bzw solche mit Zustimmung der betroffenen Person kaum vorstellbar. Eine derartige Situation, in der die Verweigerung einer Auskunft, einer Richtigstellung bzw einer Löschung gegenüber einer betroffenen Person deren lebenswichtige Interessen schützt, liegt jenseits jeder Lebenserfahrung. Auch die Zustimmung zur Verweigerung der Auskunft wird eher einen Ausnahmefall darstellen, da die betroffene Person wohl kein Auskunftsersuchen stellen wird, wenn sie dann der Verweigerung desselben zustimmt. Das Unterlassen einer Löschung mit Zustimmung der betroffenen Person ist zwar denkbar, wird aber in den meisten Fällen nicht gerechtfertigt werden müssen, da ja nur unzulässigerweise verarbeitete Daten gelöscht werden müssen und eine Zustimmung zur Datenverarbeitung deren Zulässigkeit begründet, sodass eine solche Aufbewahrung schon gar nicht vom Schutzbereich des Grundrechts auf Löschung erfasst ist.

Wichtigste Rechtfertigungsmöglichkeit ist auch im Hinblick auf diese Rechte die Wahrung überwiegender berechtigter Interessen anderer. Dabei kommt es häufig vor, dass das Recht auf Auskunft und das Recht auf Geheimhaltung gegeneinander abgewogen werden müssen. Dies ist insb dann der Fall, wenn Daten von mehreren Personen miteinander verknüpft sind und einem Auskunftsbegehren einer dieser Personen nur unter Preisgabe der Daten der anderen Person nachgekommen werden kann. In einem solchen Fall ist, je nach Ausgang der **Interessensabwägung**, das Recht auf Auskunft oder das Recht auf Geheimhaltung zur Wahrung des anderen Interesses einzuschränken. Die Unterlassung einer solchen Abwägung durch eine zur Entscheidung zuständigen Behörde (etwa die DSK) stellt jedenfalls eine Verletzung dar.[65]

62 VfSlg 16.369/2001.
63 Siehe Kap II.B.3. u 4.
64 VfSlg 16.986/2003.
65 VfGH 2.10.2007, B227/05.

D. Rechtsschutz

Verletzungen des Grundrechts auf Datenschutz finden oft in Formen statt, gegen die die Rechtsordnung (abgesehen vom DSG) keine Beschwerdemöglichkeiten vorsieht. So stellen bspw Datenverwendungen durch Behörden weder Bescheide noch Ausübungen unmittelbarer verwaltungsbehördlicher Befehls- oder Zwangsgewalt dar, sodass eine Anfechtungsmöglichkeit grundsätzlich nicht vorhanden wäre. Um diesem Problem zu begegnen, etabliert § 1 Abs 5 DSG ein eigenes Rechtsschutzinstrumentarium. Dabei richtet sich die erstinstanzliche Zuständigkeit für Beschwerden wegen Verletzungen des Grundrechts auf Datenschutz grundsätzlich nach der Rechtsform des Beschwerdegegners und der Form, in der dieser handelt.

1. Zuständigkeit der Gerichte

Das Grundrecht auf Datenschutz wirkt auch unmittelbar zwischen den Bürgerinnen und Bürgern. Für Beschwerden wegen Nichtbeachtung der Rechte auf Geheimhaltung, Richtigstellung und Löschung gegen Private oder juristische Personen des Privatrechts sind grundsätzlich die Zivilgerichte zuständig. Ausgenommen von dieser Zuständigkeit sind Beschwerden gegen Private, soweit sie in Vollziehung der Gesetze, also in Ausübung hoheitlicher Funktionen tätig werden, womit auch die schlichte Hoheitsverwaltung gemeint ist.[66] Verletzungen durch Beliehene, die in Ausübung ihrer Vollziehungsfunktion tätig werden, sind also der Zuständigkeit der Gerichte entzogen.

Auch Akte der Gerichtsbarkeit, die einen Eingriff in das Grundrecht auf Datenschutz darstellen, sind von Gerichten zu überprüfen. Die Durchsetzung der Rechte richtet sich dabei gemäß § 83 GOG[67] nach den Bestimmungen des GOG. Grundsätzlich ist zur Entscheidung über eine Beschwerde in bürgerlichen Rechtssachen das im Instanzenzug übergeordnete Gericht, in Strafsachen jedoch das **Gericht zweiter Instanz** zuständig.

2. Zuständigkeit der Datenschutzkommission

Die Datenschutzkommission ist zuständig für Beschwerden wegen Verletzungen aller vier Rechte (Geheimhaltung, Auskunft, Richtigstellung und Löschung) durch Rechtsträger, die in Formen des öffentlichen Rechts eingerichtet sind. Darüber hinaus erkennt die DSK auch über Beschwerden wegen Verletzungen des Rechts auf Auskunft durch Private. Die Entscheidungen der DSK ergehen in Bescheidform und können vor dem VfGH angefochten werden.[68]

66 Vgl RV zu § 5 DSG: 1613 BlgNR 20 GP 39.
67 Gerichtsorganisationsgesetz, RGBl 217/1896 idgF.
68 Siehe weiter zu Datenschutzkommission Abschnitt IV.

III. Kompetenzrechtliche Situation

§ 2 DSG regelt als **Sonderbestimmung** zu Art 10 ff B-VG die Kompetenzverteilung im Datenschutzrecht in spezieller Weise. § 2 Abs 1 DSG sieht vor, dass „Angelegenheiten des Schutzes personenbezogener Daten im automationsunterstützten Datenverkehr" Bundessache in Gesetzgebung sind.[69] Hervorzuheben ist, dass sich die kompetenzrechtliche Bestimmung nur auf den Schutz personenbezogener Daten im automationsunterstützten Datenverkehr bezieht, nicht aber auf den automationsunterstützten Datenverkehr selbst. Auch wenn diesbezüglich Überschneidungen bestehen, sind diese Bereiche vorerst getrennt voneinander zu betrachten.

Die Kompetenz zur Begründung eines automationsunterstützten Datenverkehrs bzw zur Verwendung personenbezogener Daten ist eine Adhäsionskompetenz zur jeweiligen Sachmaterie. Die Regelungen gem §§ 4 ff DSG sind idS als Regelungen über den Schutz personenbezogener Daten im automationsunterstützten Datenverkehr zu verstehen, die jedoch keine konkrete Grundlage für einen automationsunterstützten Datenverkehr im Einzelfall liefern.[70] Soweit es um die konkrete Verwendung personenbezogener Daten im Rahmen von Landeskompetenzen geht, ist somit auch das (jeweilige Bundes-)Land zur Gesetzgebung berufen. Anderes gilt – wie erwähnt – gem § 2 DSG in Angelegenheiten des Schutzes (!) personenbezogener Daten, in denen die Gesetzgebungskompetenz beim Bund liegt.

Bei näherer Betrachtung der Unterscheidung zwischen konkreter Datenverwendung und Datenschutz zeigt sich, dass die Grenze zwischen beiden Bereichen schwer zu ziehen ist, da mit der konkreten Datenverwendung auch Regelungen des Datenschutzes getroffen werden. *Kunnert* schlägt daher eine **Differenzierung** zwischen **allgemeinem Datenschutz** (wie er sich im DSG findet) und **bereichspezifischem Datenschutz** vor, wobei letzterer als Annexmaterie verstanden wird.[71]

Da sich die Regelung des § 2 Abs 1 DSG nur auf „automationsunterstützten Datenverkehr" bezieht, ist der Datenschutz hinsichtlich manuell verarbeiteter Daten genauso als Annexkompetenz zu betrachten und daher – ebenso wie die Datenverwendung –, soweit er Landesmaterien betrifft, Landessache.[72]

[69] Siehe Art 10 Abs 1 Z 13 ME.

[70] Die Zuordnung der Datenverwendung als Adhäsionskompetenz ergibt sich nicht explizit, aber doch implizit aus der Festlegung des Datenschutzes als eigenständige Materie. Historisch betrachtet, kann die Verwendung von personenbezogenen Daten als Teil der internen Verwaltung verstanden werden, die in die Organisationsgewalt der jeweiligen staatlichen Einrichtung gefallen ist.

[71] *Kunnert*, Der Ministerialentwurf für eine DSG Novelle 2010, jusIT 2009, 102 (103).

[72] *Dohr/Pollierer/Weiss*, DSG[2] § 2 Anm 4; siehe dazu auch die Landesdatenschutzgesetze burgenländisches Datenschutzgesetz LGBl 2005/87; Kärntner Informations- und Statistikgesetz LBGl 2005/74 idF 2006/59; Nö Datenschutzgesetz LGBl 0901-1; Oö. Auskunftspflicht-, Datenschutz- und Informationsweiterverwendungsgesetz LGBl 1988/46 idF 2006/86; Sbg Gesetz über Auskunftspflicht, Dokumentenweiterverwendung, Datenschutz und Landesstatistik LGBl 1988/73 idF 2007/69; Steiermärkisches Datenschutzgesetz LGBl 2001/39; Tiroler Datenschutzgesetz LGBl 2003/69; Vlbg Landes-Datenschutzgesetz LGBl 2000/19; Wiener Datenschutzgesetz LGBl 2001/125.

In der Vollziehung der Angelegenheiten des Datenschutzes beim automationsunterstützten Datenverkehr wird allerdings differenziert. Ausgangspunkt ist eine grundsätzliche Vollziehung durch den Bund gem § 2 Abs 2 DSG. Nachdem eine spezielle Bestimmung zur (un)mittelbaren Bundesverwaltung nicht vorhanden ist und Art 102 Abs 2 B-VG diesbezüglich keine Ausnahme vorsieht, bedeutet dies für den Datenschutz eine Vollziehung in Form mittelbarer Bundesverwaltung. Ausgenommen von der Verpflichtung zur mittelbaren Bundesverwaltung sind aber gem § 2 Abs 2 DSG iVm § 1 Abs 5 DSG sowohl die Gerichte als auch die Datenschutzkommission und der Datenschutzrat. Damit besteht kein relevanter Anwendungsbereich für die Vollziehung in mittelbarer Bundesverwaltung.[73]

In Hinblick auf den besonderen Rechtsschutz im SPG ist der Rechtsschutzbeauftragte (RSB) gem § 91a ff SPG zu erwähnen, dem in Hinblick auf den Datenschutz gem § 91c–d SPG besondere Befugnisse zukommen, die dem in § 2 Abs 2 DSG aufgestellten Konzept der mittelbaren Bundesverwaltung widersprechen würden. Da allerdings gem § 91a SPG eine verfassungsgesetzliche Einrichtung des RSB erfolgt ist, besteht somit ebenfalls kein verfassungsrechtliches Problem.

Hinsichtlich der Vollziehung durch den Bund bestehen gem § 2 Abs 2 DSG weitere Ausnahmen, die sich auf die Datenverwendung (!) durch ein Bundesland bzw im Auftrag eines Bundeslandes oder einer juristischen Person des öffentlichen Rechts des Landes beziehen. In diesen Fällen ist – wiederum mit Ausnahme der Rechtsschutzaufgaben der Gerichte, der DSK oder des DSR – die Vollziehung Landessache, fällt also in den Bereich der unmittelbaren Landesverwaltung. Dies bedeutet, dass in den Landesmaterien – denn in diesen ist die Datenverwendung Landessache – auch der Rechtsschutz von den Ländern vollzogen werden soll. Da aber dem Bundesgesetzgeber die Gesetzgebungskompetenz obliegt und dieser primär die Gerichte, die DSK und den DSR mit den Rechtsschutzaufgaben betraut, besteht auch im Rahmen unmittelbarer Landesverwaltung ein rechtlich eingeschränkter Anwendungsbereich der Vollziehung.

Durch eine DSG-Novelle 2010 könnten die kompetenzrechtlichen Sonderbestimmungen allerdings abgeschafft werden und eine Eingliederung in Art 10 Abs 1 Z 13 B-VG erfolgen.[74]

IV. Organisationsrechtliche Verfassungsbestimmungen

A. Verfassungsbestimmungen zur Datenschutzkommission

§ 1 Abs 5 DSG ist – wie dargestellt – der Ausgangspunkt für die Bestimmungen der DSK im DSG. Für das Grundrecht auf Datenschutz ist – abgese-

[73] Durch die DSG-Nov 2010 soll der Datenschutz in den Art 102 Abs 2 B-VG aufgenommen werden, womit keine Anwendung der mittelbaren Bundesverwaltung erfolgt.

[74] Siehe den ME 62, 24. GP; siehe dazu kritisch *Kunnert*, jusIT 2009, 103f.; siehe auch Abschnitt VI.

hen von den in § 1 Abs 5 DSG genannten Ausnahmen – die DSK für zuständig erklärt. Diese Zuständigkeitserklärung der Datenschutzkommission kann auch als eine **verfassungsgesetzliche Organisationsgarantie der DSK** gedeutet werden, da bei (einfachgesetzlicher) Abschaffung der DSK die Zuständigkeitsregel ins Leere laufen würde. § 1 Abs 5 DSG setzt aber damit auch eine bestimmte organisatorische Ausgestaltung der DSK, wie etwa die kollegiale Ausgestaltung derselben, voraus. Die verfassungsrechtliche Absicherung der DSK bezieht sich schon begrifflich (arg. „Kommission") auf die Kollegialität derselben.

In weiterer Folge sind mehrere Verfassungsbestimmungen iZm der DSK zu erwähnen, die nicht nur die verfassungsrechtliche Absicherung der DSK bestätigen, sondern auch die Sonderstellung der DSK in bestimmten Zusammenhängen absichert. Im Kontext der verfassungsrechtlichen Verankerung der DSK soll zum einen auf die Weisungsfreiheit der DSK (B.) und die Prüfkompetenz gegenüber obersten Organen (C.) kurz eingegangen werden.

Als weitere Verfassungsbestimmung wird gem § 38 Abs 1 DSG die **innere Ausgestaltung** der DSK verfassungsgesetzlich in bestimmten Aspekten abgesichert. Dabei ist die Erlassung einer Geschäftsordnung (GO) zwar verfassungsgesetzlich vorgesehen, doch trägt dies keinerlei weitere Bedeutung in sich, als damit eine Verpflichtung zur Konkretisierung bestimmt wird, die auch einfachgesetzlich oder verwaltungsintern vorgesehen werden könnte.[75] Viel wichtiger iSd § 38 Abs 1 DSG ist die Betrauung eines der Mitglieder der DSK mit „der Führung der laufenden Geschäfte", als sog „geschäftsführendes Mitglied". Die Bestimmung des § 38 Abs 1 DSG konkretisiert, dass die „Führung der laufenden Geschäfte" auch die „Erlassung von verfahrensrechtlichen Bescheiden und von Mandatsbescheiden im Registrierungsverfahren" beinhaltet. Damit wird zusätzlich zur DSK ein weiteres monokratisches Organ geschaffen, dem eigenständige behördliche Kompetenzen zukommen. Aufgrund der verfassungsrechtlichen Absicherung der DSK als Kollegialorgan durch § 1 Abs 5 DSG ist eine verfassungsrechtliche Ausnahme durch die Schaffung eines monokratischen Organs in Form des geschäftsführenden Mitglieds gem § 38 Abs 1 DSG erforderlich, soweit dieses Organ in Fragen des Grundrechts auf Datenschutz entscheidet. Die gem § 40 DSG vorgesehene Vorstellung an die DSK alleine würde nicht ausreichen, um § 1 Abs 5 DSG zu genügen.

Mit der in Diskussion befindlichen DSG-Nov 2010[76] soll diese Verfassungsbestimmung entfallen.[77] Diese Abschaffung ist nur insoweit gerechtfertigt, als

[75] Dies ist hinsichtlich des § 38 Abs 1 letzter Satz DSG ebenso zu sehen, der die Möglichkeit eröffnet, „einzelne fachlich geeignete Bedienstete der Geschäftsstelle der Datenschutzkommission zum Handeln für die Datenschutzkommission oder das geschäftsführende Mitglied" durch die GO zu ermächtigen.

[76] Siehe den ME 62, 24. GP.

[77] Die rechtstechnische Vorgehensweise, in der geplanten DSG-Nov nur die Bezeichnung als „Verfassungsbestimmung" zu löschen, trägt zwar implizit die Ermächtigung, diese Bestimmung als einfaches Bundesgesetz in Geltung zu belassen, in sich, ist aber als problematisch zu bezeichnen. Die bloße Löschung der Bezeichnung als Verfassungsbestimmung bezieht sich auf die Bezeichnungspflicht gem Art 44 Abs 1 B-VG. Diese Bezeichnungspflicht ist die Folge der Normierung als Verfassungsbestimmung. Die bloße Löschung der Bezeichnung macht diese Bestimmung allerdings verfassungswidrig und nicht zu einem einfachen Gesetz. Nur durch eine teleologische Interpretation der Löschung der Bezeichnung kann darauf geschlossen werden, dass eigentlich nicht die Löschung der Bezeichnung allein, sondern primär eine Entkleidung des verfassungsrechtlichen Rangs erzielt werden sollte.

damit nicht der Anwendungsbereich des § 1 Abs 5 DSG beeinträchtigt ist, also in Fragen des Grundrechts auf Datenschutz die DSK als Kollegialorgan entscheidet. Insoweit wäre die sodann einfachgesetzliche Bestimmung des § 38 Abs 1 DSG als verfassungswidrig anzusehen, da diese Bestimmung nicht vollständig verfassungskonform interpretiert werden kann. Die Ausübung monokratischer Behördenbefugnisse widerspricht der verfassungsgesetzlichen Zuständigkeitsregel des § 1 Abs 5 DSG, die die DSK als Kollegialorgan als zur Entscheidung verpflichtet vorsieht.[78]

B. Weisungsfreiheit der Datenschutzkommission

Gem § 37 Abs 1 DSG sind die Mitglieder der DSK „in Ausübung ihres Amtes unabhängig und an keine Weisungen gebunden". Diese gesetzliche Regelung war bis zur Bundesverfassungsrechtsbereinigung 2008 (1. BVRBG)[79] ebenfalls eine Verfassungsbestimmung, die die Unabhängigkeit der DSK verfassungsrechtlich abgesichert hat. Durch die **Neukonzeption des Art 20 Abs 2 B-VG** und die Idee einer „Bereinigung"[80] von Verfassungsbestimmungen wurde die verfassungsgesetzlich gewährleistete Unabhängigkeit auf die Ebene des einfachen Gesetzes zurückgestuft.[81] Es stellt sich daher die Frage, inwieweit durch die Neukonzeption des Art 20 Abs 2 B-VG Auswirkungen auf die DSK bestehen und ob die Weisungsfreistellung der DSK noch verfassungsgesetzlich abgesichert ist.

Der erste Aspekt bezieht sich auf die neue Ausgestaltung des Art 20 Abs 2 B-VG. Schon bislang konnte die DSK als Kollegialbehörde mit richterlichem Einschlag angesehen werden.[82] Somit fiel die Datenschutzkommission bereits unter das bisherige Konzept des Art 20 Abs 2 B-VG, wurde aber dennoch extra verfassungsgesetzlich in seiner Weisungsfreiheit abgesichert.

Im Rahmen der Neuregelung des Art 20 Abs 2 B-VG fällt die DSK sowohl unter Z 2 („zur Kontrolle der Wahrung der Gesetzmäßigkeit der Verwaltung")

[78] Überdies kann sich ein monokratisches Organ nicht auf Art 20 (2) Z 3 B-VG stützen.

[79] Bundesverfassungsgesetz, mit dem das Bundes-Verfassungsgesetz geändert und ein Erstes Bundesverfassungsrechtsbereinigungsgesetz erlassen wird, BGBl I 2008/2.

[80] Siehe kritisch *Lachmayer*, Zwischen Ordnung und Chaos. Von der Notwendigkeit der Verfassungsbereinigung und der Illusion des Inkorporationsgebotes, JRP 2007, 200.

[81] Siehe *Öhlinger*, Weisungsfreie Verwaltungsbehörden nach der B-VGNovelle BGBl I 2008/2. Verfassungs- und Verwaltungsreform 2008, JRP 2008, 85; *Damjanovic*, Weisungsfreie Behörden: der Vorschlag für eine Neufassung des Art 20 Abs 2 B-VG, JRP 2007, 222.

[82] Siehe die Zusammensetzung der DSK gem § 36 Abs 2 DSG und die eigenständige Kontrollbefugnisse außerhalb eines Instanzenzuges gem §§ 30ff DSG; siehe bereits unter der Rechtslage vor dem DSG 2000 *Grabenwarter*, Art 133 B-VG, in Korinek/Holoubek (Hrsg), Kommentar zum B-VG, 1. LfG (1999), 47.

als auch Z 3 leg cit („zur Entscheidung in oberster Instanz, wenn sie kollegial eingerichtet sind, ihnen wenigstens ein Richter angehört und ihre Bescheide nicht der Aufhebung oder Abänderung im Verwaltungsweg unterliegen"). Auch Z 8 leg cit („soweit dies nach Maßgabe des Rechts der Europäischen Union geboten ist") kann zumindest teilweise als Grundlage für die Tätigkeit der DSK herangezogen werden.

Die neu durch Art 20 Abs 2 B-VG geschaffenen demokratischen Verantwortlichkeitsstrukturen gelten nur zum Teil für die DSK. Von der Möglichkeit der Abberufung aus wichtigem Grund ist in den Fällen der „Z 2, 3 und 8" leg cit, also den einschlägigen Bestimmungen für die DSK, abzusehen. Allerdings bleibt das „angemessene Aufsichtsrecht der obersten Organe" bestehen. Dies beinhaltet „zumindest das Recht, sich über alle Gegenstände der Geschäftsführung der weisungsfreien Organe zu unterrichten". Die Berichtspflicht gem § 38 Abs 4 DSG erfüllt diese Vorgaben zumindest ansatzweise. Offen bleibt, inwieweit die gem § 38 Abs 2 DSG eingerichtete Geschäftsstelle beim BKA nicht ohnedies die Informations- bzw Aufsichtsmöglichkeiten für den Bundeskanzler ermöglicht.

Der zweite Aspekt bezieht sich auf die verfassungsgesetzliche Absicherung der DSK. Diese ist zumindest aus zwei Perspektiven relevant. Zum einen bedeutet dies nicht nur eine bloße Anpassung („Bereinigung") der Verfassungsrechtslage, sondern eine substantielle Änderung der Garantien der Unabhängigkeit der DSK im österreichischen Rechtssystem. Zum zweiten ist die Frage zu beantworten, ob der einfache Gesetzgeber die Unabhängigkeit der DSK einschränken könnte.[83]

Durch das 1. BVRBG ist die explizite verfassungsrechtliche Absicherung der Unabhängigkeit der DSK abgeschafft worden. Es stellt sich die Frage, ob die **Weisungsfreistellung der DSK** aber nicht dennoch im Rahmen des § 1 Abs 5 DSG als **verfassungsgesetzlich abgesichert** anzusehen ist. Auch wenn diese Bestimmung nicht explizit die Weisungsfreistellung anspricht, wird durch § 1 Abs 5 DSG die DSK explizit verankert und damit auch – wie dargestellt – ein organisationsrechtliches Bild der DSK mit in den Verfassungsrechtsbestand hineingenommen. Ohne die organisationsrechtlichen Details der DSK mit dem In-Kraft-Treten der Verfassungsbestimmung gem § 1 Abs 5 DSG im Rahmen des DSG 2000 versteinern zu wollen, ist doch auf den historischen organisationsrechtlichen Rahmen der DSK am 1. Jänner 2000 zu referenzieren. Die explizite Weisungsfreistellung bildet mit dem Grundrecht auf Datenschutz und der Zuständigkeitsregelung ein verfassungsrechtliches System des Datenschutzes. Durch den Entfall der expliziten Verfassungsbestimmung zur Weisungsfreiheit wollte der Verfassungsgesetzgeber die Weisungsfreistellung der DSK nicht abschaffen. Es wurde vielmehr argumentiert, dass eine solche – aus dem Blickwinkel der Verfassungsbereinigung – aufgrund der Neuregelung des Art 20 Abs 2 B-VG nicht mehr notwendig

[83] Dabei ist allerdings auch zu beachten, dass die DSK oft auch als nationale Rechtsschutzinstanz in unterschiedlichen Bereichen des Europarechts fungiert. Insoweit bestehen nicht nur innerstaatliche, sondern auch europarechtliche Verpflichtungen der Unabhängigkeit der DSK.

sei.[84] Die Regelung des § 1 Abs 5 DSG blieb hingegen unberührt. Spricht man der Zuständigkeitsregelung der DSK organisationsrechtlichen Charakter zu, so ist dieser über die Kollegialität hinaus, auch aus der Perspektive der Kontrolle oberster Organe (§ 35 Abs 2 DSG)[85] und des grundrechtlichen Rechtsschutzkonzepts des Grundrechts auf Datenschutz (§ 1 DSG) zu verstehen. Eine Kontrolle oberster Organe durch eine weisungsgebundene Behörde würde Art 19 B-VG widersprechen, da auf diese Weise die Stellung des obersten Organs untergraben und ihre demokratische Legitimation empfindlich beeinträchtigt würde. Bei (historischer) Betrachtung des datenschutzrechtlichen Rechtsschutzregimes ergibt sich ebenso das Verständnis unabhängiger (und damit weisungsungebundener) Kontrolle im Datenschutzrecht. Darüber hinaus bestand im Rahmen des 1. BVRBG nicht das Bestreben, die Weisungsfreiheit der DSK zu beeinträchtigen. Es kann daher aufgrund der noch bestehenden verfassungsgesetzlichen Bestimmungen des § 1 DSG iVm § 35 Abs 2 DSG argumentiert werden, dass die Benennung der DSK in § 1 Abs 5 DSG auch die Weisungsfreiheit der DSK mit umfasst.

Zusammenfassend bedeutet dies, dass die DSK als weisungsfreie Kollegialbehörde im Verfassungsrang abgesichert ist, sie aber auch die Vorgaben des Art 20 Abs 2 B-VG idF BGBl I 2008/2 (Stichwort: Aufsichtsrecht) zu erfüllen hat.[86] Damit ist auch die zweite Frage nach der Einschränkung der Unabhängigkeit der DSK durch den einfachen Gesetzgeber abschlägig zu beantworten.

C. Datenschutzkommission und oberste Organe

Eine weitere Verfassungsbestimmung im DSG, die sich auf die DSK bezieht, findet sich in § 35 Abs 2 DSG, die der DSK die **Ausübung ihrer Befugnisse auch gegenüber den obersten Organen** gem Art 19 B-VG zusichert.

Oberste Organe gem Art 19 B-VG sind durch die Weisungsfreistellung, der Ausschluss weiterer Instanzenzüge, die Nicht-Bindung an die Willensbildung anderer Organe und den Ausschluss einer sachlich in Betracht kommenden Oberbehörde gekennzeichnet.[87] Überdies darf – und dies ist idZ entscheidend – die Kontrolle der Rechtmäßigkeit des Handelns nicht an eine andere Verwaltungsbehörde übertragen werden.[88] Genau diese Kontrolle der Rechtmäßigkeit des Handelns wird durch die DSK in Bezug auf den Datenschutz, aber auch gegenüber obersten Organen ausgeübt, wofür § 35 Abs 2 DSG die verfassungsgesetzliche Ermächtigung zur Verfügung stellt.

[84] „Der Verfassungsrang der in § 5 genannten Bestimmungen ist schon nach geltender Verfassungsrechtslage entbehrlich (Abs. 1) oder sein Entfall steht in sachlichem Zusammenhang mit der in Art. 1 Z 9 vorgeschlagenen Neufassung des Art. 20 Abs. 2 B-VG (Abs. 2) […]". RV 314 BlgNR, 23. GP, 16.

[85] Siehe dazu sogleich unter C.

[86] Inwieweit das Aufsichtsrecht gem Art 20 Abs 2 B-VG mit den europarechtlichen Vorgaben an Unabhängigkeit kollidiert, kann idZ nicht nachgegangen werden.

[87] Siehe *Mayer*, B-VG Kommentar[4] (2007) Art 19 Anm I.2.

[88] Siehe etwa VfSlg 13.626/1993; 16.002/2000.

Aufgrund dieser Bestimmung sind alle obersten Organe in ihrer Rolle als solche in Bezug auf die Kontrolle der Datenverwendung durch die Kompetenzen der DSK eingeschränkt. Dies entspricht etwa auch den Kompetenzen der UVS gem Art 129a Abs 1 B-VG in Bezug auf Verwaltungsstrafverfahren oder AuvBZ, die diesen obersten Organen zuzurechnen sind.

V. Sonstige verfassungsrechtliche Implikationen

A. Gewaltenteilung

Eine weitere sich aus dem DSG ergebende Problematik bezieht sich auf die Gewaltenteilung. § 1 Abs 5 DSG stellt dabei eine eigenständige verfassungsgesetzliche Grundlage für die Gewaltenteilung im Zusammenspiel mit dem B-VG auf. Die DSK wird zur Entscheidung im Bereich der Verwaltung zuständig erklärt. Damit werden „Akte der Gesetzgebung oder der Gerichtsbarkeit“ von der Zuständigkeit des DSK ausgenommen. Es ist daher zu bestimmen, was unter Gesetzgebung und was unter Gerichtsbarkeit fällt, um den Zuständigkeitsbereich der DSK zu definieren. Generell ist festzuhalten, dass sowohl die Parlamentsverwaltung als auch die Justizverwaltung unter die Kontrolle der DSK fallen, da diese eben Akte der Verwaltung und weder der Gesetzgebung noch der Gerichtsbarkeit darstellen.

Eine besondere Fragestellung stellt sich iZm Akten im Rahmen des strafprozessualen Vorverfahrens. Da nicht mehr der Richter die Leitung des Vorverfahrens übernimmt, primär der Staatsanwalt, ist zu klären, wie sich diese Verschiebung auf die Kontrollmöglichkeiten der DSK auswirkt. Durch den neuen Art 90a B-VG werden **Staatsanwälte als Organe der Gerichtsbarkeit** verstanden, die „Ermittlungs- und Anklagefunktionen“ im strafprozessualen Vorverfahren wahrnehmen.[89] Sowohl in Art 90a B-VG als auch in § 1 Abs 5 DSG ist von einem funktionellen Organverständnis auszugehen, womit auch die Akte der Staatsanwaltschaft (und nicht nur die gerichtlichen Bewilligungen) unter § 1 Abs 5 DSG fallen und somit die DSK nicht für die Beurteilung dieser Akte zuständig ist.[90] Fraglich ist darüber hinaus, ob auch die Tätigkeiten der Sicherheitsbehörden im Rahmen der Kriminalpolizei von der Kontrolle der DSK ausgenommen werden. Für dieses Verständnis plädiert *Mayer*, der die Fragestellung anhand des § 31 DSG behandelt.[91]

B. Räumlicher Anwendungsbereich des DSG

Als weitere Verfassungsbestimmung ist der räumliche Anwendungsbereich des DSG gem § 3 DSG zu erwähnen, da spezifische Regelungen im Kontext

[89] Siehe dazu *Heißl/Lehner*, Staatsanwälte in der Verfassung, ZfV 2009, 191.

[90] Siehe dazu auch *Kunnert*, jusIT 2009, 104.

[91] *Mayer*, Die Sicherheitsbehörden im Dienst der Strafjustiz und die Zuständigkeit der Datenschutzkommission, ÖJZ 2007, 17.

der EU bzw des EU- Rechts vorgesehen sind. Das Territorialitätsprinzip (Anwendung des DSG nur auf innerstaatliche Datenverwendungen) wird dabei aufgeweicht und iSd Datenschutzes auf jene Datenverwendungen ausgedehnt, die für Zwecke eines in Österreich ansässigen Auftraggebers innerhalb der EU verwendet werden. Umgekehrt sieht aber auch § 3 Abs 2 DSG vor, dass in Österreich vorgenommene Datenverwendungen von ausländischen Auftraggebern innerhalb der EU nach dem „Recht des Sitzstaates des Auftraggebers“ zu behandeln sind. Ebenso findet das österreichische Recht keine Anwendung bei der bloßen „Durchführung“ von personenbezogenen Daten.

Die **Aufgabe des Territorialitätsprinzips** entspricht den europäischen Vorgaben[92] und ermöglicht einen freien Verkehr von personenbezogenen Daten iS eines Auftraggeberstaatsprinzips. Durch die implizite gegenseitige Anerkennung von Datenschutzstandards bzw die Vereinheitlichung derselben durch die DatenschutzRL[93] soll damit auch der grundrechtliche Schutz, den § 1 DSG gewährleistet, in allen Mitgliedstaaten der EU zur Verfügung stehen. Dabei ist auffällig, dass kein subsidiärer Schutz in jenem Staat besteht, in dem die Daten verwendet werden, wenn – aus welchen Gründen immer – der Schutz nicht im Auftraggeberstaat gewährleistet wird.[94]

C. Übergangsregelung im Polizeirecht

Eine verfassungsgesetzliche Übernahmeregelung gem § 61 Abs 4 DSG nahm Datenanwendungen gem § 17 Abs 3 DSG bis Ende 2007 vom Gesetzesvorbehalt gem § 1 Abs 2 DSG (Legalitätsprinzip) aus. Darunter fallen Angelegenheiten des Nachrichtendienstes („Schutz der verfassungsmäßigen Einrichtungen der Republik Österreich“), des Militärs („Sicherung der Einsatzbereitschaft des Bundesheeres“, „Sicherstellung der Interessen der umfassenden Landesverteidigung“), der Außen-, Wirtschafts- und Finanzpolitik Österreichs oder der EU sowie der Sicherheits- und Kriminalpolizei (§ 17 Abs 3 DSG). Ohne diese verfassungsgesetzliche Grundlage wäre die Bestimmung schon aufgrund von Art 18 B-VG als verfassungswidrig zu beurteilen gewesen. Die Übergangsregelung war sehr lange bemessen, ist aber letztlich ausgelaufen und hat etwa zu Anpassungen des Sicherheits- und Kriminalpolizeirechts geführt.[95] Auch wenn nun eine gesetzliche Grundlage für Datenanwendungen in diesen Bereichen erforderlich ist, sind derartige Datenanwendungen von der Meldepflicht gem § 17 DSG ausgenommen, wenn diese Ausnahme für den Zweck der Datenanwendung erforderlich ist (Abs 3 leg cit).

[92] So sind gem § 3 Abs 4 DSG Abweichungen nur in Angelegenheiten zulässig, die nicht dem Recht der EG unterliegen. Diese Bestimmung entfällt allerdings durch die DSG-Nov 2010.

[93] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates v 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281, 31 (DS-RL).

[94] Durch die geplante DSG-Nov 2010 erfolgt eine Anpassung über den EU-Raum hinaus auf die Mitgliedstaaten des EWR.

[95] Siehe die SPG-Novelle BGBl I 2007/114; RV 272, 23. GP, 1. XX

VI. Zusammenfassung und Ausblick

Das Datenschutzrecht erweist sich als eine durch Verfassungsrecht geprägte bzw geregelte Materie. Dabei kommt dem Grundrecht auf Datenschutz überragende Bedeutung zu. Darüber hinaus finden sich im Datenschutzrecht noch zahlreiche weitere verfassungsgesetzliche Bestimmungen, auch wenn die Anzahl derselben stark im Sinken begriffen ist.

Entscheidend ist es, die Differenz zwischen Datenschutzrecht im DSG und Datenverwendungsrecht im konkreten Einzelfall zu sehen. Während das Datenschutzrecht kompetenzrechtlich (primär) dem Bund zufällt, ist das Datenverwendungsrecht eine Adhäsionskompetenz.

Wie bereits im Einzelfall dargestellt, wird es bei allfälliger Umsetzung der geplanten DSG-Novelle 2010 zu unterschiedlichen Auswirkungen auf die verfassungsgesetzlichen Bestimmungen des DSG kommen; allerdings bleibt der Kerngehalt des Grundrechts auf Datenschutz erhalten.

Handbuch Datenschutzrecht

herausgegeben von

Dr. Lukas Bauer
Rechtsanwaltsanwärter in Wien

Mag. Sebastian Reimer
Legistischer Experte im Bundesministerium für Gesundheit

Wien 2009

facultas.wuv