Diplomstudium Rechtswissenschaften

Auskunftsrecht nach § 26 Datenschutzgesetz 2000 in der Praxis inklusive Ausblick auf die Datenschutz-Grundverordnung (VO 2016/679) ab 25.05.2018

Diplomarbeit aus Rechtsinformatik

zur Erlangung des akademischen Grades

eines Magisters der Rechtswissenschaften

der Rechtswissenschaftlichen Fakultät

an der Paris-Lodron-Universität Salzburg

Joachim Galileo Fasching, LLB.oec.

Matrikelnummer: 1121737

Betreuer: Ao. Univ.-Prof. Dr. Dietmar Jahnel

Fachbereich Rechtsinformatik/Datenschutzrecht

Salzburg, November 2016

Eidesstattliche Erklärung

Ich erkläre hiermit eidesstattlich, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe. Alle Stellen, die wörtlich oder inhaltlich den angegebenen Quellen entnommen wurden, sind als solche kenntlich gemacht. Die vorliegende Arbeit wurde bisher in gleicher oder ähnlicher Form noch nicht als Bachelor-/Master-/Diplomarbeit/Dissertation eingereicht.

Datum _____

Abbildungsverzeichnis

Inhalt

Abkürzungsverzeichnis

aA	anderer Ansicht
ABGB	Allgemeines Bürgerliches Gesetzbuch
ABl	Amtsblatt der Europäischen Union
Abs	Absatz
AEUV	Vertrag über die Arbeitsweise der europäischen Union, ABl C 2012/326, 47
Anm	Anmerkung
Art	Artikel
AVG	Allgemeines Verwaltungsverfahrensgesetz 1991 (idgF BGBl. I Nr. 161/2013)
B-VG	Bundes-Verfassungsgesetz
BAO	Bundesabgabenordnung (idgF BGBl. I Nr. 77/2016)
BSDG	Deutsches Bundesdatenschutzgesetz (idgF BGBl. I S. 162 vom 25.2.2015)
BfDI	Deutscher Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGBl	Bundesgesetzblatt
BMI	Bundesministerium für Inneres
BVB	Bezirksverwaltungsbehörde
B-VG	Bundes-Verfassungsgesetz
BVwG	Bundesverwaltungsgericht
BWG	Bankwesengesetz (idgF BGBl. I Nr. 50/2016)
bzw	beziehungsweise
ca	cirka
dh	das heißt
DSB	Datenschutzbehörde (ab 2014)
DSG	Datenschutzgesetz 2000 (idgF BGBl. I Nr. 83/2013)
DSK	Datenschutzkommission (bis 2013)
DSRL	Datenschutzrichtlinie (RL 95/46/EG)
DS-GVO	Europäische Datenschutz-Grundverordnung (VO 2016/679)
DVR	Datenverarbeitungsregister
ECG	E-Commerce-Gesetz
EGMR	Europäischer Gerichtshof für Menschenrechte
ErwGr	Erwägungsgrund
EStG	Einkommensteuergesetz 1988 (idgF BGBl. I Nr. 77/2016)
EuGH	Europäischer Gerichtshof
FN	Fußnote
GOG	Gerichtsorganisationsgesetz (idgF BGBl. I Nr. 50/2016)
GRC	Charta der Grundrechte der europäischen Union
IA	Initiativantrag

idgF	in der geltenden Fassung
insb	insbesondere
iVm	in Verbindung mit
JN	Jurisdiktionsnorm (idgF BGBl. I Nr. 87/2015)
KOV	Kontroll- und Ombudsmannverfahren nach § 30 DSG
lit	litera
mE	meines Erachtens
MeldeG	Meldegesetz 1991 (idgF BGBl. I Nr. 50/2016)
MinroG	Mineralrohstoffgesetz (idgF BGBl. I Nr. 80/2015)
mwN	mit weiteren Nachweisen
NO	Notariatsordnung (idgF BGBl. I Nr. 50/2016)
OGH	Oberster Gerichtshof
OLG	Oberlandesgericht
RAO	Rechtsanwaltsordnung (idgF BGBl. I Nr. 50/2016)
RIS	Rechtsinformationssystem des Bundes, abrufbar unter www.ris.bka.gv.at
RL	Richtlinie
Rsp	Rechtsprechung
RV	Regierungsvorlage
RZ	Randziffer
SPG	Sicherheitspolizeigesetz (idF BGBl. I Nr. 151/2004)
SVG	Signatur- und Vertrauensdienstegesetz (idgF BGBl. I Nr. 50/2016)
StF	Stammfassung
StPO	Strafprozessordnung 1975 (idgF BGBl. I Nr. 65/2016)
TKG	Telekommunikationsgesetz 2003 (idgF BGBl. I Nr. 6/2016)
ua	unter anderem
udgl	und dergleichen
uU	unter Umständen
uvm	und viele(s) mehr
VDSG	Schweizer Verordnung zum Bundesgesetz über Datenschutz
VfGH	Verfassungsgerichtshof
vgl	vergleiche
VO	Verordnung
VStG	Verwaltungsstrafgesetz (idgF BGBl. I Nr. 33/2013)
VVG	Verwaltungsvollstreckungsgesetz 1991 (idgF BGBl. I Nr. 33/2013)
VwGG	Verwaltungsgerichtshofgesetz 1985 (idgF BGBl. I Nr. 50/2016)
VwGH	Verwaltungsgerichtshof
WTBG	Wirtschaftstreuhandberufsgesetz (idgF BGBl. I Nr. 50/2016)

Z	Ziffer
zB	zum Beispiel
ZivMediatG	Zivilrechts-Mediations-Gesetz (idgF BGBl. I Nr. 29/2003)
ZPO	Zivilprozessordnung (idgF BGBl. I Nr. 94/2015)
ZustG	Zustellgesetz (idgF BGBl. I Nr. 33/2013)

1 Einleitung

Die öffentliche Debatte um Datenschutz ist in unterschiedlichen Ausprägungen parallel zum Aufkommen der Informationstechnologie seit rund 50 Jahren präsent, in Österreich reichen die Wurzeln in die 1970er Jahre zurück. Es folgten detaillierte Vorschriften zum Schutz personenbezogener Daten natürlicher Personen. Seit damals ist auf europäischer (ua RL 95/46/EG, Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte und des Europäischen Gerichtshofs) wie auf nationaler Ebene (ua Beschluss des Datenschutzgesetzes mit zahlreichen Novellen sowie darauf basierend die Einrichtung der Datenschutzkommission – nunmehr Datenschutzbehörde) viel geschehen. Hinzu kommt das Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen Nr. 108), welches ein rechtsverbindliches völkerrechtliches Instrument im Bereich des Datenschutzes darstellt. Der Schutz personenbezogener Daten erlangte mit dem Inkrafttreten des Vertrags von Lissabon im Dezember 2009 den Status eines Grundrechts, da die Charta der Grundrechte der Europäischen Union rechtlich bindend ist. Dies stellte einen Meilenstein im Datenschutzrecht dar und bildete die Grundlage eines fortschrittlichen Rechtsverständnisses im Zeitalter der digitalen Datenverarbeitung.[1]

Begriffe wie informationelle Selbstbestimmung oder das Recht auf Zugang zu den eigenen Daten werden nun auch abseits der juristischen Fachkreise diskutiert, das Bewusstsein um einen sorgsamen Umgang mit Daten wird dabei sensibilisiert. Dabei sind durchaus gegensätzliche Interessen zu vereinbaren: datenverarbeitende Unternehmen benötigen mitunter hohe finanzielle sowie personelle Ressourcen, um diese Vorgaben gesetzeskonform umzusetzen. Speziell bei dem in dieser Diplomarbeit behandelten Auskunftsbegehren – also grob gesprochen der Auskunft darüber, welche Daten über die eigene Person verarbeitet werden – stellen sich spannende Konfliktsituationen dar: häufig wird bei der Auskunftserteilung der Eingriff in fremde und dabei ebenso schutzwürdige Interessen zu prüfen sein (beispielsweise öffentliche Interessen wie die Verfolgung von Straftaten, gegengelagerte Interessen des Auftraggebers, etwa beim Schutz von Geschäftsgeheimnissen wie der Verwendung spezieller Algorithmen im Datenverarbeitungsprozess oder überwiegende Interessen Dritter, etwa bei Beauskunftung im Zusammenhang mit Überwachungskameras an öffentlichen Plätzen). Hinzu kommen weitere Grundrechte mit anderen Schutzbereichen: Meinungsäußerungsfreiheit, Schutz des Eigentums, Freiheit von Kunst und Wissenschaft, Schutz der Privatsphäre und der Korrespondenz sowie Zugang zu Dokumenten als Teil der Kommunikationsfreiheit[2].

[1] Handbuch zum europäischen Datenschutzrecht, 13-22.
[2] Handbuch zum europäischen Datenschutzrecht, 22-35.

Um einen prominenten Fall der vergangenen Jahre, in denen das geltende Datenschutzrecht bislang vergleichsweise zahnlos wirkte, aufzugreifen, wird in Folge kurz die Rechtssache Schrems gegen Facebook thematisiert. Maximilian Schrems wollte 2011 herausfinden, welche Daten der Social Media-Anbieter Facebook (mit Niederlassung in Irland) über ihn speichert. Facebook beauskunftete lediglich Teile des gesamten Datenvolumens, Schrems klagte daraufhin vor verschiedenen Rechtsschutzinstanzen und hat bis heute – fünf Jahre nach Einbringung des Auskunftsbegehrens – immer noch keine zufriedenstellende Auskunft erhalten.[3] Die wirtschaftlichen Rahmenbedingungen[4] (E-Commerce, Big Data, Internet of things, Einbau dutzender Sensoren in Maschinen) haben sich in den letzten Jahren deutlich gewandelt - aus dieser Perspektive ist eine Stärkung der Informationsmöglichkeiten des Betroffenen gegenüber dem Auftraggeber durchaus wünschenswert[5]. Diese wird in der Europäischen Datenschutz-Grundverordnung (VO 2016/679), welche am 25. Mai 2018 in Geltung tritt, bereits berücksichtigt.[6]

Die aktuelle gesetzliche Regelung zum Auskunftsrecht im § 26 des österreichischen Datenschutzgesetzes aus dem Jahr 2000 wirft an manchen Stellen Fragen auf. Dies mag daran liegen, dass in Österreich einige Bestimmungen aus dem DSG 1978 übernommen bzw manche Bestimmungen der Richtlinie 95/46/EG nicht korrekt umgesetzt wurden und daher das aktuelle DSG stellenweise einer richtlinienkonformen Auslegung bedarf. Hinzu kommt, dass in den Medien bereits vor dem Inkrafttreten der Datenschutz-Grundverordnung, die jedenfalls eine Angleichung der unterschiedlichen Datenschutzniveaus in Europa mit sich bringen wird, verschiedene Versionen der künftigen Datenschutzstandards kursierten und bei den Betroffenen für Verwirrung sorgten. Einige Auftraggeber kommen aus unterschiedlichen Gründen ihren gesetzlichen Auskunfts- und Informationspflichten nicht ordnungsgemäß nach, was in der Praxis wiederum zu einem vermeidbaren Mehraufwand aufseiten der Betroffenen sowie der in weiterer Folge in Anspruch genommenen Rechtsschutzinstanzen führt.

Ziel der vorliegenden Arbeit ist es daher, anhand von konkreten Fallbeispielen und Rechtsvergleichung (Deutschland und Schweiz) die bestehenden Unklarheiten zu thematisieren und ein umfassendes Nachschlagewerk zu schaffen, in dem sowohl aus Betroffenensicht als auch aus Sicht des Auftraggebers (für die Verarbeitung Verantwortlichen) bzw Dienstleisters (Auftragsverarbeiters) eine schematische Anleitung dargestellt wird. An den entsprechenden Stel-

[3] http://www.europe-v-facebook.org/DE/Anzeigen/anzeigen.html, abgerufen am 25. Mai 2016.
[4] *Auer*, Das Grundrecht auf Datenschutz im Unternehmen, 29-33.
[5] *Schweizer* in Passadelis/Rosenthal/Thür (Hrsg.), Datenschutzrecht, 36-40.
[6] Exemplarisch sind hier die Meldungen von Datenschutzverletzungen in Art 33 Abs 1 DS-GVO sowie die Datenschutz-Folgeabschätzung in Art 35 Abs 1 DS-GVO zu nennen. Näheres dazu in *BfDI*, Datenschutz-Grundverordnung, 23-24.

len wird auf weitere Betroffenenrechte (Geheimhaltung, Richtigstellung, Löschung und Widerspruch), Informationspflichten, Rechtsschutz und Verwaltungsstrafbestimmungen eingegangen. Hierfür werden Lehrbücher, Kommentare, Entscheidungen der Datenschutzbehörde (zuvor Datenschutzkommission), höchstgerichtliche Judikatur und nicht zuletzt Praxiserfahrungen des Autors herangezogen. In weiterer Folge werden konkrete Handlungsanweisungen (Entscheidungsbäume und Formulare bzw Vordrucke) geliefert, um eine raschere Abwicklung der Auskunftsbegehren zu ermöglichen.

Abschließend werden die Änderungen, die sich durch die ab dem 25. Mai 2018 europaweit anwendbare Datenschutz-Grundverordnung im Hinblick auf die Betroffenenrechte (insbesondere Auskunftsrecht) ergeben, diskutiert.

Mit dem Ziel der besseren Lesbarkeit wurden in der vorliegenden Arbeit die meisten Begriffe nicht gegendert und auf die Anführung der akademischen Titel verzichtet. Dennoch soll zum Ausdruck gebracht werden, dass eine geschlechtersensible Ausdrucksweise wesentlicher Bestandteil unserer Sprache ist, ebenso die Wertschätzung gegenüber akademischen Auszeichnungen. Alle zitierten Gesetzesstellen ohne Angabe des Gesetzes beziehen sich auf das Datenschutzgesetz 2000.

2 Grundlegende Definitionen im Datenschutzrecht

In diesem Abschnitt werden grundlegende Definitionen aus dem österreichischen Bundesgesetz über den Schutz personenbezogener Daten („Datenschutzgesetz 2000“ bzw kurz „DSG 2000“), StF: BGBl. I Nr. 165/1999, idgF iVm der europäischen Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr („Datenschutzrichtlinie“), ABl L 281 vom 23.11.1995, dargestellt.

2.1 Grundrecht auf Datenschutz

Das im § 1 DSG normierte Grundrecht auf Datenschutz steht im Verfassungsrang und führt zu einem Anspruch auf Geheimhaltung personenbezogener Daten. Dieses Grundrecht soll den Schutz des Betroffenen vor Ermittlung seiner Daten sowie den Schutz vor der Weitergabe seiner Daten bewirken. Eingeschränkt wird dieser Anspruch auf Geheimhaltung der personenbezogenen Daten durch das Bestehen eines schutzwürdigen Interesses des Betroffenen. Dieses Interesse ist nicht gegeben, sofern die Daten allgemein verfügbar sind (die allgemeine Zugänglichkeit ist zum Zeitpunkt der beabsichtigten Datenverwendung erneut zu prüfen, nicht bloß bei der erstmaligen Erhebung!) oder nicht auf den Betroffenen rückführbar sind.[7] Von besonderer Bedeutung ist die unmittelbare Drittwirkung, die sich aus Art 8 GRC iVm Art 1 Abs 1 DSRL ergibt: das Recht auf Datenschutz kann nicht nur bei staatlichen Eingriffen, sondern vor allem auch gegenüber (marktmächtigen) Unternehmen und Privatpersonen vor den ordentlichen Gerichten geltend gemacht werden.[8] Im § 1 Abs 3 DSG werden die Betroffenenrechte, welche parallel zum Anspruch auf Geheimhaltung bestehen, konkretisiert:

- Recht auf Auskunft darüber, wer welche Daten verarbeitet, Quelle und Zweck der Datenverarbeitung und Übermittlungsempfänger
- Recht auf Richtigstellung unrichtiger Daten
- Recht auf Löschung unzulässigerweise verarbeiteter Daten

Diese Diplomarbeit behandelt primär den Auskunftsanspruch des Betroffenen und den Umgang damit aufseiten des Auftraggebers, Dienstleisters oder Übermittlungsempfängers. Auf die weiteren Betroffenenrechte (Geheimhaltung, Richtigstellung und Löschung) wird an den entsprechenden Stellen näher eingegangen.

---

[7] *Lehner/Lachmayer* in Bauer/Reimer (Hrsg.), Handbuch Datenschutzrecht, 96-100.

[8] Vgl *von Danwitz*, Die Grundrechte auf Achtung der Privatsphäre und auf Schutz personenbezogener Daten, DuD, 581(584f) mwN. *von Danwitz* beschreibt das Grundrecht auf Datenschutz im Kontext marktmächtiger Unternehmen, deren Interessen in Konflikt mit der informationellen Selbstbestimmung des Einzelnen geraten.

2.2 Räumlicher und sachlicher Anwendungsbereich, Ausnahmen

Die Gesetzgebungskompetenz kommt gemäß § 2 dem Bund nur in Angelegenheiten des Schutzes personenbezogener Daten im automationsunterstützten Datenverkehr zu. Da die DSRL jedoch auch manuelle Dateien umfasst, wurden neun Landesdatenschutzgesetze erlassen, um die DSRL in ihrem gesamten Anwendungsbereich umzusetzen. § 58 normiert jedoch, dass die einfachgesetzlichen Bestimmungen des DSG auf die manuellen Dateien anwendbar sind.[9] Der VwGH ergänzte: „Hinsichtlich Daten außerhalb des automationsunterstützten Datenverkehrs (§ 2 Abs 1 DSG 2000) können die in den bundesgesetzlichen, einfachgesetzlichen Bestimmungen der §§ 26, 27 und 28 DSG 2000 normierten Rechte auf Auskunft, Richtigstellung, Löschung und Widerspruch aus Gründen der verfassungsrechtlichen Kompetenzverteilung zwischen Bund und Ländern nur auf Daten in jenen Angelegenheiten bezogen werden, für die eine Kompetenz des Bundesgesetzgebers besteht.“[10] Die Problematik der manuellen Dateien ist mE jedoch von geringer praktischer Relevanz, da kaum noch jemand manuelle strukturierte personenbezogene Dateien in größerem Umfang nutzt – mitunter mag dies mit ökonomischen Überlegungen zu tun haben.

Der räumliche Anwendungsbereich beschränkt sich gemäß § 3 DSG auf Personen mit Sitz bzw Niederlassung in Österreich. Grundsätzlich ist das DSG auf die Verwendung von personenbezogenen Daten im Inland anzuwenden – mit der Ausnahme des Sitzstaatsprinzips. Wenn also ein Auftraggeber seinen Sitz in einem anderen EU-Staat hat (und keine Niederlassung iSd § 4 Z 15 in Österreich unterhält) und Daten in Österreich verarbeitet, so gilt das Datenschutzrecht des Sitzstaats.[11] Die DSK schloss ihre Zuständigkeit in einem Fall aus, in der von SWIFT (mit Sitz in Belgien, ohne österreichische Niederlassung) Auskunft begehrt wurde.[12] Das bedeutet allerdings, dass eine juristische Person wie die Facebook Ireland Ltd., die in Europa lediglich eine Niederlassung in Irland hat, nicht dem österreichischen Datenschutzgesetz unterliegt. Im Praxisabschnitt dieser Diplomarbeit wird ein weiterer Fall vorgestellt, in welchem ein Unternehmen mit einer .at-Domain in Österreich keine Niederlassung betreibt und daher lediglich im Sitzstaat eine Beschwerde an die dortige Landesdatenschutzbehörde möglich war. Eine derartige Konstellation kann mitunter zu einer sechsmonatigen Bearbeitungsdauer führen, bis der Beschwerdeführer eine zufriedenstellende Antwort vonseiten der Rechtsschutzinstanz vorliegen hat. In diesem Bereich bringt die DS-GVO eine Veränderung mit sich („federführende Datenschutzbehörde“ im „One-Stop-Shop-Mechanismus“), auf diese wird abschließend näher eingegangen. Sofern der datenverwendende Rechtsträger jedoch keinen Sitz in einem EU-Mitgliedsstaat hat, gilt als Anknüpfungspunkt zu einer nationalen

[9] *Dohr/Pollirer/Weiß/Knyrim*, DSG, 51-54.
[10] VwGH 21.10.2004, 2004/06/0086 = VwSlg 16477 A/2004.
[11] *Dohr/Pollirer/Weiß/Knyrim*, DSG, 55-56.
[12] DSK 21.3.2007, K121.245/0009-DSK/2007.

Rechtsordnung jeweils der Ort der tatsächlichen Datenverwendung – dies mag mitunter in der Praxis schwierig feststellbar sein, wenn man an international tätige Firmen mit sogenannten „Serverfarmen“ auf der ganzen Welt denkt.

Der sachliche Anwendungsbereich des DSG wird durch zahlreiche Ausnahmen eingeschränkt, dazu zählen:

- § 45: ausschließlich persönliche oder familiäre Tätigkeiten („Private Zwecke“), sofern die verarbeiteten Daten vom Betroffenen selbst mitgeteilt wurden oder auf rechtmäßige Weise zugekommen sind.[13] Dies hat zur Konsequenz, dass Daten für den privaten Gebrauch nicht der Pflicht zur Auskunftserteilung, Richtigstellung und Löschung unterliegen. *Kotschy* sieht hingegen bei einer Videoüberwachung durch Private im Normalfall den Schutz vor strafbaren Handlungen – dies ist nicht vom Begriff der „ausschließlich persönlichen oder familiären Tätigkeit“ gedeckt und führt dazu, dass derartige Datenanwendungen sehr wohl auch im vermeintlich privaten Umfeld der Auskunftspflicht im DSG unterliegen.[14]
- § 46: wissenschaftliche oder statistische Untersuchungen („Wissenschaftliche Forschung und Statistik“), sofern diese keine personenbezogenen Ergebnisse zum Ziel haben und der Personenbezug der Daten im frühestmöglichen Stadium zumindest teilweise beseitigt wird.[15] Hierbei darf der Auftraggeber öffentlich zugängliche Daten oder Daten, die er für andere Untersuchungen oder andere Zwecke zulässigerweise ermittelt hat oder für ihn nur indirekt personenbezogene Daten verwenden. Im § 6 Abs 1 Z 2 wird das „Zweckbeschränkungsprinzip“ ausgehebelt, dort ist allerdings die Weiterverwendung der Daten für wissenschaftliche und statistische Zwecke explizit normiert.[16]
- § 48: der Umstand, dass auf Datenverwendungen im Rahmen von publizistischen Tätigkeiten im Sinne des Mediengesetzes von Medienunternehmen, Mediendiensten und deren Mitarbeitern die einfachgesetzlichen Bestimmungen des DSG nur eingeschränkt anwendbar („Medienprivileg“) sind.
- § 48a: besondere Bestimmungen für die Datenverwendung im Katastrophenfall.[17]

Parallel zu den vorgenannten Ausnahmen kann ein Auftraggeber die Auskunftspflicht insb betreffend des nicht-aktuellen Datenbestands negieren, sofern die Auskunftserteilung für ihn mit

[13] *Dohr/Pollirer/Weiß/Knyrim*, DSG, 281-282.
[14] *Kotschy*, Videoüberwachung, 265.
[15] *Dohr/Pollirer/Weiss/Knyrim*, DSG, 288-289.
[16] *Stärker*, DSG, 61.
[17] Siehe Begriff Katastrophenfall, 47.

einem unverhältnismäßig hohen Aufwand verbunden wäre. Hierzu wird im Praxisabschnitt dieser Diplomarbeit ein Fall aufbereitet[18].

2.3 Personenbezogene Daten

Vom Schutz des DSG sind nur personenbezogene Daten umfasst, das bedeutet im Umkehrschluss, dass Daten ohne Personenbezug nicht in den Anwendungsbereich des DSG fallen. Die Identität des Betroffenen muss dabei bestimmt oder bestimmbar sein. *Knyrim*[19] listet zahlreiche Informationen/Datenkategorien auf, die mit einer Person oder einem Unternehmen in Verbindung stehen oder gebracht werden können. Dazu zählen „klassische" Daten wie Name, Adresse, Geburtsdatum[20]/Sozialversicherungsnummer[21] – aber auch Rufnummer[22]/IP-Adresse[23], Werturteile/Leumund[24], biometrische Daten, Kontonummer[25]/Wirtschaftsdaten[26], Bild-[27] und Tondokumente[28] sowie Standortdaten. Die Bestimmbarkeit ist gegeben, wenn die Identifizierung des Betroffenen ohne unangemessene Anstrengungen („vernünftigerweise" verwendete Mittel[29]) möglich ist. Dabei muss einem Bescheid der DSK zufolge die Verwendung von Namen Betroffener nicht beabsichtigt sein – sobald die die Person beschreibenden Datenarten von einer hohen Dichte sind, sodass daraus Rückschlüsse auf einzelne Betroffene möglich sind, ist diese Verwendung der Verarbeitung direkt personenbezogener Daten gleichzustellen.[30] Die Richtigkeit einer Angabe spielt für die Qualifikation als „personenbezogenes Datum" keine Rolle.[31]

---

[18] Siehe Begriff Aufwand, 50.
[19] *Knyrim*, Datenschutzrecht³, 37-38.
[20] DSK 17.12.2010, K121.636/0010-DSK/2010, ebenso DSK 23.3.2001, K210.380/001-DSK/2001; DSK 20.1.2004, K120.888/001-DSK/2004.
[21] DSB 23.5.2014, DSB-D213.131/0002-DSB/2014.
[22] DSK 9.8.2006, K121.109/0006-DSK/2006.
[23] DSK 29.9.2006, K213.000/0005-DSK/2006.
[24] VwGH 27.6.2007, 2007/04/0105 und ausdrücklich AB 1024 der Beilagen XIV. GP, 4 zu § 3 Z 1.
[25] DSK 20.7.2011, K212.469/0008-DSK/2011.
[26] VfGH 29.9.2012, B54/12 ua = VfSlg 19673.
[27] DSK 13.12.2013, K202.128/0004-DSK/2013. In einer weiteren Entscheidung stellte die DSK bei der Bildaufzeichnung auf die Absicht der Identifizierung der darauf vorhandenen Personen ab, um auf personenbezogene Daten schließen zu können. Ein Nicht-Auftraggeber (jemand, der keine personenbezogenen Daten verarbeitet) unterliegt nicht der Auskunftspflicht nach § 26 – DSK, 11.10.2005, K121.036/0014-DSK/2005.
[28] RL 95/46/EG, 16. ErwGr.
[29] Ausdrücklich RL 95/46/EG, 26. ErwGr – abweichend jedoch VwGH 8.9.2009, 2008/17/0152 = VwSlg 17729 A/2009. Bei dieser Entscheidung ging es um die Weitergabe personenbezogener Daten (Bild- und Messdaten einer Radarüberwachungsanlage) an die Bezirkshauptmannschaft – durch die Weitergabe wurden jedoch nicht schutzwürdige Geheimhaltungsinteressen des Fahrzeughalters verletzt, wenn die Behörde auf entsprechender gesetzlicher Grundlage einschreitet.
[30] DSK 5.4.2006, K202.046/0012-DSK/2006.
[31] DSB 5.9.2014, DSB-D122.105/0015-DSB/2014.

In die Kategorie der indirekt personenbezogenen Daten fallen Daten, sobald der Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann.[32] Derartige Daten unterliegen gemäß § 29 nicht den in §§ 26 bis 28 normierten Rechten.[33]

Pseudonymisierte Daten haben verschlüsselte Kennungen. Anonymisierte Daten enthalten keine Kennungen mehr und sind unter keinen Umständen auf Betroffene rückführbar. Pseudonymisierte Daten gelten im Unterschied zu anonymisierten Daten als personenbezogen und unterliegen demzufolge ebenfalls dem Anwendungsbereich des DSG.[34] Da für indirekt personenbezogene Daten im Vergleich zu pseudonymisierten Daten unterschiedliche Rechtsfolgen vorgesehen sind, sind weitere Unterscheidungsmerkmale anzuführen. ME ist die Besonderheit von pseudonymisierten Daten, dass die dahinterstehende Person (beispielsweise ein Musiker, Schriftsteller oder Fotograf) einer breiten Öffentlichkeit bekannt sein kann und man durch entsprechende Recherchen (durch rechtlich zulässige Mittel) rasch Rückschlüsse auf eine bestimmte Person erhält. Künstler- oder Nicknamen fallen folglich in die Kategorie der pseudonymisierten Daten, da sie vom Auftraggeber einer Datenanwendung (beispielsweise Künstleragentur) zulässigerweise einem Betroffenen zugeordnet werden können – daher unterliegen diese Daten dem Anwendungsbereich des DSG.

Beispiele:

Nicht personenbezogene Daten	Die Wetterstation Salzburg-Karolingerbrücke hat am 24.05.2016 um 16:00 Uhr den Wert von +15,7° C aufgezeichnet.
Personenbezogene Daten	Joachim Galileo Fasching hat am 24.05.2016 um 16:01 Uhr am PC 123 im Netzwerk XYZ die Webseite www.uni-salzburg.at aufgerufen.
Indirekt personenbezogene Daten	Der KFZ-Lenker mit dem Kennzeichen S 123 ABC hat eine Verkehrsübertretung begangen (nur für ausgewählte Personen mit rechtlich zulässigen Mitteln bestimmbar).
Pseudonymisierte Daten	Nutzer „Leserreporter5020“ hat das Foto „salzburg.jpg“ bearbeitet.
Anonymisierte Daten	Irgendein (nicht näher konkretisierter) Nutzer hat das Foto „salzburg.jpg“ bearbeitet.

[32] DSK 18.11.2009, K121.526/0028-DSK/2009.
[33] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000, 110. Bei indirekt personenbezogenen Daten ist dem Auftraggeber der Datenanwendung der Personenbezug nicht bekannt.
[34] *Stärker*, DSG, 48.

2.4 Rollenverteilung im § 4 DSG

Das Datenschutzrecht kennt verschiedene Rollen: in der Folge werden der Betroffene, der Auftraggeber, der Dienstleister und der Übermittlungsempfänger näher charakterisiert.

2.4.1 Betroffener

Der Betroffene iSd § 4 Z 3 DSG ist jede vom Auftraggeber verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet werden. Eigene Rechtspersönlichkeit wird bei Personengesellschaften nicht verlangt, sodass beispielsweise auch eine Gesellschaft bürgerlichen Rechts (GbR)[35] eine betroffene Person sein kann.[36]

2.4.2 Auftraggeber

Als Auftraggeber (Wortlaut der DSRL: „für die Verarbeitung Verantwortlicher“) wird jene Person bezeichnet, die alleine oder gemeinsam mit anderen die Entscheidung[37] getroffen hat, Daten für einen bestimmten Zweck zu verarbeiten. Dabei spielt es keine Rolle, ob die Daten automationsunterstützt oder manuell verarbeitet werden[38] - jedoch muss eine tatsächliche Verarbeitung gegeben sein, die bloße Vorhaltung technischen Equipments – obgleich im vorliegenden Fall eine baldige Inbetriebnahme beabsichtigt war – reicht zur Qualifikation als Auftraggeber nicht aus[39]. Unter diesen Begriff können natürliche oder juristische Personen, Personengemeinschaften[40], Organe einer Gebietskörperschaft (Bund-, Länder- und Gemeindeorgane) sowie Geschäftsapparate solcher Organe (Bundesministerium, Amt der Landesregierung, Magistrat) fallen.[41]

In der Regel wird die Identität des Auftraggebers bekannt sein – etwa, weil dieser zum Betroffenen in einer langjährigen Geschäftsbeziehung steht. Die Identität kann aber auch durch die Meldepflicht (§ 17), die Informationspflicht (§ 24) oder die Offenlegungspflicht (§ 25) bekannt sein. Die Verletzung dieser Pflichten ist zwar mit einer Verwaltungsstrafe gemäß § 52 Abs 2 Z 1 und Z 4 sanktioniert – die Identität des Auftraggebers ist aber im Einzelfall für den Betroffenen schwer zu ermitteln. Der Auskunftswerber, der zugleich Betroffener der Datenverarbeitung und Anzeiger im Verwaltungsstrafverfahren ist, kann die Identität des Auftraggebers somit nur über sein Recht auf Auskunft nach den Auskunftspflichtgesetzen des Bundes bzw der Länder eruieren, da der Betroffene im Verwaltungsstrafverfahren mangels Parteistellung

---

[35] VwGH 27.4.2012, 2010/17/0003 = VwSlg 18396 A/2012 – hier qualifizierte der VwGH eine GbR potenziell als Auftraggeber oder Dienstleister iSd § 4 Z 4 bzw. Z 5, die Rechte und Pflichten kommen den Gesellschaftern zu, siehe dazu VwGH 22.11.2005, 2003/03/0041.
[36] *Lehner* in Bauer/Reimer (Hrsg.), Handbuch Datenschutzrecht, 124.
[37] Die faktische Entscheidung reicht aus – unabhängig von der Zulässigkeit der Entscheidung: DSK 21.3.2007, K121.245/0009-DSK/2007 ebenso DSK 16.10.2009, K121.533/0017-DSK/2009.
[38] VfGH 30.11.2005, B1158/03 – B200/04, B764/04, B574/04, B1325/04.
[39] DSK 26.9.2006, K121.150/0014-DSK/2006.
[40] DSK 24.4.2001, K202.010/002-DSK/2001.
[41] *Lehner* in Bauer/Reimer (Hrsg.), Handbuch Datenschutzrecht, 124-125.

nicht über das Ergebnis der Identitätsausforschung zu informieren ist. In diesem Fall liegt laut *Jahnel* ein überwiegendes Interesse des Auskunftswerbers an der Auskunftserteilung vor, sodass die Behörde sich nicht auf Amtsverschwiegenheit bzw schutzwürdige Geheimhaltungsinteressen des Beschuldigten berufen kann.[42]

Die Betroffenenrechte sind gegenüber dem Auftraggeber auszuüben. In einer Entscheidung verlangte der Beschwerdeführer von der Datenschutzkommission die Feststellung zur Verpflichtung der Löschung gemäß § 27 DSG. Der Beschwerdeführer hatte kein vorangehendes Löschungsbegehren an den Beschwerdegegner gerichtet, sondern sich direkt an die DSK gewendet. Die DSK war in diesem Fall aber nicht Auftraggeber der Datenverarbeitung und wies die Beschwerde ab.[43] Der VwGH hatte die ebenfalls die Auftraggebereigenschaft zu prüfen: hierbei war es entscheidungswesentlich, wer im Hinblick auf die Errechnung der "Scoring-Werte" als derjenige anzusehen ist, der die Entscheidung zur Verarbeitung der Daten getroffen hat. Wie sich aus § 4 Z 4 DSG ergibt, ist die Auftraggebereigenschaft unabhängig davon, ob derjenige, der die Entscheidung zur Verarbeitung getroffen hat, die Verarbeitung selbst durchführt oder hierzu einen anderen heranzieht. Die Berechnung der "Scoring-Werte" erfolgte auf jeweils ausdrücklichen Auftrag der Kunden der D GmbH und nach einem von diesem vorgegebenen Algorithmus. Daher wird die konkrete Entscheidung zur Verarbeitung der Daten in einer bestimmten Weise (nach dem vorgegebenen Algorithmus) vom jeweiligen Kunden getroffen. Auch die weiteren Bestimmungen in § 4 Z 4, nach denen in bestimmten Fällen nicht derjenige, der einem anderen Daten zur Herstellung eines von ihm beauftragten Werkes überlässt, Auftraggeber ist, bzw ein solcher ein Werk in Auftrag gebender Vertragspartner dann nicht Auftraggeber ist, wenn er seinem Auftragnehmer die Verarbeitung der überlassenen Daten ausdrücklich untersagt, sprechen nicht gegen die Annahme, dass in einer Konstellation wie im Beschwerdefall die Kunden der D GmbH als Auftraggeber anzusehen sind. Es trifft nämlich gerade nicht zu, dass die Kunden der D GmbH die Verarbeitung der Daten ausdrücklich untersagt hätten (sie haben vielmehr den Auftrag hierzu gegeben). Es braucht daher nicht - wie dies in der Beschwerde im Hinblick auf § 4 Z 5 getan wird - näher untersucht werden, ob im Beschwerdefall das Tatbestandselement "Überlassung der Daten", wie dieses in § 4 Z 4 letzter Satz ebenfalls verwendet wird, zutrifft, wenn die Daten wie im Beschwerdefall offensichtlich nicht von den Auftraggebern der Werkleistung dem Auftragnehmer zur Verfügung gestellt werden, sondern sich bereits beim Werknehmer (der mitbeteiligten D GmbH) befinden. § 4 Z 4 letzter Satz greift im Beschwerdefall mangels Untersagung der Verarbeitung der Daten durch die Kunden keinesfalls ein; er schließt somit die Auftraggebereigenschaft der Kunden nicht aus. Für die Beantwortung der Frage, wen die Auskunftspflicht nach § 26 Abs 1 trifft, ist nur erforderlich, den Auftraggeber im Sinn des § 4 Z 4 festzustellen. Nach dem Vorgesagten

[42] *Jahnel*, Datenschutzrecht, 367f in 7/12.
[43] DSK 20.7.2007, K121.289/0006-DSK/2007.

ergibt sich, dass hinsichtlich der Errechnung der "Scoring-Werte" die D GmbH nicht als Auftraggeberin im Sinn des § 4 Z 4 anzusehen war. Ob sie nach der Definition des § 4 Z 5 als Dienstleisterin zu bezeichnen war, ist gleichwohl nicht entscheidungsrelevant.[44]

Eine weitere Entscheidung der DSK hatte die Frage zum Gegenstand, ob das Auskunftsbegehren beim Auftraggeber tatsächlich einlangen muss. In diesem Fall wurde vom Beschwerdegegner angegeben, dass er das Auskunftsbegehren nicht erhalten habe, der Beschwerdeführer konnte keinen Aufgabenachweis erbringen. Die Kenntnis des Auftraggebers vom Auskunftsbegehren wird insb aus dem Wortlaut des § 26 Abs 1 DSG abgeleitet, wonach der Auskunftswerber dies „schriftlich verlangen“ müsse.[45]

2.4.3 Dienstleister

Jene Person, welcher von einem datenschutzrechtlichen Auftraggeber Daten zur Herstellung eines Werkes[46] überlassen werden, wird als Dienstleister (Wortlaut der DSRL: „Auftragsverarbeiter“) bezeichnet. Die Hauptverantwortung für die Einhaltung und Berücksichtigung aller Datenschutzaspekte liegt jedoch weiterhin beim Auftraggeber. Das Überlassen von Daten an den Dienstleister unterliegt gegenüber dem Betroffenen nicht der Auskunftspflicht nach § 26 DSG.[47] Dies stellt insofern eine Erleichterung für Auftragnehmer dar, da sie neben der Vereinbarung zur Auftragserfüllung lediglich den besonderen Pflichten für Dienstleister des § 11 DSG unterliegen. Ein Host-Provider iSd § 16 ECG ist ein Dienstleister, sofern durch dessen Tätigkeiten die Übermittlung von personenbezogenen Daten ermöglicht wird.[48] Sollte jedoch der Auftragnehmer die Vorgaben des Auftraggebers missachten oder überschreiten[49], so wird der Dienstleister selbst zum datenschutzrechtlichen Auftraggeber.[50]

Diese – auf den ersten Blick nicht einfach zu überblickende – Konstellation aus Auftraggeber und Dienstleister leitet sich einerseits aus praktischen Überlegungen (Notwendigkeit der gesetzlichen Legitimation und Normierung des Outsourcings von Datenverarbeitungstätigkeiten), andererseits aber aus rechtlichen Erwägungen ab. Bloß der Auftraggeber kann über die betroffenen Daten verfügen, also beispielsweise einem Richtigstellungs- oder Löschungsbegehren nachkommen. Weiters wird es für einen verhältnismäßig kleinen Dienstleister, der jedoch ein hohes Datenverarbeitungsvolumen bewältigt, nicht zumutbar sein – ungeachtet der rechtlichen Zulässigkeit –, alle Auskunftsbegehren selbständig zu beantworten (insb im Hinblick auf

---

[44] VwGH 11.12.2009, 2009/17/0223.
[45] DSK 22.4.2005, K120.879/0003-DSK/2005.
[46] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/59 in § 26 Anm 38, halten fest, dass die Nichtbekanntgabe von Namen und Adresse des datenschutzrechtlichen Auftraggebers durch den Auftraggeber des Werkes (den Klienten) einer Verweigerung der Auskunftsleistung gleichzuhalten sei.
[47] DSK 27.8.2010, K121.616/0012-DSK/2010.
[48] DSK 14.11.2003, K120.819/006-DSK/2003.
[49] DSK 20.10.2006, K121.155/0015-DSK/2006.
[50] *Lehner* in Bauer/Reimer (Hrsg.), Handbuch Datenschutzrecht, 125.

die gesetzlich geforderte Identitätsprüfung: der Auftragnehmer wird sich regelmäßig dabei unsicher sein, ob er die Daten dem Auskunftswerber mitteilen darf). Daher ist das Auskunftsbegehren direkt an den Auftraggeber der Datenverarbeitung zu stellen. Wird nun an den Dienstleister ein Auskunftsbegehren gestellt, so hat dieser gestützt auf § 26 Abs 10 DSG dem Auskunftswerber mitzuteilen, dass er für die betreffenden Anwendungen kein Auftraggeber ist und daher auch keine eigenständigen Datenverarbeitungen vornimmt. Sofern das Auskunftsbegehren erkennen lässt, dass der Dienstleister irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung gehalten wird, so hat der Dienstleister das Auskunftsbegehren direkt an den eigentlichen Auftraggeber weiterzuleiten. Die achtwöchige Frist zur Auskunftserteilung beginnt bereits ab dem Einlangen beim Dienstleister zu laufen.[51] Auch wenn sich der Auftraggeber eines Dienstleisters bedient, so trifft ihn immer noch die alleinige Auskunftspflicht (und nicht etwa den Dienstleister).[52] Die DSB hat in diesem Zusammenhang festgestellt, dass eine Verletzung im Recht auf Auskunft vorliegt, wenn der Dienstleister den Auftraggeber lediglich darüber in Kenntnis setzt, dass ein Auskunftsbegehren an ihn gerichtet wurde (anstatt ihm dieses unverzüglich weiterzuleiten, wie in § 26 Abs 10 normiert).[53] Die Auswirkungen der DSG-Novelle 2010 sind positiv hervorzuheben, da in dieser Konstellation dem Auskunftswerber der Irrtum nicht zu Last gelegt wird, sondern im Gegenteil sogar noch eine gewisse Form der Kooperation zwischen Dienstleister und Auftraggeber gefordert wird, diese Art der Zurechenbarkeit ist auch von der Gehilfenhaftung nach ABGB bekannt (wenn sich jemand eines Gehilfen bedient, so ist ihm dessen Verschulden – wenngleich in diesem Fall auch nur der zeitliche Verzug – anzulasten, vgl § 33 Abs 2 DSG; § 9 VStG). Die Haftung wird dabei beim Auftraggeber konzentriert, da ihm der Dienstleister und seine Gehilfen zuzurechnen sind.[54]

Dienstleister, welche durch das Beauftragungsverhältnis üblicherweise beruflich selbständig und eigenverantwortlich iSd § 4 Z 4 letzter Halbsatz über die Datenverwendung entscheiden können – hierzu zählen bestimmte freie Berufe wie Steuerberater[55], Rechtsanwälte[56], Wirtschaftstreuhänder oder Ziviltechniker -, werden in dieser Konstellation zu eigenständigen Auftraggebern und unterliegen direkt der Auskunftspflicht. Hierbei empfiehlt sich, unter Berücksichtigung der Verpflichtung in den geltenden Standesregeln und der Verantwortlichkeit, die Zusammenarbeit nach Verhaltensregeln gemäß § 6 Abs 4 näher zu definieren, um die notwendige Rechtssicherheit herzustellen.[57] Gemäß § 11 Abs 2 sind Vereinbarungen zwischen

[51] *Thanner*, DSG, 33.
[52] OGH 26.1.1995, 6 Ob 33/94; OGH 25.2.1993, 6 Ob 6/93. Vgl ecolex 1993, 380.
[53] DSB 12.5.2016, DSB-D122.515/0004-DSB/2016.
[54] ErlRV 1613 BlgNR XX. GP, 50.
[55] DSK 20.5.2005, K120.862/0011-DSK/2005.
[56] DSK 13.7.2012, K121.810/0013-DSK/2012; DSB 27.10.2014, DSB-D122.215/0004-DSB/2014 und DSB 9.3.2015 DSB-D122.299/0003-DSB/2015.
[57] *Thanner*, DSG, 33.

dem Auftraggeber und dem Dienstleister über die nähere Ausgestaltung der in Abs 1 genannten Pflichten, also auch der Rückgabe- bzw Vernichtungspflicht, soweit nicht ein Vertrag über die Aufbewahrung besteht, "zum Zweck der Beweissicherung schriftlich festzuhalten". Aus den genannten Vorschriften kann im Zusammenhang mit der in diesem Fall schlagend gewordenen Verpflichtung, auch Auskunft über allenfalls beim Dienstleister (noch) vorhandene Daten über die Mitbeteiligten zu erteilen, geschlossen werden, dass den Auftraggeber jedenfalls eine Erkundigungspflicht hinsichtlich solcher Daten trifft und er die ihm vom Dienstleister übermittelten Informationen an die Auskunftswerber weiterzuleiten hat. Auch wenn der Dienstleister nach § 11 Abs 1 Z 5 zur Vernichtung jener "Verarbeitungsergebnisse" und "Unterlagen, die Daten enthalten" verpflichtet war, die nicht an die Beschwerdeführerin "übergeben" wurden, bestand für den Fall der rechtswidrigen Nichterfüllung durch den Dienstleister dieser Verpflichtung die Auskunftspflicht hinsichtlich solcher Daten für den Auskunftswerber.[58]

Mit der DSG-Novelle 2010 wurde das Wort „nur“ eingefügt, um klarzustellen, dass die Qualifikation des Dienstleisters nur für jene Tätigkeiten gilt, in denen er ihm überlassene bzw von ihm ermittelte Daten ausschließlich für den Zweck der Werkherstellung und nicht (auch) für einen anderen Zweck verwendet. Daraus folgt, dass in manchen Konstellationen aus dem ehemaligen Dienstleister nun ein Auftraggeber (mit den daraus resultierenden Rechten und Pflichten) wurde: beispielsweise, wenn für die überlassenen Daten ein Entgelt geleistet wird, oder wenn Daten verschiedener Aufträge verknüpft werden, oder wenn selbständig über die Verwendung von Daten entschieden werden kann.[59]

Der OGH hatte einen Fall zu entscheiden, in welchem von einem Privatdetektiv die Auskunft verlangt wurde, wer dessen Auftraggeber sei. Der Überwachte wollte einen Unterlassungsanspruch gegen den Auftraggeber des beklagten Detektivs geltend machen können. Eine allgemeine Grundlage für einen derart weitgehenden, prinzipiell gegen jedermann gerichteten, Auskunftsanspruch ist jedoch nicht erkennbar. Die Vielzahl von – auch dem Schutz von Persönlichkeitsrechten dienenden – gesetzlichen Geheimhaltungsvorschriften (siehe beispielsweise auch § 130 Abs 5 GewO) steht der Annahme einer entsprechenden, in Richtung eines allgemeinen Auskunftsanspruchs gehenden gesetzlichen Wertung ebenso entgegen wie die lediglich punktuelle Normierung von gesetzlichen Offenlegungsverpflichtungen. Ein solcher Anspruch würde voraussetzen, dass die beklagten Parteien dem Kläger gegenüber zum Schutz seiner privaten Sphäre verpflichtet wären. Das Bestehen einer solchen allgemeinen (außervertraglichen) Fürsorgepflicht ist allerdings nicht zu erkennen.[60]

[58] VwGH 15.11.2012, 2008/17/0096.
[59] ErlRV 472, BlGNR XXIV. GP, 7.
[60] OGH 22.1.2014, 3 Ob 197/13m = jusIT 2014/140 = ÖJZ 2014, 744-746 = RdW 2014, 398.

2.4.4 Übermittlungsempfänger

Im § 26 Abs 1 werden als Bestandteil der Auskunft „allfällige Empfänger oder Empfängerkreise von Übermittlungen“ genannt. Für den Übermittlungsempfänger (Wortlaut der DSRL: „Empfänger“) existiert in diesem Sinne keine eigene Definition, es ist ein faktischer Begriff, der speziell bei der Zustimmungserklärung eine Rolle spielt. Da die Übermittlung nach § 4 Z 12 jedoch auf die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder den Dienstleister abstellt, liegt beim Datenaustausch zwischen Auftraggeber und Dienstleister keine Übermittlung vor (außer im Spezialfall der „Übermittlung durch Zweckänderung“ gemäß § 4 Z 12 letzter Halbsatz).[61]

2.5 Datei und Datenanwendung

Eine strukturierte Datensammlung, die nach mindestens einem Suchkriterium zugänglich ist, wird gemäß § 4 Z 6 als Datei bezeichnet. Dies schließt die Anwendbarkeit des DSG auf unstrukturierte Datensammlungen aus – in der Diskussion im Zuge der Schaffung des DSG 2000 wollte man dabei insb Aktenkonvolute ausklammern; gemeint waren vielmehr Karteien, Listen und dergleichen. Wie aus den Erläuterungen auch hervorgeht, hätte es – um der kollektiven Absicht zu entsprechen – vielmehr heißen müssen, dass eine Datei eine „Sammlung strukturierter Datensätze“ sei, welche nach mindestens einem Suchkriterium geordnet ist.[62]

In einer Entscheidung hatte der OGH zu prüfen, ob ein physischer Papierakt als „Datei“ zu qualifizieren ist. Im Urteil erfolgte der Verweis auf den 27. ErwGr der DSRL, wonach der Inhalt „nach bestimmten personenbezogenen Kriterien strukturiert“ sein müsse.[63] Hinzu kommt in § 4 Z 6 die Zugänglichkeit nach mindestens einem Suchkriterium.[64] Der OGH kam zum Schluss, dass das Datenschutzrecht auf den physischen Papierakt (ebenso für Zeitungsberichte oder Bücher, sofern nicht auch das für eine Datensammlung charakteristische Spezifikum hinzutritt) mangels Suchkriterium nicht anwendbar sei.[65] „Akten und Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien strukturiert sind, fallen unter keinen Umständen in den Anwendungsbereich“ der DSRL.[66,67] Ein Papierakt (hier: Personalakt) kann zwar innerhalb der Organisation nach einem Suchkriterium zugänglich sein, sein Inhalt jedoch ungeordnet aufbewahrt sein – das Datenschutzgesetz verleiht jedoch kein subjektives Recht

[61] DSK 20.2.2013, K121.906/0003-DSK/2013 und DSK 1.7.2003, K120.842/009-DSK/2003.
[62] ErlRV 1613 BlgNR XX. GP, 38.
[63] OGH 28.6.2000, 6 Ob 148/00h; ebenso DSK 11.3.2005, K120.969/0002-DSK/2005 und DSK 18.9.2009, K121.517/0020-DSK/2009.
[64] *Jahnel*, Datenschutzrecht, 151.
[65] OGH 6 28.6.2000, Ob 148/00h; ebenso DSK 11.3.2005, K120.969/0002-DSK/2005 und DSK 18.9.2009, K121.517/0020-DSK/2009.
[66] RL 95/46/EG, 27. ErwGr.
[67] DSK 10.11.2000, 120.707/7-DSK/00.

auf Akteneinsichtnahme.[68] Ebenso wenig kann eine „vollständige Aktenabschrift" begehrt werden.[69] In weiterer Folge bedeutet dies, dass ein als Ganzes dem DSG nicht unterliegender Papierakt auch dem im DSG normierten Auskunfts- oder Löschungsanspruch nicht zugänglich ist.[70]

Der Begriff der Datenanwendung wird in § 4 Z 7 als „die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung)" definiert. In weiterer Folge wird im § 58 die manuelle (nicht-automationsunterstützte) Datei der Datenanwendung im § 4 Z 7 gleichgestellt[71], soweit die Zuständigkeit zur Gesetzgebung Bundessache ist. Dies führte zur Schaffung von neun Landesdatenschutzgesetzen im Bereich der manuellen Datei.[72] Diese explizite Unterscheidung mag auf den ersten Blick chaotisch wirken, erschließt sich jedoch aus den Erläuterungen zur RV: Ziel des Gesetzgebers war die Aufrechterhaltung der bis dato bewährten Regelungsstruktur. Die Betroffenenrechte waren vor dem DSG 2000 grundrechtlich bei automationsunterstützter Datenverwendung garantiert und wurden nun richtlinienkonform auf manuell strukturierte Datenverwendungen (zB Karteien, Listen) ausgeweitet.[73] Damit fällt die Verwendung von Daten in Text-, Kalkulations- und Bildbearbeitungsprogrammen ebenso wie beispielsweise die analoge Aufzeichnung in einem „Besucherbuch" (nach Datum sortiert, Uhrzeit der Ankunft/Abreise, Name/Firma, KFZ-Kennzeichen) unter den Begriff der Datenanwendung. Eine Videoüberwachung mit digitaler Bildaufzeichnung stellt eine Datenanwendung dar.[74] Eine Videoüberwachung ohne Aufzeichnung der Daten („real-time monitoring")[75] wird jedoch nicht als Datenanwendung betrachtet und unterliegt lediglich dem in § 1 Abs 1 normierten Grundrecht auf Geheimhaltung, nicht aber dem Auskunftsanspruch nach § 26.[76] Eine Weitergabe von personenbezogenen Daten, die aus keiner Datenanwendung iSd DSG stammen, auch wenn dies auf elektronischem Weg erfolgt, stellt keine Übermittlung iSd DSG dar, fällt jedoch unter die Grundrechtsbestimmung des § 1.[77]

---

[68] DSK 4.6.2002, K120.810/005-DSK/2002; DSK 25.4.2008, K121.340/0006-DSK/2008; DSK 27.6.2012, K121.803/0008-DSK/2012; EuGH 14.7.2014, C-141/12, YS.
[69] DSK 14.11.2003, K120.871/004-DSK/2003.
[70] DSK 20.5.2005, K120.983/0009-DSK/2005 und DSK 6.9.2013, K121.979/0014-DSK/2013.
[71] Vgl DSK 24.4.2001, K120.737/002-DSK/2001.
[72] Siehe Begriff manuelle Dateien , 5.
[73] ErlRV 1613 BlgNR XX. GP, 30.
[74] DSK 21.3.2007, K507.515-023/0002-DVR/2007.
[75] Unter „Erfassung" der Daten nach § 4 Z 9 ist die Aufzeichnung auf einem Datenträger – und nicht wie hier, die Echtzeitüberwachung – zu verstehen, so VwGH 28.5.2013, 2011/17/0066.
[76] *Jahnel*, Datenschutzrecht, 154-155 in 3/105-3/106.
[77] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 76/3 in § 4 Anm 12.

Ein Bescheid einer Verwaltungsbehörde stellt keine Datenanwendung iSd DSG dar. Weder der Spruch eines Bescheids noch die Sachverhaltsfeststellungen oder andere Teile einer Bescheidbegründung unterliegen einer Löschung und Richtigstellung nach DSG, auch wenn der zugrundeliegende Text mit Hilfe automationsunterstützter Datenverarbeitung erstellt worden ist.[78] Ein Bescheid mit dem eventuell vorangehenden behördlichen Ermittlungsverfahren ist keine Datenanwendung, aus der Auskünfte gemäß § 26 Abs 1 zu erteilen sind. Wie schon aus der Verfassungsbestimmung des § 1 Abs 3 zu entnehmen ist, bezieht sich das Recht auf Auskunft nur auf Daten, die *„zur automationsunterstützten Verarbeitung ... bestimmt sind",* demnach auf Daten, die Prozessbestandteile einer Datenanwendung gemäß § 4 Z 7 wurden. Eine Datenanwendung kann für die Zwecke eines Behördenverfahrens dienen (zB der Aktenverwaltung oder der Erstellung, Adressierung und Versendung von Erledigungen), ein Behördenverfahren ist aber selbst keine Datenanwendung. Daher ist der Bescheid einer Behörde auch nicht gemäß § 26 zu beauskunften.[79] Als Partei eines Verwaltungsverfahrens steht dem Betroffenen bzw Beschwerdeführer aber das Recht auf Akteneinsicht gemäß § 17 AVG zu, um seinen Bedarf an Informationen über das betreffende Verfahren zu befriedigen.[80]

2.6 Verarbeitung personenbezogener Daten

Die DSRL nennt „Verarbeitung personenbezogener Daten" als Überbegriff und untergliedert diesen. Die Diktion des österreichischen Gesetzgebers spricht im Unterschied zur europarechtlichen Terminologie in § 4 Z 8 vom „Verwenden von Daten" und bezeichnet damit „jede Art der Handhabung von Daten, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten". Im Lichte des Auskunftsrechts nach § 26 sind beide Begriffe von Relevanz, da zunächst gegenüber der für die Verarbeitung verantwortlichen Person das Auskunftsbegehren gestellt werden muss und in weiterer Folge von dieser die Information verlangt wird, an wen die Daten übermittelt werden.[81]

Das Verarbeiten nach § 4 Z 9 umfasst nahezu jeden erdenklichen Bearbeitungsschritt: „Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittelns (Z 12) von Daten"[82] – dieser Begriff ist mE derart weit gefasst, um die potenziellen Grauzonen per Legaldefinition der Handhabung von Daten zu minimieren.

---

[78] DSB 24.9.2014, DSB-D121.891/0002-DSB/2014.
[79] DSK 8.11.2013, K121.972/0008-DSK/2013.
[80] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/72q in § 26 E 69.
[81] Siehe Begriff Übermittlungsempfänger, 13.
[82] Näher dazu *Jahnel*, Datenschutzrecht, 158-160 in 3/110-3/115.

Die Übermittlung ist hingegen in § 4 Z 12 prägnanter als „die Weitergabe von Daten an andere Empfänger als den Betroffenen[83], den Auftraggeber[84] oder einen Dienstleister[85], insb auch das Veröffentlichen von Daten[86]; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers“ definiert.[87] Bei der behördeninternen Weitergabe von Daten handelt es sich um eine Übermittlung, wenn die Verwendung für unterschiedliche Aufgabengebiete desselben Auftraggebers erfolgt.[88,89,90] Der Vollständigkeit halber sei an dieser Stelle angeführt, dass der Auftraggeber die in § 6 normierten Grundsätze sowie die Kriterien der Zulässigkeit der Verwendung von Daten nach § 7 zu beachten hat.

Hervorzuheben ist hier bei der in § 6 Abs 1 verankerte Grundsatz von Treu und Glauben. Dieser verlangt, dass auch mangelhafte bzw unvollständige Auskunftsbegehren nicht völlig unbeantwortet bleiben, sondern dem Auskunftswerber die Möglichkeit gegeben wird, sein Anbringen zu verbessern. Der Adressat des Auskunftsbegehrens hat daher umgehend zu reagieren und gegenüber dem Auskunftswerber darzustellen, aus welchen Gründen er vom Nicht-Vorliegen eines ordnungsgemäßen Auskunftsbegehrens ausgeht.[91]

[83] Eine Bekanntgabe von Daten an den Betroffenen (beispielsweise im Rahmen eines Auskunftsbegehrens) stellt keine Übermittlung dar, so *Dohr/Pollirer/Weiss/Knyrim*, DSG², 76/3 in § 4 Anm 12.
[84] Datenabfragen durch Mitarbeiter sind keine Übermittlungen, so DSK 30.6.2005, K121.015/0009-DSK/2005.
[85] Der Datenverkehr zwischen Auftraggeber und Dienstleister wird als „Überlassung“ bezeichnet, so DSK 9.8.2006, K121.102/0012-DSK/2006. Ebenso wird der Datenverkehr zwischen Dienstleister und Subdienstleister als „Überlassung“ betrachtet, so *Dohr/Pollirer/Weiss/Knyrim*, DSG², 76/2 in § 4 Anm 11.
[86] DSK 27.2.2004, K120.867/0001-DSK/2004 und DSK 14.6.2013, K212.780/0004-DSK/2013.
[87] Detaillierter dazu *Jahnel*, Datenschutzrecht, 160-169 in 3/116-3/126.
[88] DSK 31.5.2006, K121.108/0008-DSK/2006 und VfGH 11.10.2012, B1369/11 = VfSlg 19691 (im vorliegenden Fall wurde die Weitergabe auf die Annahme lebenswichtiger Interessen des Betroffenen gestützt – dies ist jedoch kein Zulässigkeitsgrund iSd § 1 Abs 2 DSG).
[89] VwGH 28.4.2009, 2005/06/0194 = VwSlg 17680 A/2009, jusIT 2009/75, 152 mit Anm *Jahnel*.
[90] EuGH 1.10.2015, C-201/14 (Smaranda Bara u.a.).
[91] DSK 21.3.2007, K121.258/0003-DSK/2007.

3 Umsetzung der Art 12 und 13 der RL 95/46/EG in § 26 DSG

In Art 12 der DSRL wurde das Auskunftsrecht determiniert, in Art 13 folgten Ausnahmen und Einschränkungen. Der österreichische Gesetzgeber hat die Art 12 und 13 der DSRL mit § 26 DSG umgesetzt. In diesem Abschnitt wird auf die Begriffe Auskunftswerber, eigene Daten, unentgeltliche Auskunftserteilung und Negativauskunft bzw Verweigerung der Auskunft eingegangen.

3.1 Auskunftswerber

Zunächst ist festzuhalten, dass der Begriff des Auskunftswerbers („jede Person oder Personengemeinschaft") terminologisch einen größeren Personenkreis umfasst als der Begriff des Betroffenen in § 4 Z 3 („jede vom Auftraggeber (Z 4) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z 8) werden"). Einem Auskunftsbegehren kann auch durch Erteilung einer Negativauskunft (zum Auskunftswerber sind keinerlei Daten vorhanden) nachgekommen werden.[92]

Grundsätzlich darf nur dem Auskunftsbegehren einer lebenden Person nachgekommen werden, da das dem Betroffenen zukommende höchstpersönliche Recht mit dessen Tod erlischt.[93,94] In einer aktuellen Entscheidung hatte die DSB zu beurteilen, ob dem ursprünglich bevollmächtigten Sohn des in der Zwischenzeit verstorbenen Betroffenen als Universalsukzessor bzw in analoger Anwendung von § 35 ZPO die Fortführung des Beschwerdeverfahrens vor der DSB zustünde. Die DSB hielt fest, dass die Anträge des Sohnes mangels Berechtigung zu ihrer Erhebung mit Bescheid zurückzuweisen seien und verwies diesbezüglich auf einen Beschluss des VwGH: „Über eine Beschwerde kann ungeachtet ihrer Zulässigkeit im Zeitpunkt der Einbringung nicht mehr meritorisch entschieden werden, wenn der Beschwerdeführer verstorben und kein Rechtsträger vorhanden ist, der die Rechtspersönlichkeit des Beschwerdeführers in Ansehung jener Rechte fortsetzt, deren Verletzung in der Beschwerde geltend gemacht worden ist und in welche der angefochtene Bescheid eingreift. In höchstpersönliche Rechte des Verstorbenen findet eine Rechtsnachfolge nicht statt, womit auch eine Fortsetzung des Verfahrens über solche Rechte durch die Verlassenschaft oder die Erben des Verstorbenen nicht in Betracht kommt[95].[96] Das BVwG führte dazu ebenso aus, dass ein postmortaler Persönlichkeitsschutz nach anderen Rechtsvorschriften nicht ausgeschlossen sei. Vom DSG 2000 sei ein derartiger Rechtsschutz jedoch nicht umfasst.[97] Das führt mitunter dazu, dass

[92] ErlRV 472, BlGNR XXIV. GP, 11 und VwGH 27.5.2009, 2007/05/0052 = VwSlg 17706 A/2009.
[93] *Grabenwarter*, Europäische Menschenrechtskonvention[4] § 17 Rz 4.
[94] DSK 12.9.2003, K202.028/006-DSK/2003, ebenso DSK 27.8.2010, K121.628/0015-DSK/2010.
[95] Vgl VwGH 25.8.2010, 2009/03/0161, mwH.
[96] Beschluss des VwGH 25.8.2010, 2009/03/0150.
[97] BVwG 3.12.2015, W214 2113213-1.

Rechtsnachfolger wie beispielsweise ein Erbe von einem Bankinstitut mit dem Auskunftsbegehren auf Grundlage des DSG keine Auskunft über den Erblasser erhält, da der Antragsteller nicht Betroffener iSd § 4 Z 3 ist. Diese Einschränkung gilt ebenso für juristische Personen. Das Erlöschen einer juristischen Person (beispielsweise die Auflösung eines Vereins) bedingt das Erlöschen des Auskunftsanspruchs – das bedeutet: auch wenn noch Daten über Vereinsmitglieder gespeichert sind, so können die Betroffenen die Informationen nicht auf Basis des § 26 abfragen. Die DSB hatte in einer aktuellen Entscheidung zu beurteilen, ob einem bereits aufgelösten Verein noch ein Löschungsanspruch (in diesem Fall gegen die Warnmeldung auf der Webseite der Finanzmarktaufsichtsbehörde) zustünde. Die DSB wies die Beschwerde ab bzw zurück, da es an der Aktivlegitimation des Beschwerdeführers mangelte, weil in der gegenständlichen Warnmeldung keine den personenbezogenen Daten des Betroffenen veröffentlicht wurden. Da die juristische Person bereits vor der Einbringung des Beschwerdeverfahrens durch freiwillige Selbstauflösung aus dem ZVR gelöscht wurde, ist das datenschutzrechtlich betroffene Rechtssubjekt damit nicht nur handlungsunfähig, sondern auch rechtlich nicht mehr existent. Dies ist dem Tod einer natürlichen Person gleichzuhalten. Der möglicherweise beeinträchtige „Ruf“ des Beschwerdeführers (§ 1330 ABGB) ist kein Schutzgegenstand des DSG und kann daher auch nicht mittels § 31 Abs 2 DSG geltend gemacht werden.[98]

Formal gesehen muss das Auskunftsbegehren vom Betroffenen selbst gestellt werden, da der Auskunftsanspruch prinzipiell höchstpersönlich[99] ist – somit darf auch das Auskunftsbegehren für nahe Angehörige nicht inhaltlich beantwortet werden. Diese Herangehensweise ist unter Berücksichtigung des in § 1 DSG normierten Geheimhaltungsanspruchs konsequent, führt aber mitunter bei Bevollmächtigung (beispielsweise Bestellung eines Vormunds) oder bei Vertretern einer juristischen Person (Auszug aus dem Firmenbuch oder Vereinsregister oder einen gleichartigen Nachweis[100]) zur Anwendung strengerer Maßstäbe an die Identitätsfeststellung im Zuge der Auskunftserteilung. In einer Entscheidung der DSK wurde festgestellt, dass das Verlangen auf Auskunft auch von einem Vertreter gestellt werden kann, dieser muss jedoch konkret dazu ermächtigt worden sein – der Verweis auf das Bestehen eines allgemeinen anwaltlichen Vertretungsrechts ist hier zu nicht ausreichend. Aus dem Gesamtzusammenhang muss erkennbar sein, dass die Stellung eines Auskunftsbegehrens auch von einer allgemein formulierten Vertretungsvollmacht tatsächlich und konkret mit umfasst war.[101]

[98] DSB 11.3.2015, DSB-D122.319/0002-DSB/2015; vgl DSB 13.3.2014, DSB-D121.220/0005-DSB/2014.
[99] AB 2028 der Beilagen XX. GP, 3 zu § 26.
[100] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/54 in § 26 Anm 7.
[101] DSK 21.3.2007, K121.258/0003-DSK/2007.

3.2 Fremde Daten – Konflikt mit Geheimhaltungsinteresse

Fremde Daten dürfen nicht beauskunftet werden (von der DSK wurde das Auskunftsrecht nach § 26 auf als „Recht auf Auskunft über eigene Daten“ bezeichnet). In einer Entscheidung der DSK wollte ein Berufsdetektiv Auskunft über den Stromverbrauch einer gesuchten Person von dessen Energieversorger erhalten, die Auskunft wurde jedoch unter Verweis auf die Unzulässigkeit der Datenübermittlung zu Recht nicht erteilt.[102] Die Problematik der potenziellen Beauskunftung fremder Daten führt beispielsweise bei einer Personalbeurteilungssoftware nach dem Schema „06.05.2016: Mitarbeiter Klaus Müller wurde von Putzfrau Klara Sommer dabei ertappt, wie er am Desktop von seinem Vorgesetzten Robert Wallner nach vertraulichen Inhalten suchte. Vorfall aufgenommen von Wolfgang Huber.“ zu einem Konflikt, daher darf in diesem Fall nur abstrakt („Es liegt über Robert Wallner ein Eintrag vom 06.05.2016 vor.“), jedoch nicht konkret Auskunft erteilt werden. Die Daten Dritter dürfen nicht Gegenstand der Auskunftserteilung sein, da in dieser Konstellation die Geheimhaltungsinteressen der anderen Betroffenen überwiegen.[103] Die gegen das Recht auf Auskunft angeführten Geheimhaltungsinteressen sind jeweils konkret, dh insb bezogen auf das jeweils bekannt zu gebende Datum, geltend zu machen und ihre Berechtigung muss auch jeweils darauf bezogen geprüft werden.[104] Die DSB (vormals DSK) kann in dieser Konstellation (Beauskunftung von Daten Dritter) mangels Beschwerdelegitimation des Beschwerdeführers nicht dem Auftraggeber die Auskunftserteilung auftragen.[105]

3.3 Unentgeltliche Auskunftserteilung?

Es ergab sich in den Niederlanden die Frage, ob eine Auskunft unentgeltlich zu erteilen sei – nach österreichischem Recht ist dies gemäß § 26 Abs 6 vorgesehen, sofern die Auskunft den aktuellen Datenbestand einer Datenanwendung betrifft und wenn der Auskunftswerber im laufenden Jahr noch kein Auskunftsersuchen an den Auftraggeber zum selben Aufgabengebiet gestellt hat. In der englischen Fassung der DSRL wurde der Auftraggeber zur Auskunftserteilung „without excessive delay or expense“ verpflichtet, aufgrund dieser unklaren Formulierung hatte der EuGH die möglichen zwei Lesarten zu prüfen:

- Die Mitteilung personenbezogener Daten habe ohne übermäßige Verzögerung oder übermäßige Kosten zu erfolgen, oder
- die Mitteilung personenbezogener Daten habe ohne übermäßige Verzögerung und ohne Kosten zu erfolgen.

[102] DSK 27.4.2000, 120.694/4-DSK/00.
[103] DSK 2.8.2005, K121.038/0006-DSK/2005.
[104] DSK 15.2.2005, K120.981/0002-DSK/2005.
[105] DSK 31.8.2000, 120.701/3-DSK/00 und DSK 16.5.2008, K121.323/0007-DSK/2008.

Im ersten Fall wäre die Erhebung einer Gebühr zulässig, sofern sie nicht übermäßig hoch sei. Im zweiten Fall wäre sie unzulässig. Der EuGH kam zu dem Schluss, dass eine Erhebung von Kosten für die Mitteilung von personenbezogenen Daten zulässig sei, sofern diese die tatsächlich erwachsenen Kosten nicht übersteigen, um das Kriterium der Übermäßigkeit zu wahren.[106] Im Praxisabschnitt wird näher auf die Voraussetzungen für die Entgeltlichkeit sowie die Höhe der Kosten eingegangen.[107]

3.4 Negativauskunft bzw Verweigerung der Auskunft

In § 26 Abs 2 iVm Abs 5 werden überwiegende öffentliche Interessen genannt, die der Auskunftserteilung entgegenstehen könnten. Bei Bestehen dieser Interessen ist die Auskunft nicht zu erteilen. Die DSK hatte in einer Entscheidung zu beurteilen, ob die Verweigerung der Auskunftserteilung mit dem Wortlaut „Im Übrigen werden über Sie keine der Auskunftspflicht unterliegenden Daten verwendet." gerechtfertigt sei. Die DSK bejahte dies im vorliegenden Fall, da die Standardantwort[108] immer zu verwenden sei, und zwar unabhängig davon, ob tatsächlich Daten vorliegen, um nicht die Aufgabenerfüllung zu erschweren oder zu behindern – schränkte aber auch ein, dass der Begriff „soweit" in § 26 Abs 2 deutlich zeige, „dass eine derartige Datenanwendung nicht automatisch zur Gänze der Auskunftsverweigerung unterliegt, sondern dass dies jeweils für jedes Datum konkret zu prüfen ist". Andernfalls könnte aus unterschiedlichen Auskünften auf den tatsächlichen Inhalt der Datenanwendungen geschlossen werden, was aber deren geschützte Zwecke vereiteln könnte.[109]

Es wurde an anderer Stelle schon darauf hingewiesen, dass dem Auskunftsanspruch lediglich personenbezogene Daten unterliegen – eine knifflige Konstellation ergibt sich jedoch, wenn etwa Geschäftsgeheimnisse untrennbar mit diesen personenbezogenen Daten verbunden sind. Denkbar sind beispielsweise Algorithmen einer Kreditauskunftei[110], die gewichtet nach verschiedenen Faktoren eben dazu führen, dass jemand als kreditwürdig eingestuft wird oder nicht. Wenn die Software feststellt, dass der Hauptwohnsitz des Auskunftswerbers in einer negativ bewerteten Region liegt und damit geringere Chancen zur Rückzahlung des Kredits

---

[106] EuGH 12.12.2013, C-486/12 (Vorabentscheidungsersuchen des Gerechtshof te 's-Hertogenbosch – Niederlande – in dem Verfahren auf Antrag von X).
[107] Siehe Begriff Entgelt, 28.
[108] Es ist nicht zwingend der Wortlaut der Standardantwort („Im Übrigen werden über Sie keine der Auskunftspflicht unterliegenden Daten verwendet.") anzuführen, solange der Kenntnisstand des Beschwerdeführers dadurch nicht geringer ist als bei Erteilung der Standardantwort, so DSK 28.6.2006, K121.075/0013-DSK/2006.
[109] DSK 31.5.2006, K121.133/0007-DSK/2006.
[110] DSK 15.2.2005, K120.981/0002-DSK/2005 – in dieser Entscheidung begründete der Auftraggeber die Verweigerung der Auskunft zu Unrecht mit dem betrieblichen „Know-how" (die Verarbeitung der Daten sowie deren Herkunft, die Zeitintervalle der Aktualisierung, die Gesprächspartner bei Banken und Lieferanten).

bestehen, so muss wohl wie im vorangehenden Beispiel abstrakt Auskunft erteilt werden („Unter anderem wurde die Hauptwohnsitzadresse im Zuge der Beurteilung der Kreditwürdigkeit erhoben."), jedoch nicht konkret („Rückzahlungswahrscheinlichkeit bei diesem Hauptwohnsitz liegt bei 61%."). Eine begründete Ablehnung könnte dann vorliegen, wenn Geschäftsverbindungen mit Dritten offengelegt werden müssten oder die eigene Prozesssituation in einem anhängigen Rechtsstreit mit dem Auskunftswerber geschwächt würde.[111] Die Geltendmachung von Geschäftsgeheimnissen darf jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird.[112]

In einem Beschwerdebegehren an die DSB war die Frage zu klären, ob das Auskunftsrecht nach § 26 DSG auch auf E-Mail-Attachments anwendbar sei. Wie sich aus gefestigter Rsp der DSK ergibt[113], unterliegt der Inhalt von E-Mails, ausgenommen solche, die für rein private und familiäre Zwecke (§ 45 DSG 2000) geschrieben worden sind, dem datenschutzrechtlichen Auskunftsrecht, da es sich bei E-Mails klar um die Ergebnisse einer automationsunterstützten Datenverarbeitung handelt. Es gibt keinen überzeugenden Grund, den Inhalt eigentlicher E-Mails anders als den Inhalt angeschlossener technischer Dateien (Attachments) zu behandeln. Das aus § 26 Abs 1 hervorgehende Recht bezieht sich auf den Dateninhalt, die „Angaben über Betroffene" (vgl § 4 Z 1), nicht auf die Form der Verarbeitung (etwa die Speicherung als Text oder Grafikdatei). Gegenstand des Auskunftsrechts sind daher unkörperliche, immaterielle Informationen und nicht körperliche Sachen wie eine Urkunde[114]. Auch wenn von einem datenschutzrechtlichen Auftraggeber Urkundeninhalte (etwa in Form von Scans, PDF-Dateien u.ä.) gespeichert werden, die auf einen Betroffenen Bezug nehmen, liegen automationsunterstützt verarbeitete Daten des Betroffenen vor. Diesem kommen hinsichtlich grafisch gespeicherter Textdokumente dieselben Rechte zu wie hinsichtlich in anderer Form (etwa in einer strukturierten Datenbank oder als Textdokument) verarbeiteter Daten. Allerdings umfasst das datenschutzrechtliche Auskunftsrecht, wie schon oben ausgeführt und mit Zitaten aus der einschlägigen Rsp belegt, weder einen Anspruch auf Vorlage oder Herausgabe von eigenhändig unterschriebenen Originalen einer Urkunde, noch einen solchen auf die Übermittlung von das Original vollständig wiedergebenden Foto-Kopien oder technisch in Form einer Datei (Urkundendatei) abgespeicherten Scans der Urkunde. Die Auskunft ist also auf den Dateninhalt beschränkt. Die im letzten Satz des § 26 Abs 1 eingeräumte Option auf „eine mündliche Auskunft mit der Möglichkeit der Einsichtnahme und der Abschrift oder Ablichtung" ist eine im Belieben des datenschutzrechtlichen Auftraggebers stehende Variante der Auskunftserteilung, wobei der Gesetzgeber hier erkennbar insb an eine Einsichtgewährung in automationsunterstützte

[111] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/56 in § 26 Anm 23.
[112] Vgl ErwGr 41 RL 95/46/EG.
[113] Vgl ua DSK 24.10.2007, K121.273/0016-DSK/2007; DSK 26.9.2008, K121.381/0008-DSK/2008; DSK 5.6.2009, K121.488/0007-DSK/2009.
[114] DSK 24.4.2001, K120.737/002-DSK/2001.

Datenanwendungen auf einem Bildschirm (mit der Möglichkeit des Ausdrucks von Daten) gedacht hat.[115]

Ein weiterer Aspekt betrifft das Verhältnis von DSG und etwaigen Mitarbeiter- bzw Betriebsvereinbarungen zueinander. Kann im Arbeitsvertrag etwa wirksam auf das Grundrecht der Geheimhaltung der personenbezogenen Daten verzichtet werden, weil das Unternehmen einen besonderen Transparenzanspruch erhebt? Kann im Arbeitsvertrag wirksam darauf verzichtet werden, in Zukunft Auskunftsbegehren nach dem DSG gegen den Arbeitgeber zu stellen? In Art 8 Abs 6 Schweizer Datenschutzgesetz beispielsweise ist ausdrücklich normiert, dass niemand im Voraus auf das Auskunftsrecht verzichten könne. *Auer* weist darauf hin, dass im Beschäftigungsverhältnis neben Vergütung und Leistungsbeurteilung regelmäßig auch sensible/besonders schutzwürdige Daten iSd § 4 Z 2 (beispielsweise über Gesundheit, Gewerkschaftszugehörigkeit oder religiöse Überzeugung) gespeichert werden.[116] Einerseits kann damit argumentiert werden, dass das Grundrecht auf Datenschutz kein absolutes Grundrecht ist und daher wirksam darauf verzichtet werden kann („Verwendung mit Zustimmung des Betroffenen“ in § 1 Abs 2). Andererseits darf eine derartige Regelung insgesamt nicht missbräuchlich eingesetzt werden („Sie bekommen den Arbeitsplatz nur, wenn Sie auf Ihre Rechte verzichten – es gibt hundert weitere Bewerber, die sich für diesen Arbeitsplatz interessieren.“). Die Wirksamkeit derartiger miteinander im Konflikt stehender Bestimmungen wird daher im Einzelfall zu prüfen sein. Ebenso stellt sich die theoretische Frage, ob auf die Stellung von Auskunftsbegehren pro futuro wirksam verzichtet werden kann (beispielsweise für ein Bankinstitut insofern von Interesse, als jedem Kontoinhaber folgender Vorschlag gemacht werden könnte: „Der Kontoinhaber erhält eine einmalige bzw wiederkehrende Gutschrift, sofern er kein Auskunftsbegehren stellt und dem Bankinstitut damit die Vorhaltung personeller und finanzieller Kapazitäten erspart.“) – auch derartige Übereinkommen werden einzelfallbezogen zu prüfen sein.

Bei der Auskunftserteilung können auch andere – vorrangige – Normen eine Rolle spielen, explizit erwähnt wird im § 26 Abs 9 DSG der Strafregisterauszug[117]. Eingang in die Rsp hat ebenso die Grundbuchabfrage gefunden, diese ist jedoch entsprechend den besonderen Bestimmungen entgeltlich auszufolgen.[118]

[115] DSK 22.5.2013, K121.925/0007-DSK/2013.
[116] *Auer*, Das Grundrecht auf Datenschutz im Unternehmen, 85.
[117] Für Auskünfte aus dem Strafregister gelten die besonderen Bestimmungen des Strafregistergesetzes 1968 über die Strafregisterbescheinigungen: BGBl 277/1968 idF BGBl Nr. I 107/2014: § 10.
[118] Die Gebührenpflicht für Grundbuchabfragen ergibt sich aus § 26b und § 32 Gerichtsgebührengesetz, Tarifpost 9.

Bundes-, Landes- und Gemeindeorgane sowie Organe anderer Körperschaften öffentlichen Rechts sind an die Bestimmungen im Auskunftspflicht-Grundsatzgesetz[119] gebunden. „Weitere Auskunftspflichten im öffentlichen und privaten Bereich finden sich beispielsweise in § 90 EStG 1988 (Lohnsteuerauskunft), in § 18 Abs 1 MeldeG (Meldeauskunft durch die Meldebehörde) oder § 53 Abs 3a SPG (Auskunftspflicht von Betreibern öffentlicher Telekommunikationsdienste gegenüber den Sicherheitsbehörden)"[120]. *Jahnel* empfiehlt, „bei einem Auskunftsbegehren darauf hinzuweisen, ob die Auskunft nach dem DSG 2000 oder nach dem AuskunftspflichtG verlangt wird, da als Adressaten eines Auskunftsbegehrens nach den verschiedenen gesetzlichen Grundlagen die selben Rechtsträger in Frage kommen können" und weist darauf hin, dass eine datenschutzrechtliche Auskunft im Gegensatz zu einer Auskunft nach dem AuskunftspflichtG „grundsätzlich auch jene Angaben über den Betroffenen umfasst, die der Amtsverschwiegenheit unterliegen"[121]. Für die Geltendmachung des Auskunftsrechtes nach DSG ist die Stellung als Betroffener ausschlaggebend, „nach den Auskunftspflichtgesetzen sind allgemein gehaltene Auskünfte durch die jeweilige Behörde über Angelegenheiten ihres eigenen Wirkungsbereiches an jedermann zu erteilen, und zwar auch dann, wenn er selbst nicht Betroffener iSd DSG 2000 ist"[122]. *Auer* prüfte zudem weitere Konstellationen, in denen der Schutz personenbezogener Daten eine Rolle spielte: in den Medien (§§ 7 und 7a MedienG), im Strafrecht (hier insb bei der beharrlichen Verfolgung nach § 107a StGB sowie bei Verletzung der Privatsphäre nach §§ 118 bis 124 StGB), im Gesellschaftsrecht (§ 24 GmbHG und §§ 84 und 99 AktG), im Wettbewerbsrecht (§ 11 UWG), als Geschäftsinhalt (§ 151 GewO) und im Zusammenhang mit Berufsgeheimnissen (38 BWG, § 91 WTBG) – damit soll verdeutlicht werden, dass das Datenschutzrecht in viele weitere Materien Einzug gehalten hat und der Auskunftsanspruch nach § 26 DSG keineswegs isoliert zu betrachten ist.

3.5 Leitfragen zum Auskunftsbegehren

Anhand der bislang dargestellten Definitionen, Auslegungen und Entscheidungen lässt sich als Zwischenfazit bereits ein grobes Schema zur formalen Herangehensweise bei einem Auskunftsbegehren ableiten:

- Bin ich Adressat des Auskunftsbegehrens? Falls nicht, ist eine Reaktion auf Basis des in § 6 Abs 1 verankerten Grundsatzes von Treu und Glauben geboten, verbunden mit der Darstellung, warum ich als Empfänger des Auskunftsbegehrens der Meinung bin, dass ich nicht als Adressat zu betrachten sei.

[119] Auskunftspflicht-Grundsatzgesetz BGBl 1987/286, welches auf Art 20 Abs 4 B-VG beruht. Für den Bereich der Verwaltung des Bundes gilt das Auskunftspflichtgesetz BGBl 1987/287 idF BGBl 1999/163. In den Ländern gibt es für den Bereich der Landesverwaltungen eigene Auskunftspflichtgesetze.
[120] *Jahnel*, Datenschutzrecht, 362 in FN 13 zu 7/7.
[121] *Jahnel*, Datenschutzrecht, 363 in 7/7.
[122] *Jahnel*, Datenschutzrecht, 362 in 7/7.

- Habe ich keinen Sitz oder Niederlassung in Österreich? Aufgrund des bereits dargestellten räumlichen Anwendungsbereiches des DSG unterliegen nur natürliche oder juristische Personen mit einem Sitz oder einer Niederlassung in Österreich dem DSG. Falls dies nicht zutrifft, ist eine Reaktion auf Basis des in § 6 Abs 1 verankerten Grundsatzes von Treu und Glauben geboten, verbunden mit der Darstellung, warum ich als Empfänger des Auskunftsbegehrens der Meinung bin, dass das DSG mangels Sitz oder Niederlassung in Österreich nicht anwendbar sei.
- Bin ich Auftraggeber der genannten Datenanwendung oder Aufgabengebiete? Falls nicht, ist eine Reaktion auf Basis des in § 6 Abs 1 verankerten Grundsatzes von Treu und Glauben geboten, verbunden mit der Darstellung, warum ich als Empfänger des Auskunftsbegehrens der Meinung bin, dass ich nicht als Auftraggeber der genannten Datenanwendung oder Aufgabengebiete zu betrachten sei.
- Bin ich Dienstleister der genannten Datenanwendung? § 26 Abs 10 normiert diesbezüglich: Wird ein Auskunftsbegehren an einen Dienstleister gerichtet und lässt dieses erkennen, dass der Auskunftswerber ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Dienstleister das Auskunftsbegehren unverzüglich an den Auftraggeber weiterzuleiten und dem Auskunftswerber mitzuteilen, dass in seinem Auftrag keine Daten verwendet werden.
- Falls Gründe vorliegen, die gemäß § 26 Abs 2 iVm Abs 5 der Auskunftserteilung entgegenstehen, so genügt der Hinweis „Im Übrigen werden über Sie keine der Auskunftspflicht unterliegenden Daten verwendet.“ Dabei muss jedoch berücksichtigt werden, „dass eine derartige Datenanwendung nicht automatisch zur Gänze der Auskunftsverweigerung unterliegt, sondern dass dies jeweils für jedes Datum konkret zu prüfen ist“. Eine begründete Ablehnung könnte dann vorliegen, wenn Geschäftsverbindungen mit Dritten offengelegt werden müssten oder die eigene Prozesssituation in einem anhängigen Rechtsstreit mit dem Auskunftswerber geschwächt werden würde.
- Liegt die Ausnahme der ausschließlich persönlichen oder familiären Tätigkeiten („Private Zwecke“) gemäß § 45 vor? Sofern die verarbeiteten Daten vom Betroffenen selbst mitgeteilt wurden oder auf rechtmäßige Weise zugekommen sind, besteht kein Auskunftsanspruch nach § 26 DSG.
- Werden keine direkt personenbezogenen Daten oder pseudonymisierte Daten verarbeitet? Falls dies zutrifft, ist eine Reaktion auf Basis des in § 6 Abs 1 verankerten Grundsatzes von Treu und Glauben geboten, verbunden mit der Darstellung, warum ich als Empfänger des Auskunftsbegehrens der Meinung bin, dass ich keine direkt personenbezogenen oder pseudonymisierten Daten verarbeite.
- Werden keine Daten in einer Datei iSd § 4 Z 6 und Z 9 verarbeitet? Falls dies zutrifft, ist eine Reaktion auf Basis des in § 6 Abs 1 verankerten Grundsatzes von Treu und

Glauben geboten, verbunden mit der Darstellung, warum ich als Empfänger des Auskunftsbegehrens der Meinung bin, dass ich keine Daten in einer Datei iSd § 4 Z 6 und Z 9 verarbeite, da Echtzeitvideoüberwachungen, Akten, Aktenkonvolute udgl nicht der Auskunftspflicht unterliegen. In den genannten Fällen besteht lediglich der Geheimhaltungsanspruch nach § 1 Abs 1, nicht jedoch die Verpflichtung, Auskunft nach § 26 zu erteilen.

- Werden Angaben, welche in öffentlichen Büchern einsehbar sind, abgefragt (zB Grundbuch)? Der Auskunftswerber ist in diesem Fall darauf hinzuweisen, dass diese Angaben entsprechend den besonderen Bestimmungen entgeltlich auszufolgen sind.

Im nachfolgenden Abschnitt werden die inhaltlichen Erfordernisse des Auskunftsbegehrens näher analysiert.

4 Auslegung, Entscheidungen und Rechtsprechung zu § 26 DSG und praktische Hinweise

Im Anhang 1 findet sich ein Formular der DSB, mit dem das Auskunftsbegehren an den Auftraggeber gerichtet werden kann.

Wie bereits eingangs dargestellt, sieht die Verfassungsbestimmung im § 1 Abs 1 die Geheimhaltung der personenbezogenen Daten vor. Der in § 1 Abs 3 iVm § 26 DSG normierte Auskunftsanspruch gegenüber Auftraggebern, um zu erfahren, welche personenbezogenen Daten diese verarbeiten (Auskunftsrecht), stellt einen der unter dem Begriff der Betroffenenrechte zusammengefassten Ansprüche dar. Daneben kann der Betroffene gegebenenfalls erwirken, den rechtmäßigen Zustand der Datenanwendung herzustellen (Richtigstellung, Löschung bzw Widerspruch). Dabei kann der Betroffene entsprechend Art 12 DSRL in Bezug auf Richtigstellung und Löschung Folgendes erreichen:

- je nach Fall die Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung nicht den Bestimmungen dieser Richtlinie entspricht, insb wenn diese Daten unvollständig oder unrichtig sind;
- die Gewähr, dass jede Berichtigung, Löschung oder Sperrung den Dritten, denen die Daten übermittelt wurden, mitgeteilt wird, sofern sich dies nicht als unmöglich erweist oder kein unverhältnismäßig großer Aufwand damit verbunden ist.

Die Besonderheit des Grundrechts auf Datenschutz ist die unmittelbare Drittwirkung – das bedeutet, dass dieses auch gegenüber Privaten durchsetzbar ist.[123] Ergänzend ist dabei darauf hinzuweisen, dass Art 8 der Charta der Grundrechte der europäischen Union[124] in Abs 1 das Recht auf den Schutz personenbezogener Daten statuiert und in Abs 2 auf die Betroffenenrechte (hier: Recht auf Auskunft und Berichtigung der Daten) eingeht. Art 8 Abs 3 GRC legt fest, dass die Einhaltung dieser Vorschriften von einer unabhängigen Stelle überwacht werden soll. In Österreich ist dies entsprechend § 36 DSG die Datenschutzbehörde.

In Vorbereitung auf diese Diplomarbeit wurden rund 20 Auskunftsbegehren an Firmen und Behörden gestellt, um entsprechende Praxiserfahrungen zu sammeln. Ausgehend von den erhaltenen Informationen werden weitere Überlegungen zur Auslegung sowie zu Entscheidungen der Datenschutzbehörde und höchstgerichtliche Rechtsprechung dargestellt. Schwer-

[123] *Bednar*, Rechtliche Probleme des Datenschutzgesetzes, ÖJZ 1980, 281(282). Die Drittwirkung des Grundrechts auf Datenschutz wurde bereits im DSG 1978 normiert.
[124] ABl 30.3.2010, C 83/389(393).

punkte dieses Abschnitts stellen praktische Hinweise zur reibungslosen Auskunftserteilung sowie die Möglichkeit zur Beschwerde an die Datenschutzbehörde bei unvollständiger Auskunftserteilung dar.

Das Bestehen des Auskunftsrechts ist nicht davon abhängig, dass der Betroffene eine Rechtswidrigkeit behauptet[125] oder Zweifel an der Richtigkeit der verwendeten Daten geltend macht[126]. Für das Auskunftsrecht und die Auskunftspflicht ist es unerheblich, ob der Betroffene seine Einwilligung zu dem Datenverkehr gegeben hat, über den er Auskunft begehrt.[127] Der Auskunftsanspruch ist jedoch durch das allgemeine Schikaneverbot[128] (Schädigungsabsicht bzw unlautere Motive der Handlung überwiegend) begrenzt.[129] Grundsätzlich kann der Auskunftswerber beliebig oft von seinem Recht auf Auskunft und damit von der Möglichkeit eines Auskunftsbegehrens Gebrauch machen, sofern keine schikanöse Rechtsausübung vorliegt.[130]

4.1 Kostenersatz

Wie bereits zuvor angesprochen, kann der Auftraggeber für wiederholte Auskunftsbegehren zum selben Aufgabengebiet im selben Kalenderjahr ein Entgelt verlangen. Die Auskunft ist gemäß § 26 Abs 6 unentgeltlich zu erteilen, wenn kumulativ folgende Voraussetzungen vorliegen:[131]

- Die Auskunft bezieht sich auf den aktuellen Datenbestand[132] einer Datenanwendung (Direktzugriff oder letztgültiger Datenbestand).
- Im laufenden Kalenderjahr wurde vom Auskunftswerber noch kein Auskunftsersuchen zum selben Aufgabengebiet des Auftraggebers gestellt – dabei ist das Eingangsdatum des Auskunftsbegehrens beim Auftraggeber maßgeblich. Im Falle der Geltendmachung der Mitwirkungsobliegenheit ist das Eingangsdatum des konkretisierten Auskunftsbegehrens beim Auftraggeber ausschlaggebend.

In Abgrenzung zum aktuellen Datenbestand sind historische Daten (beispielsweise auf Mikrofilm archiviert[133]) zu verstehen.[134] Die DSK nahm dabei auf die technische Auffindbarkeit der

[125] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/53 in § 26 Anm 5.
[126] VwGH 19.12.2006, 2005/06/0111 = VwSlg 17090 A/2006.
[127] OGH 10.7.1986, 6 Ob 12/85, veröffentlicht in RdW 1986, 306-308 = JBl 1986, 663.
[128] OGH 10.7.1986, 6 Ob 12/85, veröffentlicht in RdW 1986, 306-308 = JBl 1986, 663.
[129] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/53 in § 26 Anm 5.
[130] DSK 30.5.2008, K121.356/0005-DSK/2008.
[131] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/57f in § 26 Anm 30.
[132] ErlRV 1613 BlgNR XX. GP, 47 verdeutlichen, dass die Auskunft dann unentgeltlich zu erteilen sei, wenn die Auffindung der zu beauskunftenden Daten für den Auftraggeber keine besondere Belastung darstellt ("wenn sie den aktuellen Datenbestand einer Datenanwendung betrifft").
[133] DSK 25.2.2009, K121.394/0006-DSK/2009.
[134] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/57f in § 26 Anm 30.

zu beauskunftenden Daten Bezug, in diesem Fall war der Zugriff automationsunterstützt unmittelbar („auf Knopfdruck“) möglich. Die DSK stellte weiters klar, dass § 26 Abs 6 für Erwägungen darüber, ob die Auskunft aus dem aktuellen Datenbestand bei einem bestimmten Auftraggeber besondere Kosten verursacht und daher eine Kostenersatzpflicht zur Folge haben könnte, keinen Raum lasse.[135]

§ 26 Abs 6 stellt auf ein Aufgabengebiet und nicht auf die konkrete Datenanwendung ab, was uU dazu führen kann, dass der Betroffene innerhalb eines Kalenderjahres zwar verschiedene Datenanwendungen abfragt, die jedoch im selben Aufgabengebiet des Auftraggebers liegen und damit die Kostenersatzpflicht auslöst.[136] Das Aufgabengebiet ergibt sich im privaten Bereich aus dem berechtigten Zweck des Rechtsträgers (ein Anhaltspunkt ist dabei die Gewerbeberechtigung), im öffentlichen Bereich aus der Besorgung der gesetzlich übertragenen Aufgaben.[137]

Die DSK hielt fest, dass das Auskunftsrecht nicht nur hinsichtlich des aktuellen Datenbestands bestehe – schränkt der Auskunftswerber im Zuge der Mitwirkung sein Begehren nicht aus Eigenem auf aktuelle Datenbestände ein und läge auch bei Nicht-Einschränkung kein Fall eines unzumutbaren Aufwands beim Auftraggeber vor, kann nur ein entsprechender Kostenersatz in Betracht gezogen werden, vor dessen Begleichung die Auskunft nicht erteilt werden muss. Darauf muss jedoch der Beschwerdegegner den Auskunftswerber gemäß § 26 Abs 4 hinweisen.[138] Bei Abfragen zu länger zurückliegenden Datenbeständen, die beispielsweise nur mehr auf Mikrofilm archiviert verfügbar sind, wäre dem Auskunftswerber unter Offenlegung der Berechnungsgrundlagen mitzuteilen, dass die Auskunft nur nach Leistung eines Kostenersatzes erteilt wird. Sofern dem Betroffenen selbst der Zugang zu den zu beauskunftenden Daten möglich ist (im vorliegenden Fall via Online-Banking-Login), besteht kein Auskunftsanspruch.[139] Wenn der Betroffene „als Beitrag zur Mitarbeit“ jene Datenanwendungen beim Auftraggeber nennt, in denen Daten über ihn gespeichert sein könnten, so gilt das Auskunftsbegehren als auf diese Datenanwendungen eingeschränkt – möchte der Betroffene eine umfassende Auskunft erhalten, so muss er nicht aus Eigenem (dh ohne Mitwirkung gemäß § 26 Abs 3) die Datenanwendungen benennen.[140]

Bei Vorliegen der soeben genannten Kriterien sind auch die Portokosten (ausreichend frankiertes Kuvert) durch den Auftraggeber zu tragen. Etwaige Kosten, die durch den Betroffenen zwischenzeitlich übernommen wurden (im gegenständlichen Fall übersandte der Auftraggeber

---

[135] DSK 29.2.2008, K121.334/0005-DSK/2008.
[136] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/57f in § 26 Anm 30.
[137] *Jahnel*, Datenschutzrecht, 167f in 3/125.
[138] DSK 16.5.2008, K121.323/0007-DSK/2008.
[139] DSK 25.2.2009, K121.394/0006-DSK/2009.
[140] DSK 21.10.2011, K121.733/0009-DSK/2011.

die Auskunft unfrankiert mit dem Vermerk „Porto zahlt Empfänger“) führen zu einem Schadenersatz- oder Bereicherungsanspruch des Auskunftswerbers gegenüber dem Auftraggeber, die Entscheidung darüber obliegt den Zivilgerichten („bürgerliche Rechtssache“ iSd § 1 JN).[141] Bei Vorliegen der Voraussetzungen einer kostenlosen Auskunft sind auch die Portokosten vom Auftraggeber zu übernehmen, sodass sich die Auskunftserteilung als seine Bringschuld darstellt.[142] In einem weiteren Fall erteilte ein Auftraggeber zunächst entgeltlich (via Post, „Porto zahlt Empfänger“) und später unentgeltlich (via Fax) die Auskunft – dies stellt keine kostenfreie Auskunft dar.[143]

Sofern die Kriterien (aktueller Datenbestand, laufendes Jahr) jedoch nicht erfüllt werden, darf der Auftraggeber gemäß § 26 Abs 6 einen pauschalierten Kostenersatz von € 18,89[144] bzw die tatsächlich erwachsenen höheren Kosten verlangen. Ob derartige Abweichungen gerechtfertigt sind, wäre in einem Verfahren vor der DSB gemäß § 31 Abs 1 überprüfbar.[145] Ein etwa geleisteter Kostenersatz ist ungeachtet allfälliger Schadenersatzansprüche zurückzuerstatten, wenn Daten rechtswidrig verwendet wurden oder wenn die Auskunft sonst zu einer Richtigstellung geführt hat. Bei Errechnung eines individuellen Kostenersatzes sind folgende Kostenkomponenten zu berücksichtigen: Materialkosten, Portokosten, Lohn- und Gehaltskostenanteil, der auf jene Zeit entfällt, in der sich Mitarbeiter des Auftraggebers mit Tätigkeiten wie Heraussuchen von Daten, Erstellen von Abschriften, Anfertigen von Kopien oder Ausdrucken sowie Verfassen von Mitteilungen beschäftigen; Telefonkosten, anteilige EDV-Kosten, Kosten im Zusammenhang mit Identitätsprüfung.[146]

In dem Fall, dass der datenschutzrechtliche Auftraggeber den Kostenersatzanspruch nach § 26 Abs 6 mit der in § 26 Abs 4 vorgesehen Wirkung (Suspendierung des Anspruchs auf inhaltliche Auskunftserteilung bis zur Zahlung) geltend machen will, muss er dem Auskunftswerber (Betroffenen) unverzüglich eine entsprechende Rechnung legen (im Fall eines Abgehens vom pauschalierten Kostenersatz sind die „tatsächlich erwachsenen höheren Kosten“ darin detailliert auszuweisen) und eine angemessene Frist für die Zahlung setzen. Er muss weiters – in Erfüllung der dem Auskunftsrecht gemäß § 26 Abs 4 innewohnenden Begründungspflicht – darauf hinweisen, dass im Fall der Zahlungsverweigerung die Auskunft aus dem Grunde des § 26 Abs 4 letzter Halbsatz nicht erteilt werden wird. Hält der Auskunftswerber (Betroffene)

[141] DSK 18.9.2009, K121.521/0007-DSK/2009.
[142] DSK 18.9.2009, K121.514/0008-DSK/2009.
[143] DSK 19.3.2010, K121.593/0009-DSK/2010.
[144] Dieser auf den ersten Blick seltsam anmutende Betrag ergibt sich aus der Umstellung von Schilling (260 S) auf Euro (18,89 €), vgl RV 742 BlgNR XXI. GP, 1. Abschnitt, Artikel 3.
[145] ErlRV 1613 BlgNR XX. GP, 47.
[146] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/58 in § 26 Anm 31.

das Kostenersatzbegehren für unbegründet oder überhöht, steht ihm zur Abhilfe die Beschwerde an die Datenschutzkommission gemäß § 31 Abs 1 offen.[147] Sofern die Kostenersatzpflicht zu Recht besteht, beginnt die achtwöchige Frist zur Auskunftserteilung nach § 26 Abs 4 erst ab Begleichung des Kostenersatzes,[148] es liegt somit am Betroffenen, durch Einzahlung die Auskunft zu erwirken.[149] Sollte der Betroffene den Kostenersatz nicht leisten (wollen), so ist dieser nicht in seinem Recht auf Auskunftserteilung verletzt.[150,151]

4.2 Aufbau des Auskunftsbegehrens

Besonderes Augenmerk sollten aus Sicht des Auskunftswerbers auf die formellen Kriterien des Auskunftsbegehrens gerichtet werden: zunächst ist zu klären, in welcher Form (schriftlich oder mündlich) das Auskunftsbegehren an den Auftraggeber gerichtet werden kann und in welcher Weise der Identitätsnachweis zu erbringen ist. Bei Wahrung der formellen Aspekte des Auskunftsbegehrens spricht die DSK von einem „rechtsgültigen" Auskunftsbegehren.[152] Es ist dabei jedenfalls erforderlich, dass aus der Anfrage hervorgeht, dass ein Auskunftsbegehren iSd § 26 Abs 1 gefordert wird – dabei kommt es der DSK zufolge (vergleichbar mit privatrechtlichen Willenserklärungen) auf den Wortlaut und das Verständnis der Erklärung aus objektiver Sicht an. Dies ist hier von zentraler Bedeutung, da an den Erhalt eines rechtsgültigen Auskunftsbegehrens besondere Rechtsfolgen (ua Reaktionspflicht, Erteilung einer Negativauskunft) geknüpft sind – im betreffenden Fall ging jedoch aus der Anfrage nicht hervor, dass es sich um ein Auskunftsbegehren handelte.[153]

4.3 Identitätsnachweis

Es ist ratsam, das Auskunftsbegehren schriftlich (als eingeschriebenen Brief, Telefax[154], E-Mail[155]) an den Auftraggeber zu richten – dies dient einerseits zu Beweiszwecken vor der Rechtsschutzinstanz, andererseits ist damit für den Auftraggeber auch klar ersichtlich, welchen Umfang das Auskunftsbegehren hat.[156] *Dohr/Pollirer/Weiß/Knyrim* vertreten die Meinung, dass der zweifelsfreie Identitätsnachweis via Telefon, Fax oder E-Mail nicht erbracht

---

[147] DSK 25.2.2009, K121.394/0006-DSK/2009; DSK 29.2.2008, K121.362/0006-DSK/2008.
[148] *Jahnel*, Datenschutzrecht, 400 in 7/48. Ebenso *Drobesch/Grosinger*, Datenschutzgesetz, Anm 5 zu § 26 Abs 4, 208 welche darauf hinweisen, dass die Kostenersatzpflicht bereits vor der Auskunftserteilung entsteht.
[149] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/58 in § 26 Anm 31.
[150] DSK 7.6.2005, K121.008/0007-DSK/2005.
[151] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/57 in § 26 Anm 29 beziehen auch ein Verhalten des Auskunftswerbers ein, das einer Verweigerung gleichzuhalten ist.
[152] DSK 10.7.2009, K121.495/0013-DSK/2009.
[153] DSK 22.10.2008, K121.386/0009-DSK/2008; ebenso DSK 20.1.2010, K121.578/0002-DSK/2010; DSK 25.2.2009, K121.492/0004-DSK/2009.
[154] VwGH 9.9.2008, 2004/06/0221 = VwSlg 17515 A/2008 = jusIT 2008/109, 225 mit Anm *Jahnel*.
[155] So Bescheidpraxis der DSK, ua in DSK 5.6.2009, K121.525/0004-DSK/2009; DSK 2.2.2007, K121.225/0001-DSK/2007; DSK 16.11.2004, K120.959/0009-DSK/2004.
[156] VwGH 27.11.2007, 2006/06/0262.

werden könnte und das Auskunftsbegehren damit nicht den gesetzlichen Formvorschriften entspricht.[157] Diese Auffassung ist in Anbetracht der vorgenannten Bescheidpraxis der DSB nicht nachvollziehbar. Wenn in den Datenanwendungen des Auftraggebers eine Person mit Namen und Geburtsdatum des Auskunftswerbers aufscheint, und Zweifel an der Identität bestehen, muss der Auftraggeber im Sinn des § 26 Abs 3 den Auskunftswerber zur Mitwirkung dahingehend auffordern, weitere Identifikationsnachweise anzugeben. Ein unterschiedlicher Wohnort kann – wenn die übrigen Identifikationsdaten übereinstimmen – nicht als eindeutiges Indiz für unterschiedliche Identität angenommen werden, da der Wohnort ja jederzeit geändert worden sein kann. Dementsprechend enthalten etwa die „Identitätsdaten" nach § 1 Abs 5a MeldeG keinen Wohnort.[158]

Mit Zustimmung des Auftraggebers kann das Auskunftsbegehren gemäß § 26 Abs 1 auch mündlich (telefonisch, persönlich) gestellt werden. Die Erbringung des Identitätsnachweises (aktive Nachweispflicht durch den Auskunftswerber) ist hierbei von besonderer Bedeutung, da im Gegensatz zum schriftlich gestellten Auskunftsbegehren keine Unterschriften oder anderen Merkmale verglichen werden können. In der Regel wird daher ebenso eine Ausweiskopie vorzulegen sein.[159] Sollte der Auftraggeber der Meinung sein, dass der dem Auskunftsbegehren beiliegende Identitätsnachweis nicht lesbar oder sonst mangelhaft sei, so hat er unter dieser Begründung gegenüber dem Auskunftswerber von der Auskunftserteilung Abstand zu nehmen bzw dem Beschwerdeführer durch entsprechende Mitteilung die Möglichkeit zu bieten, einen lesbaren Identitätsnachweis nachzubringen.[160]

Die korrekte Erbringung „in geeigneter Form" des Identitätsnachweises der Person, deren Daten Gegenstand der Auskunft sein sollen, gegenüber dem Auftraggeber ist laut VwGH conditio sine qua non für das Entstehen des Anspruchs auf Auskunft. Diese Bestimmung habe den klar erkennbaren Zweck, jedem möglichen Missbrauch des Auskunftsrechts zur Informationsbeschaffung durch Dritte einen Riegel vorzuschieben. Ein Auftraggeber dürfe ohne Vorliegen eines Identitätsnachweises keine Daten an den Auskunftswerber – von dem er in diesem Moment nur annehmen könne, dass er tatsächlich der Betroffene sei – übermitteln, da er sonst das Datengeheimnis gemäß § 15 Abs 1 DSG verletzen könnte. Die Nennung des Geburtsdatums des Betroffenen ist zwar ein bedeutsames Kriterium, reicht für sich genommen jedoch

[157] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/53f in § 26 Anm 7.
[158] DSK 29.2.2008, K121.344/0002-DSK/2007.
[159] *Jahnel*, Datenschutzrecht, 375 in 7/19.
[160] DSK 29.2.2008, K121.344/0002-DSK/2007; vgl DSK 1.2.2013, K121.930/0004-DSK/2013.

nicht aus.[161] Die beigelegte Kopie eines amtlichen Lichtbildausweises (beispielsweise Personalausweis, Führerschein oder Reisepass) des Betroffenen zum Abgleich der Unterschrift im schriftlich gestellten Auskunftsbegehrens ist ausreichend, die eigenhändige (qualifizierte) Zustellung für sich genommen hingegen nicht.[162] Die Zustellung (im öffentlichen Bereich beispielsweise in Form einer Zustellung zu eigenen Handen[163] oder über einen Zustelldienst[164]; im privaten Bereich beispielsweise in Form eines Einschreibens mit der Zusatzleistung „eigenhändig" oder „mit Rückschein"[165]) dient vielmehr dazu, dass der Auftraggeber dem Risiko begegnet, die Auskunft an jemanden anderen als den Betroffenen zu erteilen – dies ist klar von der Erbringung des Identitätsnachweises durch den Betroffenen zu trennen und kann diese Obliegenheit auch nicht ersetzen.[166] Das Heerespersonalamt ist der Ansicht, dass der Identitätsnachweis bei natürlichen Personen auch durch beglaubigte Unterschrift bzw beglaubigte Kopie des Reisepasses, Personalausweises oder Führerscheins oder durch persönliche Vorsprache an der Adresse des Auftraggebers mit amtlichem Lichtbildausweis erfüllt werden könnte.[167] In einer aufrechten Geschäftsbeziehung kann die Pflicht zur Prüfung der Identität des Auskunftswerbers dadurch erfüllt werden, dass die Unterschrift im Auskunftsbegehren mit den vorhandenen Vertragsunterlagen verglichen wird. *Jahnel* zufolge ist die beglaubigte Abschrift eines Ausweises oder eine beglaubigte Unterschrift des Auskunftsbegehrens nicht erforderlich. Er geht zudem auf die Möglichkeit ein, die Identität durch eine qualifizierte elektronische Signatur iSd SVG (das Signaturgesetz war bis zum 30.06.2016 in Kraft) nachzuweisen.[168] Darunter fällt beispielsweise die Handysignatur. Der Auftraggeber hat die Eignung des vom Betroffenen gewählten Identitätsnachweises im Einzelfall zu prüfen.[169] Die DSK entschied in einem Fall, dass der Betroffene in seinem Recht auf Auskunft über eigene Daten verletzt sei, da der Auftraggeber – trotz eines erbrachten Identitätsnachweises – auf die Übermittlung der Vornamen der Eltern des Betroffenen bestanden und die datenschutzrechtliche Auskunft nicht erteilt hat.[170]

---

[161] VwGH 9.9.2008, 2004/06/0221 = VwSlg 17515 A/2008 = jusIT 2008/109, 225 mit Anm *Jahnel*. Vgl OGH 25.2.1993, 6 Ob 6/93, der feststellte, dass das Auskunftsrecht eines Betroffenen gegenüber dem Auftraggeber davon abhängig sei, dass er als Erheber eines Auskunftsbegehrens seine Wesensgleichheit mit der Person nachweist, deren Daten Gegenstand der Auskunft sein sollen.

[162] DSK 10.7.2009, K121.495/0013-DSK/2009.

[163] § 21 ZustG.

[164] § 35 ZustG.

[165] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/54 in § 26 Anm 8 mit Verweis auf die Tarifstruktur der Österreichischen Post AG: https://www.post.at/tarife_privat.php, Abschnitt „Einschreiben/Zusatzleistungen" (abgerufen am 08. September 2016).

[166] VwGH 9.9.2008, 2004/06/0221 = VwSlg 17515 A/2008 = jusIT 2008/109, 225 mit Anm *Jahnel*.

[167] DSK 2.2.2007, K121/225/0001-DSK/2007.

[168] *Jahnel*, Datenschutzrecht, 373f in 7/18.

[169] *Jahnel*, Datenschutzrecht, 375 in 7/19.

[170] DSK 2.9.2011, K121.715/0010-DSK/2011.

Der Identitätsnachweis ist bei Auskunftsbegehren von juristischen Personen durch (zusätzliche) Beifügung des Firmenbuchauszugs bzw des Vereinsregisters zu erbringen, aus dem hervorgeht, dass das Begehren durch ein vertretungsbefugtes Organ gestellt wurde.[171] Wird der Auskunftswerber vertreten (durch eine natürliche oder juristische Person oder durch einen Rechtsanwalt), so muss eine Spezialvollmacht zur Vertretung in Datenschutzangelegenheiten beigelegt werden, aus der im Gesamtzusammenhang hervorgeht, dass der Vertretene auch die Stellung des Auskunftsbegehrens in die Vollmacht einschließen wollte.[172]

Wie der VwGH ausführte, enthebt das Nichtvorliegen eines Identitätsnachweises den datenschutzrechtlichen Auftraggeber nicht von der Pflicht, auf das Auskunftsbegehren zu reagieren. Denn nach § 26 Abs 3 DSG habe der Betroffene auf Verlangen ("Befragen") des Auftraggebers am Auskunftsverfahren mitzuwirken (sogenannte Mitwirkungsobliegenheit[173]). Damit stehe dem Auftraggeber ein Instrument zur Verfügung, das Nachholen des Identitätsnachweises zu erwirken – und der datenschutzrechtliche Auftraggeber habe gemäß § 26 Abs 4 zumindest gegenüber dem Auskunftswerber schriftlich zu begründen, warum die Auskunft nicht erteilt werde. Wiese der Auskunftswerber also seine Identität nicht nach, so reduziere sich der Vollanspruch auf inhaltliche Auskunft darauf, eine entsprechende schriftliche Begründung für das Nichterteilen der Auskunft zu erhalten.[174] Diese Aufforderung zur Mitwirkung des Betroffenen kann unterbleiben, wenn es sich um das Auskunftsbegehren einer rechtsanwaltlich vertretenen Person handelt, welchem keine Vollmacht an den Rechtsanwalt beigefügt wurde. Beim Auskunftsrecht des Betroffenen handelt es sich um ein höchstpersönliches Recht[175], daher ist an den Nachweis der Bevollmächtigung durch den Betroffenen ein besonders strenger Maßstab anzulegen.[176] Es entfällt dabei auch die Pflicht des Auftraggebers, den Auskunftswerber zur nachträglichen Vorlage eines Identitätsnachweises aufzufordern.[177]

Hinsichtlich des Identitätsnachweises durch die Beifügung einer Kopie des Lichtbildausweises des Betroffenen lässt sich entgegnen, dass „dieses Mittel untauglich erscheine, die erforderliche Gewissheit über die Identität des Auskunftswerbers herbeizuführen, zumal dieser Ausweis gestohlen, gefälscht oder sonst wie manipuliert sein könnte, überdies aus einer Kopie auf Grund der drucktechnisch bedingten schlechteren Qualität der Darstellung üblicherweise nicht erkennbar sei und daher dem [...] Zweck des Missbrauches des Auskunftsrechtes nicht tat-

[171] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/54 in § 26 Anm 8.
[172] DSK 21.3.2007, K121.258/0003-DSK/2007.
[173] Siehe Begriff Mitwirkungsobliegenheit, 53.
[174] VwGH 9.9.2008, 2004/06/0221 = VwSlg 17515 A/2008 = jusIT 2008/109, 225 mit Anm *Jahnel;* ebenso DSK 10.4.2013, K121.924/0006-DSK/2013.
[175] AB 2028 der Beilagen XX. GP, 3 zu § 26.
[176] DSK 10.7.2009, K121.495/0013-DSK/2009.
[177] DSK 25.10.2013, K122.023/0006-DSK/2013; DSK 6.9.2013, K121.964/0015-DSK/2013.

sächlich dienen könne. Auch der Umstand, dass auf einem Personalausweis ein Foto aufgebracht sei, könne wohl keinen wirkungsvollen Beitrag zur Feststellung der Identität des Auskunftssuchenden leisten, zumal dieser dem datenschutzrechtlichen Auftraggeber regelmäßig nicht persönlich bekannt sein werde“, so ein Beschwerdeführer vor dem VwGH. Der VwGH hält fest, dass das beabsichtigte Ziel hinter der Erbringung des Identitätsnachweises lediglich Missbrauch erschweren soll und daher ein hoher Grad an Verlässlichkeit hinsichtlich des Identitätsnachweises ausreichend ist (im Gegensatz dazu könnte beispielsweise auch eine zweifelsfreie Identifizierung des Betroffenen gefordert werden).[178]

Zusammenfassend lässt sich damit festhalten, dass die Erbringung des Identitätsnachweises durch den Betroffenen zwei Funktionen erfüllt: einerseits ist er Grundvoraussetzung für das Entstehen des Auskunftsanspruchs, andererseits dient er dem Auftraggeber bei einem schriftlich gestellten Auskunftsbegehren dazu, durch Abgleich der Unterschriften mit hinreichender Sicherheit die Identität des Auskunftswerbers und die Echtheit des Auskunftsbegehrens feststellen zu können.[179]

In einer aktuellen Entscheidung[180] der DSB begehrte die Beschwerdeführerin Auskunft (gemäß § 26 Abs 1 DSG) über Standortdaten (diese ermöglichen die Feststellung, wo sich ein Nutzer zu einem bestimmten Zeitpunkt aufgehalten hat und sind in der Regel insofern personenbezogen, als sich der Mobilfunkteilnehmer in der unmittelbaren Nähe seines Mobiltelefons befindet) von ihrem Telekommunikationsdiensteanbieter. Dieser kann jedoch im Regelfall nicht feststellen, ob ein Auskunftswerber, dessen Standortdaten Gegenstand des Auskunftsverlangens sind, tatsächlich (zu jedem Zeitpunkt im fraglichen Zeitraum) Nutzer der einem Endgerät zugeordneten Rufnummer ist bzw war. Der Teilnehmer (Vertragsinhaber) ist nämlich tatsächlich häufig eben gerade nicht jener tatsächliche Nutzer, dessen Aufenthaltsort (und Wechsel von Aufenthaltsorten) in den betriebstechnischen Standortdaten abgebildet ist. Denkbar ist etwa, dass Teilnehmer (Vertragsinhaber) und Nutzer des mobilen Endgerätes auseinanderfallen, etwa wenn Vertragsinhaber ein Elternteil und Nutzer das Kind ohne eigenes Erwerbseinkommen ist. Auch gibt es am österreichischen Mobilfunkmarkt eigene Produkte, die Vergünstigungen gewähren, wenn zB Festnetzanschluss und Mobilfunk (mit mehreren SIM-Karten) in einem Paket mit einem einzigen Teilnehmer/Vertragsinhaber abgeschlossen werden. Klar tritt der Unterschied zwischen Teilnehmer und tatsächlichem Nutzer auch bei Firmenhandys hervor. Weiters verwies die Beschwerdeführerin auf § 90 Abs 8 TKG, wonach Anbieter von Mobilfunknetzen Aufzeichnungen über den geografischen Standort der zum Betrieb ihres Dienstes eingesetzten Funkzellen zu führen hätten, sodass jederzeit die richtige Zuordnung einer

[178] VwGH 9.9.2008, 2004/06/0221 = VwSlg 17515 A/2008 = jusIT 2008/109, 225 mit Anm *Jahnel*.
[179] DSK 2.2.2007, K121.225/0001-DSK/2007; DSK 2.8.2005, K121.034/0006-DSK/2005.
[180] DSB 15.4.2016, DSB-D122.418/0002-DSB/2016.

Standortkennung (Cell-ID) zum tatsächlichen Standort unter Angabe der Geo-Koordinaten für jeden Zeitpunkt innerhalb eines 6 Monate zurückliegenden Zeitraums gewährleistet sei. Der Telekommunikationsdiensteanbieter verweigerte ebenso die Auskunft nach TKG, da Standortdaten ausschließlich im Zuge polizeilicher Ermittlungen oder richterlicher Anordnungen bzw den Betreiber von Notrufdiensten, wenn ein Notfall dadurch abgewehrt werden kann, übermittelt werden dürften[181]. Aus der im § 90 Abs 8 TKG normierten sechsmonatigen Speicherpflicht der Standortdaten für Mobilfunkanbieter lässt sich kein subjektives Recht auf Auskunft von allenfalls gespeicherten Standortdaten eines Teilnehmers im Sinne des § 3 Z 19 TKG ableiten.[182] Insgesamt bleibt dabei jedoch offen, in welcher Form der „Nutzernachweis" gegenüber einem Telekommunikationsdiensteanbieter (bzw weiteren ähnlich gelagerten Anbietern, wie zB für mobilen Internetzugang oder Fahrzeuge mit GPS-Sender) zweifelsfrei erbracht werden kann, sodass der Betroffene vom Auftraggeber Auskunft über die zu seiner Person gespeicherten personenbezogenen Daten erhält. Denkbar wäre eine Art Anmeldung/Zuordnung bei verschiedenen Nutzern eines Geräts, sodass nur der „korrekte" Betroffene Auskunft erhalten könnte – dies liefe jedoch dem Vorteil der Anonymität bei Wertkartenmobiltelefonie zuwider.

4.4 Postversand

Ein Praxishinweis zum postalischen Versand des Auskunftsbegehrens: zu Beweiszwecken ist die Aufgabe als Einschreiben mit Rückschein bei der Post empfehlenswert. Der vorab ausgefüllte Rückschein begleitet den Brief bis zum Empfänger, wird von diesem unterzeichnet und mir zugestellt, sodass ich die Bestätigung bekomme, dass der Adressat mein Auskunftsbegehren entgegengenommen hat. Damit weiß ich genau, wann und von wem mein eingeschriebener Brief übernommen wurde.[183] Bei meinem an Facebook Ireland Ltd. gerichteten Auskunftsbegehren habe ich die Versandform Einschreiben/Rückschein gewählt, um sicher zu gehen, dass ich einen Abschnitt zurückbekomme, auf dem ich die Bestätigung habe, dass mein Auskunftsbegehren bei Facebook eingelangt ist. Im vorliegenden Fall hatte ich allerdings nach acht Wochen weder den Rückschein, noch die Auskunft mit den über mich gespeicherten Daten, noch Informationen über den Verbleib des Briefes (ob dieser tatsächlich zugestellt wurde) erhalten. Die Online-Abfrage der Sendungsverfolgung via Strichcode funktionierte im konkreten Fall auch nicht, sodass ich nicht wusste, wo sich mein Brief befindet. Die Post bietet in diesem Fall kostenpflichtige (€ 25,-, die man zurückbekommt, wenn die Post zum Ergebnis gelangt, dass die Zustellung nicht funktioniert hat) Nachforschungen an, denn sie sieht ihre

[181] Vgl OGH 13.4.2011, 15 Os 172/10y.
[182] DSB 15.4.2016, DSB-D122.418/0002-DSB/2016.
[183] Details dazu: https://www.post.at/privat_versenden_brief_oesterreich_zusatzleistungen.php#6359, abgerufen am 09. August 2016.

Hauptaufgabe bei der Nachforschung darin, die erfolgreiche Zustellung zu beweisen. Ich hingegen sehe die Hauptaufgabe der Post darin, die ordnungsgemäße Abgabe des Briefes online zu dokumentieren (mittels Sendungsverfolgungs-Funktion) sowie mir den Rückschein zuzustellen. Ich habe daraufhin beschlossen, Facebook ein zweites Auskunftsbegehren zuzusenden, um die gewünschte Auskunft zu erhalten – Details dazu später. Im vorliegenden Fall habe ich wohl bei der ersten Sendung eine veraltete Anschrift verwendet, sodass dieser Brief nicht zugestellt wurde und ich auch den Rückschein nicht erhalten habe.

4.5 Erteilung der Auskunft

Im nächsten Abschnitt wird die Erteilung der Auskunft thematisiert. Das subjektive Recht auf Auskunft über eigene Daten gemäß § 26 Abs 1 umfasst den Anspruch, eine vollständige und richtige Auskunft im vom Gesetz umschriebenen Umfang über eigene Daten, die der Auftraggeber verarbeitet, vom Auftraggeber zu erhalten.[184] Weiters sind Informationen über die Herkunft (soweit verfügbar[185]), etwaige Empfänger bzw Kategorien der Empfänger von Übermittlungen, der Zweck sowie die Rechtsgrundlage der Datenverwendung beizufügen. Auf Verlangen des Betroffenen sind Name und Anschrift herangezogener Dienstleister bekanntzugeben. Auf das Gebot, die Auskunft in allgemein verständlicher Form zu erteilen, wird anhand eines Praxisfalls detaillierter eingegangen.[186]

4.5.1 Verarbeitete Daten

Die Auskunft hat § 26 Abs 1 zufolge lediglich „verarbeitete Daten“ iSd § 4 Z 9 zu umfassen. Daten, die der um Auskunft ersuchte Auftraggeber einer Datenanwendung aus einer anderen Datenanwendung, für die er nicht Auftraggeber ist, erhoben hat, ohne sie in der eigenen Datenanwendung verarbeiten zu wollen, unterliegen daher nicht dem Auskunftsrecht. Das bloße Erheben von Daten ohne Verarbeitungsabsicht ist nach § 4 Z 10 kein „Ermitteln“ und damit auch kein „Verarbeiten“. Im konkreten Fall wurden Daten zu Kontrollzwecken abgefragt, aber nicht verarbeitet.[187] Denkbar wären auch Datensätze, die ohne Verarbeitungssicht in die Sphäre des Auftraggebers gelangen – wie beispielsweise postalische Zusendungen oder andere unverlangt eingegangene Informationen. Ebenfalls nicht von der Auskunftspflicht umfasst sind bereits vernichtete Datensätze – da es de facto unmöglich ist, sorgfältig gelöschte bzw aus anderen Gründen nicht länger verfügbare Daten zu beauskunften.[188] Dies hielt die DSB

[184] DSK 23.8.2002, K120.819/003-DSK/2002.
[185] Aus dem Gesetz geht keine ausdrückliche Pflicht hervor, die Herkunft von Daten zu dokumentieren. Auch besteht keine auf das DSG 2000 gegründete Pflicht, eine in den Jahren 2008 oder 2009 gesendete E-Mail zu archivieren und dem Beschwerdeführer in Kopie vorzulegen – so DSK 24.2.2012, K121.751/0006-DSK/2012.
[186] Siehe Begriff Abkürzungen, 41.
[187] DSK 20.10.2006, K121.154/0014-DSK/2006.
[188] Vgl *Drobesch/Grosinger*, Datenschutzgesetz, Anm 6 zu § 26, 204. Ebenso DSK 18.1.2008, K121.326/0002-DSK/2008: „... darauf hinzuweisen, dass sich die Auskunftspflicht des § 26 DSG 2000 (...) ausschließlich auf beim Auftraggeber (noch) gespeicherte Daten bezieht.“

auch im Zusammenhang mit der Aufhebung der Vorratsdatenspeicherung[189] fest: das Beschwerdeverfahren nach § 31 DSG dient der Durchsetzung des Auskunftsanspruchs und nicht der Feststellung möglicher vergangener Rechtsverletzungen. Folglich kann ein durch eingetretene faktische Unmöglichkeit nicht mehr durchsetzbares Recht gemäß § 31 Abs 7 und 8 auch nicht zum Gegenstand der Feststellung gemacht werden, in diesem Recht in der Vergangenheit verletzt gewesen zu sein.[190]

§ 26 Abs 1 umfasst nur „verarbeitete Daten", worunter in einer gegenwärtig existierenden Datenanwendung vorhandene Daten zu verstehen sind, nicht jedoch Daten in früheren Datenanwendungen, selbst wenn die Daten physisch identisch sind und nur der Zweck ihrer Verwendung (unter Aufgabe des früheren Zweckes) geändert wurde.[191] Der Begriff der „verarbeiteten Daten" impliziert eine bereits vergangene Handlung – ein Auskunftsbegehren kann folglich niemals in die Zukunft gerichtet sein („Was wird mit meinen Daten geschehen?"), zudem hielt die DSK fest, dass das Recht auf Auskunft keinen Anspruch auf Unterlassung der Verwendung irgendwelcher Daten beinhaltet. Ein solcher Unterlassungsanspruch kann aber, wie aus § 32 Abs 2 zu folgern ist, gegenüber Auftraggebern des privaten Bereichs durch Klage auf dem gerichtlichen Rechtsweg eingefordert werden, wobei als Anspruchsgrundlage insb die (Grund-)Rechte auf Geheimhaltung gemäß § 1 Abs 1 und auf Löschung gemäß § 27 Abs 1 in Frage kommen.[192] Ein Auskunftswerber begehrte Auskunft über eine Pensionsvorausberechnung („Höhe des Pensionsanspruchs zum gegenwärtigen Zeitpunkt"). Selbst wenn eine solche Berechnung auf Grundlage verarbeiteter Daten möglich sein sollte, fällt sie nicht unter das datenschutzrechtliche Auskunftsrecht, solange das Ergebnis der Berechnung nicht im Zeitpunkt des Einlangens des Auskunftsbegehrens bereits gespeichert und jederzeit abrufbar vorliegt.[193] Der Auskunftsanspruch des Betroffenen umfasst nicht die Bekanntgabe, in welcher Form Daten konkret verarbeitet wurden (beispielsweise Abfragen, Benützen oder Ausgeben bzw Ausdrucken von Daten).[194]

Die DSB hat weiters festgestellt, dass erst nach tatsächlicher Auskunftserteilung entstandene Daten nicht dem Auskunftsrecht des § 26 DSG unterliegen, da diese ja zum Auskunftszeitpunkt noch gar nicht beauskunftet werden konnten – das Auskunftsbegehren wurde damit vollständig erfüllt.[195] Es besteht kein Anspruch, laufend vom Auftraggeber über neu hinzugekommene Daten informiert zu werden – dafür kann jederzeit ein weiteres Auskunftsbegehren gestellt werden. Falls jedoch Daten zwischen dem Einlangen des Auskunftsbegehrens und

[189] VfGH 27.6.2014, G 47/2012 ua = VfSlg 19892, Kundmachung BGBl. I Nr. 44/2014.
[190] DSB 1.10.2014, DSB-D122.020/0012-DSB/2014 bestätigt durch BVwG 17.11.2015, W214 2014069-1/15E.
[191] DSK 28.6.2006, K121.075/0013-DSK/2006.
[192] DSK 23.8.2002, K120.819/003-DSK/2002.
[193] DSK 25.5.2012, K121.791/0008-DSK/2012.
[194] DSK 20.8.2002, K120.800/010-DSK/2002; VwGH 28.4.2009, 2005/06/0194 = VwSlg 17680 A/2009.
[195] DSK 8.10.2004, K120.826/0002-DSK/2004; DSK 7.6.2005, K120.912/0008-DSK/2005.

der tatsächlichen Auskunftserteilung neu hinzukommen, so sind diese ebenfalls zu beauskunften – denkbar sind etwa die Dokumentation des erhaltenen Auskunftsbegehrens, Kommunikation mit dem Auskunftswerber oder anderweitige Informationen, die im Zeitablauf hinzutreten.

Für Protokolldaten, die ausschließlich durch sequentielle Suche (nicht automationsunterstütztes Lesen der Protokolle) aufgefunden werden können, besteht keine Auskunftsverpflichtung.[196] Der Auftraggeber müsste in diesem Fall einen unverhältnismäßigen Aufwand gemäß § 26 Abs 2 geltend machen, abhängig davon, wie umfangreich das in die Prüfung miteinzubeziehende Datenvolumen jeweils ist. Der Begriff „Protokolldaten" wird dabei als Überbegriff für umfangreiche Datensammlungen gewählt und könnte insofern irreführend sein. Ein kategorischer Ausschluss der Auskunftserteilung aus sequentiell gespeicherten Daten wäre jedoch grundrechtswidrig, da es darauf ankommt, ob der Auftraggeber in concreto nicht selbst über Suchinstrumente (beispielsweise Standardsoftware wie MS-Excel) verfügt, die ihm eine gezielte Suche trotz der zeitlich sequentiellen Speicherform ermöglichen oder zumindest erheblich erleichtern. Der Auftraggeber wird in diesem Fall in derselben Weise Auskunft geben müssen, in der er selbst eine Suche zu den von ihm angestrebten Zwecken durchführen würde. Im betreffenden Fall wurden Logfiles zur Kontrolle von potenziell strafrechtswidrigen Internetzugriffen durch den Auftraggeber gespeichert.[197] Reine Protokolldaten (zB zu welcher Uhrzeit wurde eine Eintragung vorgenommen) unterliegen ebenfalls nicht dem Auskunftsanspruch.[198]

4.5.2 Allgemein verständliche Form

Die im § 26 Abs 1 normierte „allgemein verständliche Form" bezieht sich auf den ersten Blick auch auf die Struktur der Auskunftserteilung. Die DSK hat diesbezüglich in einer Entscheidung allerdings festgehalten, dass kein „Rechtsanspruch auf klare Strukturierung einer Datenanwendung" (zwecks besserer Lesbarkeit durch den Betroffenen) besteht.[199] Der Auftraggeber kann folglich selbst im eigenen Ermessen die Struktur der Datenanwendung festlegen. Es wäre dem Auftraggeber auch zu raten, für entsprechende Abfragemöglichkeiten zu sorgen, denn das Auskunftsrecht umfasst alle personenbezogenen verarbeiteten Daten – der Auskunftsanspruch darf folglich nicht durch eine bewusst mangelhafte technische Strukturierung der Datenbank eingeschränkt werden.[200] Unklar scheint, ob die Daten in Reinform (im Sinne von: unbearbeitet) zur Verfügung gestellt werden dürften oder ob entsprechende Kennzeichnungen bzw Bearbeitungsschritte (sensible Daten entschlüsseln, chronologische Sortierung) durch den Auftraggeber vorgenommen werden müssen, damit der Betroffene mit den Daten

[196] AB 2028 der Beilagen XX. GP, 3 zu § 26.
[197] DSK 23.5.2007, K121.259/0013-DSK/2007.
[198] DSK 2.8.2005, K121.038/0006-DSK/2005.
[199] DSK 5.4.2005, K120.986/0008-DSK/2005.
[200] VwGH 27.5.2009, 2007/05/0052 = VwSlg 17706 A/2009, jusIT 2009/76, 153 mit Anm von *Jahnel*.

auch etwas anfangen kann. *Dohr/Pollirer/Weiß/Knyrim* weisen in diesem Zusammenhang darauf hin, dass „interne Codes, technische Abkürzungen, und fremdsprachige Ausdrücke für einen Betroffenen derart zu verdeutlichen oder zu erläutern sind, um unter Anlegung einer Durchschnittsbetrachtung die Verständlichkeit der Auskunft zu gewährleisten“[201]. Auch verarbeitete Codes, deren Bedeutung dem Auftraggeber nicht mehr geläufig sein sollte, sind unter Offenlegung dieser Tatsache zu beauskunften.[202] In einer Entscheidung der DSK waren die Daten in den Datenanwendungen des Auftraggebers zu einem Großteil unter englischsprachigen Bezeichnungen bzw mit englischsprachigen Inhalten gespeichert, deren Bedeutung sich für den durchschnittlichen Empfänger nicht erschließt, sodass die Auskunftserteilung zwar nicht als falsch oder unrichtig bezeichnet werden kann, mangels allgemeiner Verständlichkeit aber nicht dem Gesetz entspricht. Da die deutsche Sprache die verfassungsmäßige Amts-, Unterrichts- und allgemeine Verkehrssprache auf dem Staatsgebiet der Republik Österreich ist, den Auskunftswerber also niemand verpflichten kann, die englische Sprache zu sprechen oder sich ihrer im Rechtsverkehr zu bedienen, hätte der Auftraggeber englischsprachige Inhalte ihrer Datenanwendungen zumindest durch Beifügung einer entsprechenden Erklärung oder Übersetzung allgemein verständlich machen müssen. Diese Verfassungsbestimmung bindet direkt zwar nur Staatsorgane (ua sind Verfahren vor der DSB zwingend in deutscher Sprache zu führen[203]), und hindert Privatpersonen nicht daran, sich auch im Rechtsverkehr (etwa bei der Abfassung von Verträgen) im Konsens anderer Sprachen zu bedienen.[204]

In einem Praxisfall bekam ich Zugriff auf Daten, die nicht verständlich aufbereitet waren. In diesem Datensatz wurden Metadaten von Telefongesprächen (Uhrzeit, Gesprächsdauer, gewählte Rufnummer uvm) protokolliert – ohne die Unterstützung von einem Informatiker hätte ich nicht herausgefunden, an welchen Stellen Trennzeichen einzufügen sind, um aus dem Datensatz eine lesbare Übersicht zu machen. In Anbetracht dessen wird wohl deutlich, dass die „allgemein verständliche Form“ sich auch auf die Art der Darstellung der gespeicherten Daten bezieht, dh die Daten müssen für den Betroffenen in einer leicht lesbaren und einfach verständlichen Form aufbereitet werden.

In einem Praxisfall hat mir mein Telekommunikationsanbieter die Einzelentgeltnachweise der vergangenen fünf Jahre (chronologisch geordnet) in Papierform übermittelt – dies waren weit mehr als hundert Seiten. Auch der beträchtliche Umfang der Datenanwendung kann für sich genommen keinen Grund darstellen, die Auskunftserteilung als nicht in „allgemein verständlicher Form“ erbracht zu bemängeln. Vielmehr ist es erfreulich, wenn die Datenanwendung vollständig (im vorliegenden Fall wurden 689 Beilagen angefügt) an den Betroffenen übermittelt

[201] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/55 in § 26 Anm 17.
[202] DSK 3.10.2007, K121.290/0015-DSK/2007.
[203] VwGH 23.2.2000, 2000/12/0026.
[204] DSK 22.5.2013, K121.935/0006-DSK/2013.

wird.[205] Auch dauerhaft verarbeitete interne Personennummern, Personenkennzeichen und ähnliche Suchbegriffe sind dem Betroffenen der Vollständigkeit halber zu übermitteln[206] – mE fällt beispielsweise auch die Matrikelnummer eines Studenten unter diese Kategorie.

Falls Unklarheiten (beispielsweise über Abkürzungen) hinsichtlich der erteilten Auskunft bestehen, so hat der Betroffene dies im Rahmen seiner Mitwirkungspflicht dem Auftraggeber mitzuteilen, dieser hat darüber aufzuklären.[207] In einem Praxisfall wurden vonseiten des Bundesministeriums für Landesverteidigung und Sport (Bundesheer) mir nicht geläufige (hauptsächlich medizinische Werte betreffende) Abkürzungen verwendet und mir auf Nachfrage erklärt, was beispielsweise die Kategoriebezeichnungen „Hb1AC“, „MCHC“ oder „H90.0“ bedeuten.

4.5.3 Konkrete Feldinhalte

Der Auskunftsanspruch umfasst die Bekanntgabe der konkret über die eigene Person gespeicherten Daten (beispielsweise „männlich“ oder „01.06.2016“) – die Auskunft ist folglich unvollständig, wenn bloß die Kategorien bzw Feldbezeichnungen (beispielsweise „Geschlecht“ oder „DNA-Auswertung“[208]) wiedergegeben werden.[209] Ebenso genügt nicht der allgemeine Verweis einer Bank, dass die über den Betroffenen gespeicherten Daten aus einem bestimmten Kreditvertrag entnommen worden sind, ohne die konkret vorliegenden Daten zu nennen.[210] Das Auskunftsrecht nach § 26 enthält keine Verpflichtung, die Beilagen einer Auskunft mit DVR- Nummer und Schriftköpfen zu versehen. Das Fehlen der DVR-Nummer und/oder Schriftköpfe auf Beilagen ist daher nicht als unvollständige Auskunft zu qualifizieren.[211] Die Auskunft gilt als vollständig erteilt, wenn der Auftraggeber bei einem Einfamilienhaus die Adresse nur mit Straßennamen und Hausnummer bekannt gibt, während die Postwurfsendung auch die Türnummer enthält.[212] In einem Praxisfall hatte der Auftraggeber lediglich angegeben, dass meine Daten „im Schulverwaltungsprogramm und (...) in der Absolventenliste gespeichert“ seien. Dies stellte klarerweise eine unvollständige Auskunft dar, die mithilfe der DSB ergänzt wurde.

Wie bereits zuvor zur Datenanwendung[213] ausgeführt, unterliegen der Auskunftspflicht nach § 26 automationsunterstützt verarbeitete Daten sowie nach den Bestimmungen des § 58 auch

---

[205] DSK 5.4.2005, K120.986/0008-DSK/2005.
[206] DSK 12.11.2004, K120.902/0017-DSK/2004.
[207] DSK 5.4.2005, K120.986/0008-DSK/2005.
[208] DSK 27.2.2004, K120.761/0002-DSK/2004. In der vorliegenden Entscheidung gab die DSK der Beschwerde statt und trug dem BMI auf, dem Betroffenen die Auswertung der DNA-Untersuchung zu überlassen bzw ein Gleichstück des dabei aufgenommenen Filmstreifens auszufolgen.
[209] DSK 23.11.2001, K120.748/022- DSK/2001 und DSK 14.12.2012, K121.877/0011-DSK/2012.
[210] DSK 20.3.2009, K121.493/0007-DSK/2009.
[211] DSK 18.5.2011, K121.652/0022-DSK/2011.
[212] OGH 28.10.1999, 3 Ob 132/99d = ecolex 2000, 578.
[213] Siehe Begriff Datenanwendung, 14.

Daten in manueller, strukturierter Form (Karteien, Listen). Für Auskünfte aus manuellen Dateien, soweit sie in den Zuständigkeitsbereich der Landesgesetzgeber fallen, gelten die Bestimmungen der Landesdatenschutzgesetze.[214] Demnach fallen jene Daten, die ausschließlich in Papierform aufbewahrt werden und nicht strukturiert zugänglich sind, nicht unter das datenschutzrechtliche Auskunftsrecht – wie beispielsweise eine schriftliche Maturaarbeit aus dem Fach Englisch.[215]

4.5.4 Herkunft der Daten

Zentraler Bestandteil des Auskunftsanspruchs sind die verfügbaren Informationen über die Herkunft der Daten. Die Daten können entweder vom Betroffenen selbst bekannt gegeben, vom Auftraggeber bei Dritten ermittelt oder ihm von Dritten übermittelt worden sein. Vom Auftraggeber selbst vorgenommene Bewertungen bzw Einstufungen (zB Bonität, Kaufkraftschicht usw) sind als solche zu deklarieren. Die Information über die Herkunft der Daten müsste verfügbar sein, da den Auftraggeber Protokollierungspflichten (insb § 14 Abs 2 Z 7) treffen.[216] Dementsprechend sind beispielsweise der „Melder“ von Bonitätsinformationen[217] oder Bank(en) und Lieferanten, welche Quellen abgespeicherter Daten sind, festzuhalten und im Rahmen der Auskunftserteilung konkret zu benennen. Allerdings wurde der Auftraggeber im vorliegenden Fall (nur) verpflichtet, die Bank(en) und Lieferanten, welche Quellen abgespeicherter Daten sind, konkret zu benennen (der Diktion der Eingabe folgend: wer etwas bekannt gegeben hat), nicht aber, was diese Bank(en) und Lieferanten jeweils allenfalls auch wann aus welcher Ursache und gegebenenfalls unter welchen Umständen bekannt gegebenen haben, also nicht aufgetragen, welche Daten ("was") konkret bekannt gegeben wurden (uU auch unter welchen Modalitäten). Vor diesem Hintergrund ist ein überwiegendes Interesse des Beschwerdeführers oder Dritter an einer Geheimhaltung dieser Angaben nicht zu erkennen.[218]

Sollte es dennoch nicht bzw nur mit unverhältnismäßig hohem Aufwand möglich sein, die Herkunft der Daten zu eruieren, so kann eine Information diesbezüglich unterbleiben[219] – die Beweislast, dass eine Ausnahme von der Verpflichtung zur Auskunftserteilung über die Herkunft der Daten vorliegt, trifft den Auftraggeber. Ein Klagebegehren ist in diesem Fall wegen Unmöglichkeit der Leistung (Rekonstruktion der Herkunft der Daten) abzuweisen.[220] Der VfGH stellte fest, dass über vorhandene Daten, auch wenn sie nicht gespeichert werden mussten,

---

[214] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/53 in § 26 Anm 4.
[215] DSK 25.2.2009, K121.427/0003-DSK/2009.
[216] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/54 in § 26 Anm 11.
[217] DSK 3.10.2007, K121.290/0015-DSK/2007.
[218] VwGH 23.1.2007, 2006/06/0039 mit Verweis auf den zugrundeliegenden Bescheid DSK 16.12.2005, K121.049/0023-DSK/2005.
[219] DSK 12.11.2004, K120.902/0017-DSK/2004 und DSK 20.5.2005, K120.908/0009-DSK/2005 und DSK 10.8.2007, K121.276/0014-DSK/2007.
[220] OGH 5.5.1988, 6 Ob 9/88; WBl 1989,66. Vgl JBl 1986, 663.

grundsätzlich Auskunft zu geben ist.[221] Unklar ist, aus welchen Gründen das Wort „verfügbaren“ vor Informationen durch die DSG-Novelle 2010 gestrichen wurde – im Sinne einer richtlinienkonformen Auslegung bleibt die Einschränkung auf verfügbare Informationen über die Herkunft der Daten weiterhin bestehen.[222] Es genügt zudem, wenn der Auftraggeber angibt, von wem er die Daten bezogen hat – wie der OGH bereits feststellte, muss der Datenfluss nicht über alle Vormänner bis an die Quelle zurückverfolgbar sein.[223] Dies ist auf etwaige „Nachmänner“ zu übertragen: der Auftraggeber ist nach § 26 DSG lediglich verpflichtet, die Empfänger der Daten durch seine Übermittlungen, nicht aber die Empfänger von Daten der Übermittlungen anderer Auftraggeber zu beauskunften.[224]

4.5.5 Empfänger bzw Empfängerkreise von Übermittlungen

Die Auskunft hat weiters „allfällige Empfänger oder Empfängerkreise von Übermittlungen“ zu enthalten. Übermittlungen sind jeweils so konkret zu beauskunften, dass der Betroffene seine Berichtigungs- und Löschungsrechte sowohl gegenüber der Quelle der Daten als auch gegenüber Übermittlungsempfängern durchsetzen kann. Stellt der Betroffene nämlich bei Prüfung der ihm erteilten Auskunft fest, dass unrichtige Daten betreffend seiner Bonität übermittelt worden sind, so muss er sich nicht drauf verlassen, dass der Auftraggeber seiner Pflicht gemäß § 27 Abs 8 DSG 2000 (Verständigung der Übermittlungsempfänger von einer durchgeführten Richtigstellung) nachkommen wird. Der Betroffene hat vielmehr ein überwiegendes berechtigtes Interesse daran, alle beim Auftraggeber vorhandenen Daten der Übermittlungsempfänger zu erhalten, die er benötigt, um diese nötigenfalls selber ansprechen zu können.[225]

Zur Frage, ob es genügt, den Empfängerkreis zu beauskunften oder ob der konkrete Empfänger genannt werden muss, ist zu berücksichtigen, ob eine Übermittlung lediglich an einzelne Empfänger oder an eine Gruppe von Empfängern, also an einen Empfängerkreis, gegangen ist. Darüber hinaus kann sich aus der gebotenen Interessenabwägung zwischen dem Interesse des Betroffenen an der Auskunft und allfälligen berechtigten Interessen des Auftraggebers an der Geheimhaltung von Empfängern von Daten ergeben, sodass, obwohl Daten an einzelne Empfänger gegangen sind, zur Wahrung eines überwiegend berechtigten Geheimhaltungsinteresses des Auftraggebers oder Dritter, nur ein Empfängerkreis bekannt zu geben ist. [226] Der Empfängerkreis kann sich allerdings einerseits dadurch reduzieren, dass sich gemäß § 14 Abs 3 aus der Registrierung einer zu beauskunftenden Datenanwendung (bzw aus einer zutreffenden Standard- oder Musteranwendung) ein „Empfängerkreis“ ergibt, der keiner

[221] VfSlg 18.230/2007.
[222] ErlRV 472, BlGNR XXIV. GP, 11.
[223] OGH 28.10.1999, 3 Ob 132/99d = ecolex 2000, 578.
[224] DSK 16.12.2009, K121.550/0017-DSK/2009; ebenso DSK 22.11.2013, K121.974/0019-DSK/2013.
[225] DSK 3.10.2007, K121.290/0015-DSK/2007.
[226] VwGH 19.12.2006, 2005/06/0111 = VwSlg 17090 A/2006.

weiteren Präzisierung bedarf; andererseits kann dieser Kreis dadurch erweitert sein, dass der Auftraggeber selbst als (weiterer) „Empfänger“ anzuführen ist, wenn er Daten, die für ein bestimmtes Aufgabengebiet bei ihm verarbeitet werden, auch für Zwecke eines anderen Aufgabengebietes verwendet und dadurch eine Übermittlung bewirkt.[227] Der VfGH hält die Regelung des § 26 Abs 1 zur Auskunft über "allfällige Empfänger oder Empfängerkreise von Übermittlungen" auch unter dem Blickwinkel des Art 18 B-VG für unbedenklich. Die mit den beiden Möglichkeiten notwendige Entscheidung, ob Empfänger individuell bekannt gegeben oder auf (dem Datenverarbeitungsregister gemeldete oder in einer Muster- oder Standardverordnung genannte) Empfängerkreise hingewiesen wird, lässt sich im Einzelfall auf Grund einer Abwägung der Gesichtspunkte der Datenschutzinteressen der Beteiligten und öffentlicher Geheimhaltungsinteressen treffen. Die nur allgemein gehaltene Behauptung, mit einer Auskunft seien auch datenschutzrechtliche Interessen von Auftraggeber und Übermittlungsempfänger berührt, vermag eine Darlegung der Interessen und die gebotene Interessenabwägung nicht zu ersetzen.[228]

Die Pflicht zur Führung von Aufzeichnungen darüber, welche Datenübermittlungen aus einer bestimmten Datenanwendung vorgenommen wurden, treffen (alleine) den Auftraggeber – eine „Unmöglichkeit der Leistung“ ist im Gegensatz zur „Herkunft der Daten“[229] hierbei nicht denkbar, da diese Übermittlungsvorgänge jedenfalls rekonstruierbar sind.[230] Es ist zu empfehlen, den konkreten Empfänger (beispielsweise ein bestimmtes Unternehmen oder die Konzernleitung) zu bezeichnen und unter Beifügung der Anschrift zu beauskunften. Sollte dies mit unverhältnismäßig hohem Aufwand verbunden sein – etwa, weil eine große Anzahl gleichartiger und eindeutig bestimmbarer Empfänger vorliegt (beispielsweise „alle Bürgermeister Österreichs“) – so genügt die Angabe des Empfängerkreises. Weitere Beispiele aus der Literatur sind Banken, Versicherungen, Gerichte usw.[231] Der Empfängerkreis darf jedoch nicht zu weit gefasst sein – „alle Unternehmen des B-Konzerns“ wurde von der bisherigen Judikatur wegen Intransparenz (in Bezug auf das in § 6 Abs 3 KSchG normierte Transparenzgebot) für nichtig erklärt.[232]

Es trägt jedenfalls zur Transparenz für den Betroffenen bei, wenn er weiß, wer Übermittlungsempfänger seiner Daten ist bzw war – und er kann die weiteren Betroffenenrechte (Löschung, Richtigstellung, Widerspruch) rascher durchsetzen. Als Grundsatz sei dazu auf die Rsp der

---

[227] DSK 16.12.2009, K120.973/0015-DSK/2009; VwGH 28.4.2009, 2005/06/0194 = VwSlg 17680 A/2009; ebenso DSK 17.6.2011, K121.691/0015-DSK/2011.
[228] VfGH 2.10.2007, B227/05 = VfSlg 18230; siehe dazu die Anm von *Jahnel* und *Knyrim*, jusIT 2008, 25.
[229] OGH 5.5.1988, 6 Ob 9/88; WBl 1989, 66. Vgl JBl 1986, 663.
[230] OGH 10.7.1986, 6 Ob 12/85, veröffentlicht in RdW 1986, 306-308 = JBl 1986, 663.
[231] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/54a in § 26 Anm 13 und 14.
[232] OGH 27.1.1999, 7 Ob 170/98w; ecolex 1999, 464f = RdW 1999, 458. Näher dazu auch *Knyrim*, Datenschutzrecht³, 174-176 und 194.

DSK hinzuweisen, wonach Übermittlungen jeweils so konkret zu beauskunften seien, dass der Betroffene seine Berichtigungs- und Löschungsrechte sowohl gegenüber der Quelle der Daten als auch gegenüber Übermittlungsempfängern durchsetzen könne.[233] Die DSK sieht im Zusammenhang mit Gesundheitsdaten[234] und bei Bonitätsdaten[235] ein besonderes Auskunftsinteresse des Betroffenen zur Beauskunftung der Identität der konkreten Übermittlungsempfänger, um einerseits die Rechtmäßigkeit der Übermittlung nachprüfen zu können, aber andererseits auch gegen möglicherweise unrichtige oder missverständliche Daten vorgehen zu können. Im Fall von Datenvermietung durch einen Adressverlag und Direktmarketingunternehmen hingegen genügt die Anführung von „Werbetreibende“ als Empfängerkreis.[236]

4.5.6 Verwendungszweck und Rechtsgrundlage

Der Betroffene hat weiters gemäß § 26 Abs 1 3. Satz das Recht, über den tatsächlichen Verwendungszweck der personenbezogenen Daten informiert zu werden – und zwar unabhängig davon, ob sich dieser bereits aus der Bezeichnung der Datenanwendung selbst ergibt.[237] Ebenso ist die Rechtsgrundlage der Datenverwendung (Verarbeitung und Übermittlung der personenbezogenen Daten) Gegenstand der Auskunftserteilung. Diese „gesetzliche Zuständigkeit bzw rechtliche Befugnis“ ist iSd §§ 7 ff zu beauskunften.[238] Im öffentlichen Bereich ergibt sich die Rechtsgrundlage aus der „gesetzlichen Zuständigkeit“ iSd § 7 Abs 1, im privaten Bereich beruht die Rechtsgrundlage meist auf den Statuten, dem Gesellschaftsvertrag iVm den Eintragungen im Firmenbuch oder auf dem Gewerbeschein iVm dem Gewerberegister.[239] Eindeutig dem Gesetz bzw den Materialien entnehmbarer Zweck des Auskunftsrechts und damit auch des Anspruches auf Bekanntgabe der Rechtsgrundlage von Verwendungsvorgängen ist es nämlich, dem Betroffenen die Verfolgung seiner sonstigen subjektiven Datenschutzrechte, insb des Rechts auf Geheimhaltung, zu ermöglichen. Somit ist es ausreichend, wenn der Auftraggeber die aus seiner Sicht in Betracht kommenden Rechtsgrundlagen bekannt gibt. Wenn der Beschwerdeführer diese für unzutreffend hält, so hat er dies mittels des ihm zur Verfügung stehenden Rechtsschutzes gegen Verletzungen im Recht auf Geheimhaltung (§§ 30 ff) geltend zu machen.[240] Hierbei liegt mE eine der besonderen Fallkonstellation der soeben zitierten Entscheidung zugrunde: der Beschwerdeführer brachte darin vor, dass die

---

[233] VwGH 19.12.2006, 2005/06/0111 = VwSlg 17090 A/2006 mit Verweis auf den zugrundeliegenden Bescheid DSK 15.2.2005, K120.981/0002-DSK/2005; ebenso DSK 2.9.2003, K120.743/004-DSK/2003.
[234] DSK 3.10.2007, K121.278/0018-DSK/2007.
[235] Ua VwGH 19.12.2006, 2005/06/0111 = VwSlg 17090 A/2006; DSK 8.5.2009, K121.470/0007-DSK/2009; DSK 15.2.2005, K120.981/0002-DSK/2005; DSK 7.5.2007, K121.280/0007-DSK/2007; DSK 2.9.2003, K120.743/004-DSK/2003.
[236] DSK 14.1.2005, K120.970/0002-DSK/2005.
[237] Anderer Ansicht jedoch *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/55 in § 26 Anm 15.
[238] DSK 1.7.2003, K501.349-040/003-DVR/2003.
[239] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/55 in § 26 Anm 16.
[240] DSK 5.4.2005, K120.972/0004-DSK/2005.

Salzburger Jägerschaft seine Daten gegen Entgelt für Zwecke der Versendung von Werbematerial weitergegeben hatte – in diesem Fall ist es zutreffend, dass der Geheimhaltungsanspruch des Betroffenen verletzt wurde. Anders ist die Konstellation jedoch, wenn die Daten lediglich „intern" unzulässig verarbeitet werden – dann steht der Löschungsanspruch gemäß § 27 Abs 1 Z 1 (der Auftraggeber hat die Daten zu löschen, sobald ihm die unzulässige - mangels rechtlicher Zulässigkeit – Verarbeitung bekannt geworden ist) bzw das Widerspruchsrecht gemäß § 28 Abs 2 (öffentliche Datenanwendung wie beispielsweise eine Online-Suchmaschine)[241] im Vordergrund. Das Widerspruchsrecht nach § 28 Abs 1 wird in der Praxis schwieriger durchsetzbar sein, da der Betroffene in diesem Fall überwiegende schutzwürdige Geheimhaltungsinteressen nachzuweisen hat.[242]

Die klare Angabe von Zweck und Rechtsgrundlage der Datenverwendung ist ein obligatorischer Bestandteil der vollständigen datenschutzrechtlichen Auskunftserteilung.[243] Der Betroffene ist nicht verpflichtet, sich selbst derartige Informationen zu beschaffen (beispielsweise aus dem Firmenbuch oder dem zentralen Gewerberegister). Für die Erfüllung des Auskunftsrechts genügt es aber nicht, dass der Zweck der Datenverwendung aus einer Gesamtbetrachtung der erteilten Auskünfte und des Schriftwechsels im Verlauf des Auskunfts- und Beschwerdeverfahrens für die Beteiligten allenfalls schlüssig hervorgeht.[244] In einer Entscheidung der DSK beschwerte sich der Betroffene darüber, dass der Zweck der Datenanwendung sowie die Rechtsgrundlage von seinem ehemaligen Arbeitgeber, dem Bundesministerium für Inneres, nicht ausdrücklich beauskunftet wurden. Die DSK hielt dazu fest, dieser Umstand könne im vorliegenden Fall keine ins Gewicht fallende Verletzung der Auskunftspflicht bedeuten, da die Kenntnis von diesen Informationen beim Beschwerdeführer als langjährigem, rechtskundigem Bediensteten des BMI als selbstverständlich vorausgesetzt werden durfte.[245]

4.5.7 Dienstleister

Die Auskunft über durch den Auftraggeber herangezogene Dienstleister gehört nicht zum Standardumfang des Auskunftsbegehrens und ist nur auf besonderes Verlangen im Auskunftsbegehren dem Betroffenen zu erteilen. Fehlt dieses „besondere Verlangen" im Auskunftsbegehren, so ist der Auskunftswerber durch das Fehlen einer Auskunft in der Frage der Dienstleister nicht im Recht auf Auskunft verletzt.[246]

---

[241] Diese Bestimmung wurde bereits als verfassungswidrig aufgehoben (vgl VfGH 8.10.2015, G264/2015), die Aufhebung tritt jedoch erst mit 31.12.2016 in Kraft.
[242] § 28 Abs 1 stellt auf den Sonderfall ab, dass die Datenanwendung zwar zulässig ist, eine aus der spezifischen Situation des Betroffenen heraus vorgenommene Interessenabwägung aber zu Gunsten des Betroffenen ausfällt (vgl OGH 14.9.2006, 6 Ob 167/06m).
[243] DSK 23.11.2001, K120.748/022- DSK/2001 und DSK 14.12.2012, K121.877/0011-DSK/2012.
[244] DSK 21.3.2007, K121.32/0005-DSK/2007.
[245] DSK 16.5.2008, K121.323/0007-DSK/2008.
[246] DSK 6.2.2008, K121.328/0003-DSK/2008.

4.5.8 Auskunftserteilung im Katastrophenfall

Die Bestimmungen der § 48a Abs 4 und 6 iVm § 52 Abs 1 Z 5 sollen gewährleisten, dass Daten über Katastrophenopfer auch wirklich an die richtigen Adressaten gelangen. Weiters sollen sie der Verhinderung von Missbrauch durch anfragende Personen dienen, die etwa ein Angehörigenverhältnis zu einer von der Katastrophe persönlich betroffenen Person vortäuschen. Insb da die Anfragen von Angehörigen im Katastrophenfall oft telefonisch erfolgen (vgl die für die Flutwellen-Katastrophe zuständige Hotline des Außen- und Innenministeriums) oder per E-Mail erfolgen, ergibt sich die Problematik der Identifizierung der Anfragenden als Angehörige der gesuchten Person. Die anfragende Person muss daher neben Namen und Geburtsdatum der von der Katastrophe tatsächlich oder vermutlich unmittelbar betroffenen Person auch eigene Daten (Name, Wohnadresse, Telefonnummer oder E-Mail-Adresse oder dergleichen) zur Verfügung stellen und überdies die Angehörigenbeziehung glaubhaft machen. Behörden sind in diesem Zusammenhang berechtigt, die notwendigen Überprüfungen dieser Angaben durchzuführen, was insb im Zweifelsfall stattfinden müsste. Die dafür notwendigen Informationen sind der Behörde allenfalls von anderen Behörden im Wege der Amtshilfe zur Verfügung zu stellen. Speziell war in diesem Zusammenhang eine Unterstützungsverpflichtung der Sozialversicherungsträger gegenüber Behörden und Hilfsorganisationen zu normieren, da diese über Informationen bezüglich der Angehörigeneigenschaft von Personen verfügen. Die im letzten Satz des § 48a Abs 5 genannte Zweckbestimmung soll klar stellen, dass Daten von Katastrophenopfern von den Angehörigen nur zur persönlichen Information und um den Betroffenen Hilfe zu leisten verwendet werden dürfen, nicht aber für andere, zB kommerzielle Zwecke.[247]

4.6 Pflicht zur Reaktion

Wie zuvor bereits geschildert, hat der Auskunftswerber Anspruch[248] auf eine Antwort vom Auftraggeber, diese kann nach § 26 Abs 1 5. Satz auch in Form einer Negativauskunft erteilt werden.[249] Die DSK präzisierte dies: es müsse vom Auftraggeber eine eindeutige und unmissverständliche Äußerung (Auskunft oder Mitteilung über die Gründe für die Nichterteilung einer Auskunft) ausgehen[250] – erst dann ist das Auskunftsbegehren iSd § 26 Abs 4 als erfüllt anzusehen. Konsequenterweise sind im Falle einer Negativauskunft (keine Daten zum Auskunftswerber gespeichert) auch die durch den Auftraggeber herangezogenen Dienstleister nicht zu

[247] IA 515 BlGNR XXII. GP, 10.
[248] Siehe Begriffe Auskunftsverweigerung, 52 und Pflicht zur Reaktion , 56.
[249] ErlRV 472, BlGNR XXIV. GP, 11 und VwGH 27.5.2009, 2007/05/0052 = VwSlg 17706 A/2009.
[250] DSK 2.4.2008, K121.345/0005-DSK/2008; ebenso DSK 18.1.2008, K121.326/0002-DSK/2008 und DSK 20.5.2005, K120.897/0003-DSK/2005.

beauskunften (diese sind nur bekanntzugeben, falls sie mit der Verarbeitung seiner Daten beauftragt sind). Die Begründung für die Nichterteilung der Auskunft ist dabei auf § 1 Abs 4 zu stützen[251].

Die Auskunft wird im Regelfall schriftlich erteilt, dies ist schon aus Beweisgründen zu empfehlen. Der Auskunftswerber hat keinen Anspruch auf die mündliche Erteilung der Auskunft, kann dieser aber zustimmen. Das DSG verlangt keine ausdrückliche Zustimmung, weshalb im Hinblick auf die §§ 863f ABGB, die auf datenschutzrechtliche Willenserklärungen analog anzuwenden sind, soweit das DSG keine abweichenden Regelungen enthält, davon auszugehen ist, dass auch eine konkludente Zustimmung, insb durch tatsächliche Entgegennahme einer mündlich erteilten Auskunft möglich ist.[252] Mit Einverständnis des Betroffenen sind auch folgende Formen der Auskunftserteilung denkbar: Akteneinsicht, Abschrift, Ablichtung, automationsunterstützt (zB Hardcopy, Einsichtnahme über Bildschirm, Screenshots[253], E-Mail). Dabei ist, wie zuvor schon erwähnt, sicherzustellen, dass die Auskunft ausschließlich dem Auskunftswerber zukommt.[254]

4.7 Beschränkung der Auskunft

Der Auskunftsanspruch ist in mehrfacher Hinsicht beschränkt, dabei ist gemäß § 1 Abs 2 letzter Satz zu beachten, dass der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art, vorgenommen werden darf. Zunächst ist auf die Bedeutung des erkennbaren Rechtschutzinteresses[255] des Betroffenen hinzuweisen. Das Auskunftsrecht ist nicht absolut, sondern seiner Funktion nach (nur) ein Begleitgrundrecht, das der Durchsetzung des Grundrechts auf Geheimhaltung dient. Der Umfang des Auskunftsrechts muss daher in Relation zum jeweiligen Rechtsschutzinteresse gesehen werden.[256] Soweit eine Datenanwendung von Gesetzes wegen durch den Betroffenen einsehbar ist, besteht lediglich das Einsichtsrecht nach § 26 Abs 8, darüber hinaus besteht das Auskunftsrecht nach § 26 Abs 1.[257] Der Betroffene hat keinen Anspruch auf konkrete Darstellung der Datenanwendung[258] oder auf Vorlage von Ausdrucken aus der Datenanwendung[259]. Fragen, wie beispielsweise „von wem

[251] DSK 14.12.1984, GZ 120.052 = ZfVB 1987, 257(258).
[252] DSK 23.5.2007, K121.259/0013-DSK/2007.
[253] DSK 23.5.2007, K121.259/0013-DSK/2007. Im vorliegenden Fall wurden die 57 übermittelten Screenshots als „unverständlich" eingestuft, weil die Vollständigkeit aufgrund der großen Datenmenge schwer zu prüfen sei.
[254] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/55 in § 26 Anm 19.
[255] Vgl VwGH 19.12.2006, 2005/06/0111 = VwSlg 17090 A/2006.
[256] DSK 21.1.2009, K121.415/0002-DSK/2009 – hier hatte der Betroffene laufend die Möglichkeit, die Anzahl seiner Krankenstands-, Urlaubs- und Sonderurlaubstage mittels „Tagfiles" einzusehen. Anders jedoch DSK 23.5.2007, K121.259/0013-DSK/2007 – hier konnte der Betroffene nicht selbst abfragen, wer aller auf seinen dienstlichen Mail-Account Zugriff hatte, die Auskunft darüber wurde dem Auftraggeber aufgetragen.
[257] ErlRV 472, BlGNR XXIV. GP, 11.
[258] DSK 21.6.2005, K120.839/0005-DSK/2005.
[259] DSK 2.8.2005, K121.038/0006-DSK/2005.

Passwörter abgefragt wurden“ oder „von wem die e-mail Adresse wieder eingerichtet wurde“, sind ebenfalls nicht Gegenstand des Auskunftsrechts.[260] Sofern nicht der aktuelle Datenbestand Gegenstand des Auskunftsbegehrens ist, kann der Auftraggeber einen Kostenersatz vom Betroffenen verlangen.[261]

§ 26 Abs 2 normiert in Umsetzung des Art 13 DSRL weitere Beschränkungen des Auskunftsrechts. Die Auskunft ist nicht zu erteilen,

- soweit dies zum Schutz des Auskunftswerbers aus besonderen Gründen notwendig ist oder
- soweit überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten
- insb auch überwiegende öffentliche Interessen, der Auskunftserteilung entgegenstehen.

4.7.1 Schutz des Auskunftswerbers aus besonderen Gründen

Stelzer schlägt vor, die „besonderen Gründe“ auf „lebenswichtige Interessen“ des Betroffenen zu reduzieren, um eine verfassungskonforme Auslegung des § 26 Abs 2 zu erreichen.[262] In der österreichischen Rechtsordnung sind lediglich vereinzelt gesetzliche Beschränkungen des Auskunftsrechts durch eine staatliche Behörde vorgesehen.[263] Die Einschränkung der Auskunft zum Schutz des Auskunftswerbers wird nur in wenigen Ausnahmefällen gerechtfertigt sein (zB im medizinischen Bereich oder hinsichtlich von Auskünften aus dem Strafregister[264]).[265] Jedoch ist in diesem Falle darauf zu achten, dass dem Betroffenen möglichst umfangreich die gewünschte Auskunft, zB im Wege eines Arztes, erteilt wird, da die Beschränkungen des Grundrechts restriktiv auszulegen sind.[266] *Dammann/Simitis* vertreten die Auffassung, dass der betroffene Patient selbst am besten einschätzen kann, ob er Auskunft über seine eigenen personenbezogenen Daten erhalten möchte und ihm prinzipiell die volle Wahrheit mitzuteilen sei.[267] Auch das Fehlen eines Vollmachtsnachweises („Außenvollmacht“) stellt einen „besonderen Grund“ dar, der nach § 26 Abs 2 erster Satz dazu führt, dass die Auskunft nicht zu erteilen ist, weil dies zum Schutz des Betroffenen, konkret seines Anspruches auf Geheimhaltung, notwendig ist. Die begründete Verweigerung der Auskunft ist in diesem Falle

---

[260] DSK 7.6.2005, K120.976/0003-DSK/2005.
[261] Siehe Begriff Kostenersatz, 29.
[262] *Stelzer*, Datenschutz im Gentechnikrecht, 39.
[263] *Jahnel*, Datenschutzrecht, 407 in 7/57 mit Verweis auf § 185 Abs 10 MinroG sowie auf den 2004 aufgehobenen § 251 Z 4 ZPO idF BGBl. I Nr. 76/2002. Die Durchsetzung der Betroffenenrechte im Bereich der Gerichtsbarkeit ist seitdem im GOG geregelt.
[264] Für Strafregisterauszüge ist jedoch die Sonderbestimmung des § 26 Abs 9 zu beachten.
[265] ErlRV 1613 BlgNR XX. GP, 47.
[266] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/55f in § 26 Anm 22.
[267] *Dammann/Simitis*, EG-Datenschutzrichtlinie, Anm 11 zu Artikel 13, 208f.

direkt dem Betroffenen nach § 26 Abs 4 mitzuteilen – und nicht etwa dem vermeintlich Bevollmächtigten.[268]

4.7.2 Überwiegende „private" Interessen

Falls die berechtigten Interessen des Auftraggebers oder eines Dritten gegenüber den Interessen des Auskunftswerbers überwiegen, sind die Voraussetzungen für eine berechtigte Nichterteilung der Auskunft erfüllt. Diese Konstellation könnte vorliegen, wenn der Auftraggeber bei voller Auskunftserteilung etwa in einem anhängigen Rechtsstreit mit dem Auskunftswerber seine eigene Prozesssituation schwächen würde. In Bezug auf die überwiegenden Interessen eines Dritten ist die Offenlegung von Geschäftsverbindungen denkbar.[269] Im Konfliktfall ist jedoch eine Interessensabwägung durchzuführen – das Auskunftsinteresse des Betroffenen ist in dem Falle, dass an dem in Frage stehenden Datum vom Betroffenen auch berechtigte Zweifel an seiner Richtigkeit des in Frage stehenden Datums erhoben werden, von größerem Gewicht. Insoweit kann das Argument des Vorliegens berechtigter Zweifel an der Richtigkeit bei dieser Interessenabwägung eine Rolle spielen.[270] In einem Praxisfall machte der Auftraggeber zunächst Geschäftsgeheimnisse geltend (Aufbau und Sicherung des Zugriffs auf die Online-Banking-Applikation). Diese Bedenken erwiesen sich als unbegründet, da ich nicht an Aufbau und Sicherung der Datenbank, sondern vielmehr an den personenbezogenen Daten interessiert war, die zu meiner Person gespeichert wurden (beispielsweise IP-Adresse, Beginn und Ende der Nutzung, Browserversion – derartige Informationen sind auch unter dem Begriff „Digital Fingerprint" bekannt). Ich erhielt in weiterer Folge die gewünschten Auskünfte zum laufenden Geschäftsjahr, die Auswertung der Vorjahre stellte jedoch aus Sicht des Auftraggebers einen unverhältnismäßig hohen Aufwand dar (es wurden folgende Arbeitsschritte mit einer Gesamtdauer von ca zwei Personentagen genannt: Backup-Bänder der betroffenen Daten/Jahre suchen, Backups wiederherstellen, Daten in eine temporäre Datenbank laden, Datenbank-Abfragen schreiben, Abfragen auswerten und exportieren). In diesem Fall wäre der Vollständigkeit halber ein Kostenersatz zu nennen gewesen, anhand dessen ich entscheiden hätte können, ob ich auf vollständige Auskunftserteilung (hinsichtlich des nicht-aktuellen Datenbestands) bestehe.

In einer Entscheidung der DSK begehrte der Betroffene von seinem ehemaligen Arbeitgeber Informationen über die von ihm während des Beschäftigungszeitraumes erbrachten Tagesarbeitszeiten, der dabei zurückgelegten Fahrtstrecken sowie der ausbezahlten Tagesdiäten. Der Auftraggeber verweigerte dies aus verschiedenen Gründen, zuletzt mit der Begründung, dass

[268] DSK 7.12.2004, K120.928/0009-DSK/2004.
[269] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/56 in § 26 Anm 23.
[270] VwGH 19.12.2006, 2005/06/0111 = VwSlg 17090 A/2006.

die Tagesarbeitsblätter und Fahrtaufträge unternehmensspezifische Daten und personenbezogene Daten Dritter (Kunden, sonstige Geschäftspartner) enthielten. Derartige berechtigte überwiegende Interessen an der Geheimhaltung besagter Daten gegenüber dem ehemaligen Mitarbeiter, dem diese Daten bereits bekannt gewesen waren, waren aber im vorliegenden Fall nicht erkennbar.[271] Im Übrigen müsste dies für jeden Kundenkontakt getrennt begründet werden, da § 26 Abs 2 den Auftraggeber nicht unbedingt berechtigt, zur Gänze von der Auskunftserteilung abzusehen, sondern nur soweit überwiegende berechtigte Interessen entgegenstehen. Ein pauschaler Hinweis auf die Verletzung von Betriebs- und Geschäftsgeheimnissen vermag einen Auftraggeber nicht generell von der Pflicht zur Auskunftserteilung zu entbinden.[272] Die Bekanntgabe des konkreten Sachbearbeiters ist für die Verfolgung der Rechte auf Geheimhaltung bzw Löschung nicht notwendig – das Geheimhaltungsinteresse des Sachbearbeiters überwiegt in diesem Fall das Auskunftsinteresse des Betroffenen.[273] Eingeschränkt werden kann der Anspruch auf Beauskunftung der Herkunft der Daten durch einen übermäßigen Suchaufwand beim Auftraggeber.[274]

Weiters wird das Auskunftsrecht durch die Amtsverschwiegenheit nach Art 20 Abs 3 B-VG und Berufsgeheimnisse[275] beschränkt. In einer aktuellen Entscheidung der DSB hatte diese zu beurteilen, ob sich der Beschwerdegegner zu Recht auf die anwaltliche Verschwiegenheitspflicht bzw überwiegende berechtigte Interessen berufen und somit die Erteilung der begehrten Auskunft zur Gänze verweigern konnte. Im Zusammenhang mit Berufsgeheimnissen bedarf es besonderer Umstände, um ein überwiegendes Interesse des Auftraggebers oder des Dritten an der Nichterteilung der Auskunft über die eigenen Daten des Betroffenen zu begründen. Die Verweigerung der Auskunft ist detailliert schriftlich zu begründen, damit sowohl der Betroffene als auch die DSB die Gründe nachvollziehen können.[276]

4.7.3 Überwiegende öffentliche Interessen

Überwiegende öffentliche Interessen können gemäß § 26 Abs 2 ebenfalls der Auskunftserteilung entgegenstehen, diese ergeben sich aus der Notwendigkeit

- des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder
- der Sicherung der Einsatzbereitschaft des Bundesheeres oder
- der Sicherung der Interessen der umfassenden Landesverteidigung oder
- des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder

[271] DSK 21.8.2001, K120.734/014-DSK/2001.
[272] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/56 in § 26 Anm 25a.
[273] DSK 2.8.2005, K121.038/0006-DSK/2005.
[274] DSK 12.11.2004, K120.902/0017-DSK/2004 und DSK 20.5.2005, K120.908/0009-DSK/2005.
[275] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/56 in § 26 Anm 24 verweist dabei auf § 9 RAO, § 91 WTBG, § 37 NO und § 38 BWG. Weiters ist § 18 ZivMediatG zu nennen.
[276] DSB 9.3.2015, DSB-D122.299/0003-DSB/2015; DSB 27.10.2014, DSB-D122.215/0004-DSB/2014.

- der Vorbeugung, Verhinderung oder Verfolgung von Straftaten.

Diese Beschränkungen sind als eine beispielhafte Aufzählung zu verstehen, da der Art 13 DSRL weitergehende Ausnahmen (ua „Feststellung von Straftaten“) zulässt.[277] Unter dem Ausnahmetatbestand „öffentliche Sicherheit“ sind alle polizeilichen Funktionen staatlicher Organe einschließlich der Verbrechensverhütung zu verstehen. Do wäre auch eine Einschränkung des Auskunftsrechts aus Gründen der Aufrechterhaltung der öffentlichen Ruhe und Ordnung durch § 26 Abs 2 gedeckt.[278]

In einer Entscheidung der DSK hatte der Auftraggeber die Auskunftserteilung zunächst nach § 26 Abs 2 Z 5 zur Gänze mit der Begründung abgelehnt, dass sich die vom Beschwerdeführer gestellten Fragen auf ein gegen ihn anhängiges strafgerichtliches Verfahren beim Landesgericht für Strafsachen Wien beziehen würden und damit eine Auskunftserteilung auf Grund eines in diesem Zusammenhang bestehenden überwiegenden öffentlichen Interesses (Verfolgung einer Straftat) nicht möglich sei. Das datenschutzrechtliche Auskunftsrecht kann nicht dazu benutzt werden, um im strafprozessualen Vorverfahren dem Beschuldigten Kenntnis vom jeweiligen Stand der Ermittlungen gegen ihn zu verschaffen – diesen Zweck kann er nur im Rahmen der ihm von der StPO hiefür zur Verfügung gestellten Mittel verfolgen. Im vorliegenden Fall war ein überwiegendes öffentliches Interesse an der Geheimhaltung der Informationen über die Rechtsgrundlage der Ermittlung dieser Daten nicht erkennbar; zudem müssen die Ermittlungsquellen spätestens im Strafprozess schon im Hinblick auf ihre Beweiskraft offengelegt werden.[279] Ein weiterer Fall betraf das BMI: die besonderen Verfahrensvorschriften im Disziplinarverfahren sehen Regelungen über die Akteneinsichtnahme durch die Parteien vor – diese spezielle Bestimmung geht dem Auskunftsrecht nach § 26 DSG vor.[280]

Entsprechend § 26 Abs 5 ist in jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in Abs 2 Z 1 bis 5 bezeichneten Aufgaben betraut sind, dem Auskunftswerber anstelle einer inhaltlichen Begründung der Hinweis zu geben, dass keine der Auskunftspflicht unterliegenden Daten über den Auskunftswerber verwendet werden – jedoch nur, „soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, die eine Auskunftsverweigerung erfordert“.[281] Diese Antwort ist in allen Fällen, in welchen keine Auskunft erteilt wird – also auch weil tatsächlich keine Daten verwendet werden, zu geben. Der Auftraggeber hat folglich nach

[277] AA jedoch *Drobesch/Grosinger*, Datenschutzgesetz, Anm 5 zu § 26 Abs 2, 207.
[278] *Drobesch/Grosinger*, Datenschutzgesetz, Anm 4 zu § 26 Abs 2, 206 mit Hinweis auf die bei *Dammann/Simitis*,203 abgedruckte Begründung des Richtlinienvorschlags.
[279] DSK 28.6.2006, K121.075/0013-DSK/2006.
[280] DSK 16.5.2008, K121.323/0007-DSK/2008.
[281] Siehe Begriff Standardantwort, 21.

§ 26 Abs 5 vorzugehen, wenn die Voraussetzungen für die Erteilung der standardisierten Auskunft vorliegen – er hat dabei keinen Ermessensspielraum.[282] Die Zulässigkeit der Auskunftsverweigerung aus Gründen der überwiegenden öffentlichen Interessen iSd § 26 Abs 2 unterliegt der Kontrolle durch die DSB nach § 30 Abs 3 und dem besonderen Beschwerdeverfahren vor der DSB gemäß § 31a Abs 4.[283,284] In jenen Fällen, in denen diese Sonderregelung nicht anwendbar ist und dennoch die Auskunft verweigert werden soll (beispielsweise aufgrund überwiegender Geheimhaltungsinteressen des Auftraggebers oder eines Dritten), ist die Vorgehensweise inhaltlich gemäß § 26 Abs 4 zu begründen.[285] Es werden regelmäßig auch Daten verarbeitet, die nicht dem Auskunftsanspruch unterliegen (beispielsweise Bekanntgabe der Speicherdauer von Daten[286]).

4.8 Mitwirkungspflicht des Auskunftswerbers

Der Auskunftswerber hat gemäß § 26 Abs 3 am Auskunftsverfahren über Befragung in dem ihm zumutbaren Ausmaß mitzuwirken, um ungerechtfertigten und unverhältnismäßigen Aufwand beim Auftraggeber zu vermeiden. Der Auftraggeber muss grundsätzlich seinen gesamten Datenbestand nach personenbezogenen Daten zum Auskunftswerber durchsuchen – je umfangreicher dieser Datenbestand ist, desto mehr Zeit nimmt die Bearbeitung des Auskunftsbegehrens in Anspruch. Der Auftraggeber kann den Auskunftswerber auffordern, im Rahmen seiner Mitwirkungsobliegenheit jene Sachverhalte oder Dokumente, hinsichtlich welcher er genauere Auskunft begehrt, näher zu bezeichnen. Die Formulierung „über Befragung“ legt den Schluss nahe, dass der Auftraggeber nicht ohne Rücksprache mit dem Auskunftswerber die Auskunftserteilung mit der Begründung eines ungerechtfertigten oder unverhältnismäßigen Aufwands verweigern kann. In diesem Fall muss von der Unvollständigkeit der Auskunftserteilung ausgegangen werden.[287] Das Zitat einer unpassenden Gesetzesstelle schadet der objektiven Qualifikation als Auskunftsverlangen nicht. Hätte der Beschwerdegegner im vorliegenden Fall tatsächlich Zweifel gehabt, welches Recht der Beschwerdeführer ausüben wollte, so hätte er diesen im Rahmen der Mitwirkungspflicht zur Klärung auffordern können.[288] Daher ist dem Auftraggeber zu empfehlen, dass er die an den Betroffenen gerichtete Befragung dokumentiert und nachweisbar festhält.[289] Wenn der Auskunftswerber nicht bereit ist, trotz mehrfacher Aufforderung/Rechtsbelehrung durch den Auftraggeber die Datenverarbeitungen zu bezeichnen,

---

[282] *Drobesch/Grosinger*, Datenschutzgesetz, Anm 3 zu § 26 Abs 5, 209.
[283] VwGH 6.6.2007, 2001/12/0004 = VwSlg 17215 A/2007.
[284] Siehe auch ErlRV 1613 BlgNR XX. GP, 47 – dort wird näher auf die zuvor geltende Rechtslage im § 4 Z 3 DSG 1978 eingegangen. Vormals § 31 Abs 4, nunmehr § 31a Abs 4, vgl ErlRV 472, BlGNR XXIV. GP, 14 – ausführlicher dazu *Jahnel*, Datenschutzrecht, 526-528 in 9/48.
[285] Vgl *Drobesch/Grosinger*, Datenschutzgesetz, Anm 2 zu § 26 Abs 5, 208.
[286] DSK 28.6.2006, K121.075/0013-DSK/2006.
[287] DSK 16.5.2008, K121.323/0007-DSK/2008.
[288] DSK 16.11.2004, K120.959/0009-DSK/2004.
[289] *Drobesch/Grosinger*, Datenschutzgesetz, Anm 2 zu § 26 Abs 2, 207.

bezüglich derer er Betroffener sein kann, so kann die Auskunft zu Recht verweigert werden, da eine Suche in allen denkbaren Datenanwendungen wohl mit einem ungerechtfertigten und unverhältnismäßigen Aufwand verbunden wäre.[290]

Der Auskunftswerber wird etwa durch Kopien automationsunterstützt erstellter Schriftstücke, Adressen-Aufkleber und dergleichen glaubhaft machen können, dass seine Daten verarbeitet wurden. Wenn er seinem Auskunftsersuchen ein solches Indiz beifügt, so wird er zumeist schon dadurch seine Mitwirkungspflicht erfüllt haben. Diese Art der Mitwirkung wird ihm jedenfalls zumutbar sein.[291] Steht aber die Datenanwendung, über die Auskunft gegeben werden soll fest, und ist auch der zeitliche Rahmen des Auskunftsbegehrens in zumutbarer Weise abgegrenzt, dann bedarf es keiner weiteren Klarstellungen des Betroffenen. Die Mitwirkungsverpflichtung des Betroffenen darf insb nicht dahingehend missverstanden werden, dass den Betroffenen die Beweislast dafür trifft, dass Übermittlungen tatsächlich stattgefunden haben. Sie soll nur einen unverhältnismäßigen Aufwand beim Auftraggeber vermeiden.[292] Die DSB präzisierte in zwei aktuellen Entscheidungen die Mitwirkungsobliegenheit durch den Betroffenen weiter und führte aus, dass es dem Beschwerdeführer angesichts der in der gegenständlichen Aufstellung angeführten Datenanwendungen, die zum Teil auf einen bestimmten Beruf, den Gesundheitszustand, den Wohnort, die Freizeitgestaltung etc. des betroffenen Personenkreises abstellen, sehr wohl möglich und zumutbar gewesen wäre, anhand seiner konkreten Lebensumstände das Auskunftsbegehren auf bestimmte Datenanwendungen einzuschränken bzw bestimmte Datenanwendungen davon auszuschließen, um im Rahmen seiner Mitwirkungspflicht gemäß § 26 Abs 3 den notwendigen Suchaufwand möglichst zu begrenzen.[293] Dasselbe gilt hinsichtlich anderer sich allenfalls aus § 26 Abs 3 ergebender Mitwirkungsverpflichtungen der Auskunftswerberin. Ist etwa, wie von der Beschwerdegegnerin behauptet, die Erteilung der Auskunft ohne Kenntnis des Geburtsdatums der Beschwerdeführerin nicht möglich, wäre ihr dies mitzuteilen und sie um Mitwirkung zu ersuchen, wobei die Mitteilung (Befragung) auch eine schlüssige Begründung für die Aktualisierung der Mitwirkungspflicht zu enthalten hätte.[294] Die Aufforderung zur Bekanntgabe des Geburtsdatums durch den Auftraggeber zwecks eindeutiger Identifizierbarkeit des Betroffenen stellt keine unzulässige Beschränkung des Auskunftsrechts dar.[295]

---

[290] DSK 25.3.2003, K120.744/001-DSK/2003; vgl DSK 21.1.2009, K121.414/0003-DSK/2009.
[291] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/56f in § 26 Anm 26.
[292] DSK 3.9.2002, K120.790/010-DSK/2002 mit Verweis auf ErlRV 1613 BlgNR XX. GP, 47.
[293] DSB 3.3.2015, DSB-D122.272/0004-DSB/2014 und DSB 3.3.2015, DSB-D122.273/0002-DSB/2015; ebenso DSK 16.12.2009, K121.541/0012-DSK/2009.
[294] DSK 4.5.2004, K120.905/0008-DSK/2004.
[295] VwGH 18.3.1992, 91/12/0007 = EDVuR 1992/11, 191-194.

Die Organisation der Datenanwendung PAD (elektronisches „Protokoll-, Akten- und Datensystem“ zur Dokumentenverwaltung bei den Polizeibehörden) wird durch § 13 Abs 2 SPG[296] normiert. Hiebei sind auch datenschutzrechtliche Kriterien festgelegt, die verhindern sollen, dass aus einem elektronischen Aktenindex unschwer ein Personenprofil durch Abfrage, ob und in welchem Zusammenhang eine Person bei den Polizeibehörden auffällig geworden ist, erstellt werden kann. So darf gemäß § 13 Abs 2 letzter Satz SPG die Auswählbarkeit von Daten aus der Gesamtmenge der gespeicherten Daten allein mit einem Namen nicht vorgesehen sein; vielmehr ist für die Auswahl zusätzlich zum Namen ein auf einen Sachverhalt bezogenes weiteres Datum anzugeben, was nur dann zu einem „Treffer“ führt, wenn ein Dokument im PAD mit beiden Suchkriterien beschlagwortet wurde. Wenn es für Zwecke einer „besseren“, weil umfangreicheren Auskunftserteilung erforderlich wäre, gesetzlich vorgesehene Suchbeschränkungen wie jene des § 13 Abs 2 letzter Satz SPG aF umgehbar zu machen, wäre damit der bezweckte Schutz des Betroffenen vereitelt: Es widerspricht aber dem Grundgedanken des Datenschutzes, wenn personenbezogene Daten, die so gespeichert sind, dass sie angesichts des in einer konkreten Datenverarbeitung vorgesehenen Suchsystems nur durch sequentielles Prüfen von Datensätzen gefunden werden können, „künstlich“ direkt findbar gemacht werden müssten. Dadurch würde ohne sachliche Notwendigkeit eine erleichterte Auffindbarkeit der Daten ermöglicht, - ein dem Datenschutz geradezu diametral entgegengesetztes Ergebnis. Die Grenzen des Auskunftsrechts sind somit eng mit der Frage verbunden, wie der Auftraggeber mit Hilfe des für ihn verfügbaren automationsunterstützten Suchsystems Daten zulässigerweise finden darf und kann. Im Geltungsbereich des § 13 Abs 2 SPG aF wird davon auszugehen sein, dass andere Suchsysteme als das PAD nicht eingesetzt werden dürfen, soweit dadurch die Gefahr bestünde, dass die im Interesse des Betroffenen geschaffene Schutzfunktion des § 13 Abs 2 SPG aF unterlaufen wird. Demzufolge wird aber ein Auskunftsersuchen im Anwendungsbereich des § 13 Abs 2 SPG aF, welches als einziges Suchkriterium den Namen des Betroffenen nennt, a priori zum Scheitern verurteilt sein, da der Name als einziges Suchkriterium keinen „Treffer“ liefern darf. Dieser Umstand bedingt nach Ansicht der Datenschutzkommission allerdings eine besondere „Aufklärungspflicht“ des polizeilichen Auftraggebers: Unter Hinweis auf die Bestimmung des § 13 Abs 2 letzter Satz SPG aF wären die Beschwerdeführer gemäß § 26 Abs 3 DSG 2000 zur Mitwirkung am Auskunftsverfahren in Form der Bekanntgabe von Sachverhaltselementen aufzufordern gewesen, welche das Auffinden von Daten über die Betroffenen überhaupt erst ermöglicht.[297]

[296] § 13 SPG Abs 2 wurde in der Zwischenzeit aufgehoben, dementsprechend ist an dieser Stelle darauf hinzuweisen, dass sich die von der DSK zitierte Bestimmung auf § 13 Abs 2 idF BGBl. I Nr. 151/2004 bezieht.
[297] DSK 12.4.2007, K121.142/0003-DSK/2007.

4.9 Reaktionsfrist

§ 26 Abs 4 normiert, dass dem Auskunftswerber die Auskunft innerhalb von acht Wochen nach Einlangen des Begehrens zu erteilen oder schriftlich zu begründen ist, warum sie nicht oder nicht vollständig erteilt wird. Dabei obliegt es dem Auskunftswerber, die Tatsache des Einlangens nachzuweisen.[298] Die achtwöchige Frist für die Auskunftserteilung beginnt somit mit dem Einlangen beim Auftraggeber oder Dienstleister (vgl § 26 Abs 10). Die Auskunft gilt auch als rechtzeitig erteilt, wenn der Auftraggeber diese innerhalb der acht Wochen zur Post bringt.[299] Wenn zunächst kein ausreichender Nachweis der Identität vorlag und dieser durch den Auskunftswerber nachgereicht wird, so beginnt die Achtwochenfrist für die Auskunftserteilung erst mit vollständigem Einlangen des Auskunftsbegehrens beim Auftraggeber und nicht rückwirkend (wie vom Beschwerdeführer im vorliegenden Fall irrtümlich angenommen) mit der erstmaligen Anfrage.[300]

Die Überschreitung der achtwöchigen Auskunftsfrist begründet in der Regel ab jenem Augenblick keine durch Feststellungsbescheid rügbare Verletzung des § 26 mehr, in dem tatsächlich Auskunft erteilt wurde. Sobald dies – und sei es auch verspätet – geschehen ist, ist der Zweck des Auskunftsrechts erfüllt.[301] Ein darüber hinausgehendes subjektives Recht des Betroffenen auf bescheidmäßige Feststellung einer Überschreitung der achtwöchigen Auskunftsfrist oder des Umstandes, dass die Beschwerde im Zeitpunkt ihrer Erhebung berechtigt war, hat der Gesetzgeber expressis verbis nicht normiert.[302]

Die Auskunft ist vollständig schriftlich zu erteilen, mit Zustimmung des Auskunftswerbers kann die Auskunft davon abweichend auch mündlich mit der Möglichkeit der Einsichtnahme[303] und der Abschrift oder Ablichtung erteilt werden (vgl § 26 Abs 1). Wenn die Auskunft nicht oder nicht vollständig erteilt wird, so ist dies ebenfalls binnen acht Wochen dem Auskunftswerber schriftlich begründet mitzuteilen. § 26 Abs 4 bestimmt weiters, dass von der Erteilung der Auskunft auch deshalb abgesehen werden kann, weil der Auskunftswerber am Verfahren nicht gemäß § 26 Abs 3 mitgewirkt[304] oder weil er den Kostenersatz[305] nicht geleistet hat.

---

[298] DSK 22.4.2005, K120.879/0003-DSK/2005.
[299] *Drobesch/Grosinger*, Datenschutzgesetz, Anm 1 zu § 26 Abs 4, 207.
[300] DSK 5.6.2009, K121.525/0004-DSK/2009.
[301] VwGH 27.9.2007, 2006/06/0330, jusIT 2008/31, 72 mit Anm von *Jahnel* mit Verweis auf den zugrundeliegenden Bescheid DSK 12.3.2004, K120.892/0003-DSK/2004.
[302] DSK 7.6.2005, K120.912/0008-DSK/2005; vgl weiters DSK 30.6.2005, K120.977/0005-DSK/2005; DSK 18.5.2004, K120.899/0004-DSK/2004; DSK 1.7.2003, K120.698/002-DSK/2003 und DSK 26.2.2002, K120.760/004-DSK/2002.
[303] Die Möglichkeit der Einsichtnahme ist von der Bereitschaft des Auftraggebers, Einsicht zu gewähren, abhängig so DSK 16.12.2009, K120.973/0015-DSK/2009.
[304] Siehe Begriff Mitwirkungsobliegenheit, 53.
[305] Siehe Begriff Kostenersatz, 29.

Daraus lässt sich die Pflicht zur Reaktion durch den Auftraggeber ableiten – selbst wenn das Begehren auf Auskunft unvollständig sein sollte oder der Identitätsnachweis[306] fehlt, hat der Auftraggeber den Auskunftswerber im Rahmen der Mitwirkungsobliegenheit zu befragen, um binnen der Achtwochenfrist die Auskunft vollständig erteilen zu können (bzw schriftlich begründen zu können, warum die Auskunft nicht oder nicht vollständig erteilt wird). Wenn der fehlende Identitätsnachweis auch nach Aufforderung durch den Auftraggeber nicht nachgereicht wird, so reduziert sich der Vollanspruch darauf, eine entsprechende schriftliche Begründung für die Nichterteilung der Auskunft zu erhalten. Das Unterbleiben jeglicher Reaktion des datenschutzrechtlichen Auftraggebers auf ein Auskunftsbegehren verletzt den Betroffenen aber jedenfalls in seinem subjektiven Recht gemäß § 26 Abs 1 und 4 und damit implizit auch im Grundrecht auf Datenschutz (Auskunft) gemäß § 1 Abs 3 Z 1.[307]

4.10 Löschungsverbot

Für den Auftraggeber besteht gemäß § 26 Abs 7 ein viermonatiges Vernichtungsverbot[308] ab dem Zeitpunkt der Kenntnis von einem Auftraggeber für die Daten über den Betroffenen. Diese Vorgabe besteht bis zum rechtskräftigen Abschluss des Verfahrens (schließt mE wohl auch etwaige Rechtsmittelzüge an BVwG/VwGH ein, und nicht nur das Beschwerdeverfahren vor der DSB selbst[309]), sofern der Auskunftswerber eine Beschwerde gemäß § 31 an die DSB erhebt. Da den Auftraggeber auch im Falle der Heranziehung eines Dienstleisters die volle datenschutzrechtliche Verantwortung gegenüber dem Betroffenen trifft, hat der Auftraggeber sicherzustellen, dass das Löschungsverbot auch durch den Dienstleister eingehalten wird. Diese Bestimmung trifft weiters die Auftraggeber gemäß § 4 Z 4 letzter Halbsatz.[310]

§ 26 Abs 7 sieht keinerlei Einschränkungen für das Löschungsverbot vor, wie beispielsweise kapazitätsorientierte oder zu festen Zeitpunkten vorgenommene Löschungen.[311] Die DSK hielt zur Konkurrenz von Auskunfts- und Löschungsrecht im § 26 Abs 7 fest, dass § 26 Abs 7 als lex specialis § 27 Abs 1 und 4 vorgehe, auch dann, wenn grundsätzlich die Voraussetzungen für die Löschung gegeben sind. Die Daten dürfen in einem solchen Fall erst gelöscht werden,

---

[306] Ua DSK 6.9.2013, K121.964/0015-DSK/2013; DSK 10.4.2013, K121.924/0006-DSK/2013.

[307] DSK 7.12.2004, K120.928/0009-DSK/2004; vgl weiters DSK 13.12.2013, K122.039/0008-DSK/2013; DSK 16.5.2008, K121.323/0007-DSK/2008; DSK 23.5.2007, K121.259/0013-DSK/2007; DSK 20.5.2005, K120.897/0003-DSK/2005; DSK 4.5.2004, K120.905/0008-DSK/2004. Vgl Dohr/Pollirer/Weiss/Knyrim, DSG², 210/56a in § 26 Anm 27.

[308] In DSK 5.12.2008, K121.410/0008-DSK/2008 hielt die DSK fest: „Der Begriff 'vernichten' in § 26 Abs. 7 DSG 2000 umfasst dabei sowohl das Löschen von Daten in automationsunterstützt geführten Datenanwendungen wie auch das Unleserlichmachen von Daten auf oder die physische Zerstörung von sonstigen Datenträgern einer (manuellen) Datei."

[309] AA jedoch *Jahnel*, Datenschutzrecht, 400 in 7/49.

[310] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/58 in § 26 Anm 33.

[311] AA jedoch *Drobesch/Grosinger*, Datenschutzgesetz, Anm zu § 26 Abs 7, 210 welche noch die AB zum § 25 Abs 8 DSG 1978 zitieren.

wenn das Auskunftsbegehren im Sinne von § 26 Abs 7 als erledigt gelten kann, dh mit Ablauf der Viermonatsfrist bzw Beendigung des Beschwerdeverfahrens vor der DSB.[312] Mit dieser Bestimmung soll insb sichergestellt werden, dass bei Erhebung einer Auskunftsbeschwerde an die Datenschutzkommission innerhalb dieser vier Monate noch Daten vorhanden sind und daher überhaupt sinnvollerweise eine Auskunftsbeschwerde erhoben werden kann.[313] Mit der DSG-Novelle 2010 wurde klargestellt, dass sich die in § 26 Abs 7 vorgesehene Speicherfrist von vier Monaten verkürzt, wenn der Auskunftswerber gleichzeitig oder etwa gleich nach Erhalt der Auskunft ein Löschungsbegehren (§ 27 Abs 1 Z 2) stellt oder Widerspruch (§ 28) gegen eine Datenverarbeitung erhebt. Diesfalls ist – sofern das Löschungsbegehren oder der Widerspruch berechtigt ist – unverzüglich eine Löschung der Daten vorzunehmen.[314,315] Auch wenn nach Löschung aktuell keine Daten mehr verarbeitet werden – eine Löschung nach Einlangen des Auskunftsbegehrens würde eine Verletzung des § 26 Abs 7 bedeuten – muss das Auskunftsbegehren beantwortet werden (insb Herkunft, Tatsache der Löschung, Verwendungszweck).[316]

4.11 Konkurrenz zu weiteren Einsichtsrechten

In § 26 Abs 8 wird bestimmt, dass das Auskunftsrecht nach Maßgabe der das Einsichtsrecht (hinsichtlich der zur Person verarbeiteten Daten) vorsehenden Bestimmungen für jene Datenanwendungen besteht, die von Gesetzes wegen einsehbar sind. Damit wird insb auch die immer häufiger werdende Führung elektronischer Verfahrensakten durch Behörden jedenfalls hinsichtlich der Verfahrensparteien umfasst (zB § 17 AVG, §§ 90 f BAO). Wenn durch das Einsichtsrecht nicht alle Bestandteile einer Auskunft nach § 26 Abs 1 erlangt werden können[317], besteht darüber hinaus – soweit Informationen vorhanden sind – das Auskunftsrecht nach dem DSG 2000. Bei (teil-)öffentlichen Registern ist freilich die Bekanntgabe von Empfängerkreisen – mehr wird im Hinblick auf fehlendes Rechtsschutzbedürfnis im Regelfall nicht erforderlich sein[318] – schon durch den dem Auskunftswerber bekannten Umstand der (teil-)öffentlichen Einsehbarkeit verwirklicht. Weiterhin nicht möglich sein soll freilich die Umgehung

[312] DSK 5.4.2005, K120.873/0003-DSK/2005; DSK 18.1.2008, K121.327/0002-DSK/2008.
[313] DSK 21.1.2009, K121.407/0001-DSK/2009.
[314] ErlRV 472, BlGNR XXIV. GP, 11.
[315] *Jahnel*, Datenschutzrecht, 401 in 7/49 ergänzt, dass dasselbe aber nach dem Wortlaut der neuen Regelung auch für jedes berechtigte Löschungsbegehren und jeden berechtigten Widerspruch gelten müsse, die zwar später, aber immer noch innerhalb der grundsätzlichen Sperrfrist von vier Monaten gestellt werden.
[316] DSK 3.8.2004, K120.921/0006-DSK/2004. *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/64 weisen mE zu Recht darauf hin, dass unklar sei, wie bei gelöschten Daten deren Herkunft beauskunftet werden kann.
[317] Beispielsweise Inhalt eines elektronischen Verfahrensverzeichnisses, so *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/58f in § 26 Anm 36.
[318] Vgl VwGH 19.12.2006, 2005/06/0111 = VwSlg 17090 A/2006.

von Beschränkungen von Einsichtsrechten durch das Auskunftsrecht: Die für die Beschränkung maßgeblichen Gründe werden idR auch nach § 26 Abs 2 eine Ablehnung der Auskunft ermöglichen.[319]

Jahnel weist in diesem Zusammenhang auf die wirtschaftlichen Gesichtspunkte zum Ausschluss des Auskunftsrechts bei öffentlichen Punkten auf den Aspekt hin, dass die Einnahmen aus externen Grundbuch- und Firmenbuchabfragen für das Justizressort einen nicht unerheblichen Budgetbeitrag leisten. Da die Auskunft nach dem DSG für den (praktisch relevanten) aktuellen Datenbestand kostenfrei ist, könnte so die Kostenpflicht der externen Abfrage hinsichtlich der eigenen Eintragungen unterlaufen werden.[320]

In einer Entscheidung der DSK brachte der Beschwerdeführer vor, dass er in seinem Recht auf Auskunft dadurch verletzt worden sei, dass ihm zwar mitgeteilt wurde, dass über ihn ein Akt im polizeilichen Aktenverwaltungssystem PAD angelegt worden sei, verweigerten ihm jedoch die direkte Kenntnisnahme des authentischen Inhalts mit der Begründung, dass man damit „den bisherigen Gepflogenheiten“ entspräche. Der von den Regelungen über die Akteneinsicht erfasste Bereich fällt daher als Spezialfall der direkten Kenntnisnahme des authentischen Inhalts (auch) elektronisch dokumentierter Aktenstücke unter die Ausnahmebestimmung des § 26 Abs 8. Das Auskunftsrecht nach § 26 DSG 2000 ermöglicht den Betroffenen, von den sie betreffenden Akten Kenntnis zu erlangen – die Frage, ob sie Anspruch darauf haben, vom Inhalt des Aktes zu erfahren, wird aber durch die jeweiligen Bestimmungen über die Akteneinsicht geregelt. Im vorliegenden Fall war die die Einsicht in den elektronischen Akt eines kriminalpolizeilichen Ermittlungsverfahrens nur nach den dafür vorgesehenen Regeln (§§ 51 ff StPO) zulässig. Dies zeigt sich auch aus § 53 Abs 2 StPO, der ausdrücklich die Möglichkeit einer „elektronischen Akteneinsicht“ vorsieht, also auch elektronisch dokumentierte Ermittlungsakten erfasst. Daraus folgt, dass die Beschwerdegegnerin den Beschwerdeführer durch die Ablehnung einer inhaltlichen Auskunft über die im PAD verarbeiteten, ihn betreffenden äußeren Verfahrensdaten des kriminalpolizeilichen Ermittlungsverfahrens in seinem Recht auf Auskunft verletzt hat.[321]

4.12 Auskunftsrecht in Deutschland und Schweiz

4.12.1 Deutschland

Im Bundesdatenschutzgesetz ist der Auskunftsanspruch in § 19 („Auskunft an den Betroffenen“) geregelt. Die Voraussetzungen in § 19 Abs 4, nach denen die Auskunftserteilung unterbleiben kann, ist nahezu ident mit denen im öDSG. Wie § 6 Abs 1 festhält, kann das Recht auf

[319] ErlRV 472, BlGNR XXIV. GP, 11.
[320] *Jahnel*, Datenschutzrecht, 402 in 7/50.
[321] DSK 24.11.2010, K121.632/0008-DSK/2010.

Auskunft nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden. Die Auskunft von öffentlichen Stellen ist kostenlos (§ 19 Abs 7), im privaten Bereich kann ein Kostenersatz in Rechnung gestellt werden (§ 34 Abs 8), wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Im Fall von Scoring (§ 28b iVm § 34 Abs 2) sind die Algorithmen offenzulegen. Hinsichtlich der Fristsetzung wird empfohlen, dem Auftraggeber einen Zeitpunkt mitzuteilen, bis wann man gerne Auskunft haben möchte[322].In Deutschland ist die Beauskunftung von personenbezogenen Daten eines Verstorbenen möglich, da § 3 BDSG („Begriffsbestimmungen“) auf Einzelangaben über natürliche Personen abstellt – vom Schutzbereich des BDSG sind folglich Verstorbene nicht erfasst.[323]

4.12.2 Schweiz

Schweiz: Im Bundesgesetz über den Datenschutz ist der Auskunftsanspruch in Art 8 („Auskunftsrecht“) geregelt. Hervorzuheben sind dabei Art 8 Z 3, bei der der Inhaber der Datenanwendung medizinische Daten durch einen Arzt mitteilen lassen kann und Z6, in welcher ausdrücklich normiert wird, dass niemand im Voraus auf das Auskunftsrecht verzichten kann. Art 9 („Einschränkungen des Auskunftsrechts“) sieht allgemeine, mit Art 13 DSRL vergleichbare Beschränkungen vor. Art 10 („Einschränkungen des Auskunftsrechts für Medienschaffende“) hingegen normiert spezielle Vorschriften für Medien, aufgrund derer Inhaber einer Datenanwendung die Auskunft verweigern können, wenn diese ausschließlich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums verwendet wird oder die Datensammlung ausschließlich als persönliches Arbeitsinstrument dient. Im Unterschied zu Österreich sind im Todesfalle sehr wohl Auskünfte über den Verstorbenen möglich (nahe Verwandtschaft oder Ehe mit der verstorbenen Person begründen automatisch ein Interesse), so Art 1 Z 7 VDSG. Als Frist zur Auskunftserteilung sind 30 Tage vorgesehen – benötigt der Inhaber der Datenanwendung jedoch länger, so hat er den Gesuchsteller darüber zu benachrichtigen und ihm die Frist mitzuteilen (Art 1 Z 4 VDSG). Zudem wird die Kostenersatzpflicht mit maximal 300 Franken limitiert (das entspricht zurzeit etwa € 275,-).

Wie das Auskunftsrecht in Deutschland und Schweiz zeigt, ist die Herangehensweise hinsichtlich einiger „Subthemen“ durchaus unterschiedlich, dazu gehören die Fristsetzung, der Kostenersatz (Deckelung), Verzicht im Voraus auf Auskunftserteilung nicht möglich, Auskunft für Verstorbene, Aufschub der Auskunftserteilung (Art 9 Schweizer DSG) sowie keine Formvorschriften bei Verweigerung, Einschränkung oder Aufschub der Auskunftserteilung für natürliche Personen („private Inhaber“ iSd Art 9 Abs 5 Schweizer DSG)[324]. Besonders beim Kosten-

[322] Vgl „Datenschutz-Wiki“ des BfDI, https://www.bfdi.bund.de/bfdi_wiki/index.php/Auskunftsrecht, abgerufen am 12. September 2016.
[323] Landgericht Berlin 17.12.2015, 20 O 172/15.
[324] Ausführlicher dazu *Widmer* in Passadelis/Rosenthal/Thür (Hrsg.), Datenschutzrecht, 149(159).

ersatz wäre mE eine Deckelung zur Rechtssicherheit wünschenswert, ebenso ist zu überlegen, ob es nicht auch in Österreich möglich sein sollte, Auskünfte über Verstorbene einzuholen. Ungelöst ist nach wie vor die Thematik der Beauskunftung von Standortdaten durch Telekommunikationsdiensteanbieter.

4.13 Besondere Auskunftsrechte

Als Besonderheiten hinsichtlich den Modalitäten der Auskunftserteilung sind die automatisierte Einzelentscheidung (§ 49 Abs 3)[325], die Informationsverbundsysteme (§ 50 Abs 1) sowie die Videoüberwachung (§ 50e) hervorzuheben.

4.13.1 Automatisierte Einzelentscheidungen in § 49 Abs 3 DSG

Automatisierte Einzelentscheidungen gewinnen zunehmend an wirtschaftlicher Bedeutung, sei es nun im Geschäftsfeld von Wirtschaftsauskunftsdiensten oder Adressverlagen, aber auch bei Matchingplattformen (Partner- oder Arbeitgebervermittlung) und Geschwindigkeitsmessgeräten werden derartige Algorithmen genutzt. § 49 Abs 1 nennt drei konkrete Anwendungsbereiche automatisierter Einzelentscheidungen: die Bewertung der beruflichen Leistungsfähigkeit (zB durch Systeme, die an Hand der Zahl und des Intervalls der Bedienungsvorgänge eines Computersystems Leistungsprofile erstellen), die Bewertung der Kreditwürdigkeit (zB die Errechnung von Score-Werten auf Grundlage der „Zahlungserfahrungsdaten" eines Wirtschaftsauskunftsdienstes) und die qualitative Bewertung des Verhaltens (zB durch Auswertung von Bewegungen eines Betroffenen in den Bilddaten einer oder mehrerer Videoüberwachungen im Hinblick auf verbrechenstypische Verhaltensmerkmale). In allen drei Beispielsfällen ist das Auskunftsinteresse eines Betroffenen an der Logik der Entscheidungsfindung evident.[326] Dem Betroffenen ist dabei über den Auskunftsanspruch nach § 26 auf Antrag der logische Ablauf der automatisierten Entscheidungsfindung in allgemein verständlicher Form[327] darzulegen. § 49 Abs 3 setzt damit die Vorgaben des Art 15 Abs 1 DSRL um. Dieses Recht darf weder das Geschäftsgeheimnis noch das Recht an geistigem Eigentum, insb das Urheberrecht zum Schutz von Software, berühren. Dies darf allerdings nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird.[328] Die DSB hatte sich jüngst in drei Entscheidungen mit dieser Bestimmung auseinanderzusetzen, dabei handelte es sich um zwei Wirtschaftsauskunftsdienste und einen Adressverlag.[329]

---

[325] *Preiß*, Die Bedeutung der Risikoanalyse für den Rechtsschutz bei automatisierten Verwaltungsstrafverfahren.
[326] DSB 10.3.2016, DSB-D122.322/0001-DSB/2016.
[327] Siehe Begriff allgemein verständliche Form, 39.
[328] RL 95/46/EG, 41. ErwGr.
[329] DSB 10.3.2016, DSB-D122.322/0001-DSB/2016; DSB-D122.304 und DSB-D122.305. Ausführlicher dazu DSB Newsletter 2/2016, 3f.

4.13.2 Informationsverbundsysteme in § 50 Abs 1 DSG

Die Besonderheit des Informationsverbundsystems ist der Definition im § 4 Z 13 zu entnehmen: es handelt sich dabei um eine Datenanwendung, in welcher von mehreren Auftraggebern Daten verarbeitet werden (insb Zugriffsmöglichkeiten auf Daten, die von anderen Auftraggebern dem System zur Verfügung gestellt wurden). Die Hürde aus Sicht des Auskunftswerbers ist dabei, dass er den Betreiber der Datenanwendung kontaktieren muss, sofern ihm der konkrete Auftraggeber nicht bekannt ist. § 50 Abs 1 2. Satz normiert dabei die Verpflichtung für den Betreiber, dem Betroffenen auf Antrag binnen zwölf Wochen alle Auskünfte zu geben, die notwendig sind, um den für die Verarbeitung seiner Daten im System verantwortlichen Auftraggeber festzustellen. Bei dieser Vorgehensweise kennt der Auskunftswerber jedoch noch nicht die konkret über ihn gespeicherten Daten, sondern lediglich den Auftraggeber, an den er das Auskunftsbegehren nach § 26 richten kann.[330]

4.13.3 Videoüberwachung in § 50e DSG

Hinsichtlich der Videoüberwachung ist festzuhalten, dass nach Rsp der DSB[331] der Auskunftsanspruch nur bei „verarbeiteten Daten“ gegeben ist – bei nicht ausgewerteten Bilddaten einer Videoüberwachung bestehe folglich kein Auskunftsrecht.[332] Die „verarbeiteten Daten“ entstehen erst mit dem Auswertungsanlass (beispielsweise Vandalismus, Verdacht von strafrechtlich relevanten Vorfällen). Der Auftraggeber einer Videoaufzeichnung weiß nicht, „zu wessen Person“ Daten gespeichert sind, und darf es auch – außer im Auswertungsanlassfall – nicht in Erfahrung bringen. Das Bestehen eines Auskunftsrechts aus nicht ausgewerteten Videoaufzeichnungen ist in gleicher Weise zu beurteilen wie dies § 29 DSG für indirekt personenbezogene Daten vorsieht.[333] Art 13 lit g DSRL sieht Einschränkungen vor, um die Rechte und Freiheiten anderer Personen zu wahren. Es soll nicht allein aufgrund eines Auskunftsbegehrens dem Auftraggeber die Kenntnis über die erfassten – anderen – Personen gegeben werden.[334] In Fällen der Echtzeitüberwachung[335] ist das Auskunftsrecht gemäß § 50e Abs 3 ausgeschlossen, da keine Verarbeitung (Speicherung) von Daten vorliegt.[336]

Nach aktueller Rechtslage (§ 50a DSG 2000) wäre eine Auswertung nur wegen „gefährlicher Angriffe“ iSd § 50a Abs 4 Z 1 zulässig. „Gefährliche Angriffe“ iSd Bestimmung sind gerichtlich strafbare Vorsatztaten, Angriffe auf Betriebs- oder Geschäftsgeheimnisse sowie allenfalls grobe Verwaltungsübertretungen. Im Fall der Wiener Linien (Betreiber von U-Bahn-Stationen

---

[330] Ausführlicher ua *Jahnel*, Datenschutzrecht, 481ff in 8/83-8/86.
[331] 2014 und 2015 war die Videoüberwachung der zahlenmäßig größte Anwendungsbereich des Kontroll- und Ombudsmannverfahrens nach § 30 DSG, siehe auch 5.1 KOV, 63.
[332] DSB 15.7.2016, DSB-D122.453/0008-DSB/2016.
[333] DSK 5.12.2008, K121.385/0007-DSK/2008.
[334] DSK 6.9.2013, K121.605/0003-DSK/2013.
[335] Siehe Begriff Echtzeitüberwachung in FN 157575.
[336] ErlRV 472, BlGNR XXIV. GP, 21.

und -Zügen) werden die Bilddaten verschlüsselt gespeichert, die Auswertung erfolgt entweder durch Setzen eines „Markers“ auf dem Datenträger, bei Auslösen der Notruf- oder Notstoppeinrichtung im Fahrgastraum durch einen Fahrgast oder einen Mitarbeiter der Wiener Linien, bzw durch Entnahme des Datenträgers. Für die weitere Entschlüsselung und Auswertung müssen die Datenträger ausgebaut und an die entsprechende Abteilung weitergegeben werden. Dafür gibt es stets einen Übergabeschein. Wenn dieser Übergabeschein nicht vorliegt, so wurde die Kassette nicht ausgebaut und die gespeicherten Daten automatisch überschrieben.[337]

Der VwGH hat in seinem Erkenntnis zur Videoüberwachung festgehalten, dass der Auftraggeber nach Maßgabe des § 26 zu Recht eine Negativauskunft erteilt hatte, da die Bildaufzeichnungen der Videoüberwachungen für den gegenständlichen Ort und Zeitraum nicht ausgewertet wurden – ein weiteres Recht auf Auskunft stehe dem Beschwerdeführer nicht zu. Durch die Verschlüsselung der Videoüberwachung gemäß § 50c Abs 1 hätten die Videodaten nur mit einer speziellen Software ausgewertet werden können – fraglich ist daher, ob es sich um bloß indirekt personenbezogene Daten nach § 29 handelt, welche durch den Auftraggeber mit rechtlich zulässigen Mitteln nicht ausgewertet werden können. Da der einzige Schlüssel bei der DSB zu hinterlegen ist, kann der Auftraggeber der Videoüberwachung die Bilddaten nicht selbständig auf Personen rückführen. Dem Auskunftswerber ist daher lediglich mitzuteilen, dass eine verschlüsselte Videoüberwachung betrieben wird.[338] Im vorliegenden Fall war es dem Auftraggeber sehr wohl möglich, das Videomaterial selbständig zu entschlüsseln. Der Argumentation des VwGH, dass es sich hierbei um für den Auftraggeber indirekt personenbezogene Daten gemäß § 29 handle, kann demnach nicht gefolgt werden.[339]

Der Beschwerdeführer führte im Anlassfall[340] auch ein Auskunftsrecht bei nicht-ausgewerteten Daten der Videoüberwachung an. Eine Positivauskunft sei entsprechend der Einschränkungen des § 50a auf rechtmäßige Zwecke der Einsichtnahme bzw Auswertung nur dann zu erteilen, wenn die Daten der Videoüberwachung bereits ausgewertet worden waren, bevor das Auskunftsbegehren vorlag. Die Auswertung aufgrund eines Auskunftsbegehrens stellt keinen rechtmäßigen Zweck in der taxativen Aufzählung des § 50a dar. Der Auftraggeber einer Videoüberwachung ist *Gerhartl* zufolge nur selten berechtigt, die Daten der Videoüberwachung auszuwerten (beispielsweise bei Verdacht des Vorliegens einer strafbaren Handlung), da der Auftraggeber selbst oftmals nicht zur Strafverfolgung berufen ist. Dies würde den Anwen-

[337] DSK 19.7.2013, K121.698/0004-DSB/2013.
[338] VwGH 29.10.2014, 2013/01/0127 mit Verweis auf ErlRV 472, BlGNR XXIV. GP, 21.
[339] *Löffler,* (K)Ein Auskunftsrecht bei (nicht ausgewerteten) Videoüberwachungen. Eine Besprechung von VwGH 29. 10. 2014, 2013/01/0127, jusIT 2015/27, 71.
[340] DSK 19.7.2013, K121.698/0004-DSB/2013.

dungsbereich des § 50e weitgehend reduzieren, könne jedoch nicht die Intention des Gesetzgebers bei der Modifikation des Auskunftsanspruchs nach § 26 gewesen sein. Es sei daher plausibel, dass der Auftraggeber bei Vorliegen eines (zulässigen) Auskunftsbegehrens ebenfalls zur Einsichtnahme und Auswertung der Videoüberwachung berechtigt sei, um die Auskunft vollständig erteilen zu können.[341] Die Art-29-Datenschutzgruppe hat festgehalten, dass eine Videoüberwachung erst dadurch rechtmäßig werde, dass der Betroffene Auskunft („Zugang") über eigene Daten erhält.[342]

Dem Wortlaut von § 4 Z 9 zufolge werden Daten ab der Ermittlung („Speicherung") verarbeitet und nicht erst ab deren Auswertung („Betrachtung") – dies führt dazu, dass alle Videodaten (ausgenommen Echtzeitüberwachungen) zu beauskunften wären (Auskunft über verarbeitete Daten zu Betroffenen, deren Identität bestimmbar ist). Grundsätzlich müssen Auftraggeber ihren gesamten Datenbestand auswerten, um sämtliche Daten aufzufinden, die zu dem Betroffenen verarbeitet werden – der VwGH ließ jedoch im vorliegenden Erkenntnis offen, warum dies im Falle einer Speicherung von Bild- bzw Videodaten (Videoaufzeichnungen sind technisch betrachtet eine Serie von Einzelbildern) anders sein sollte. Selbst wenn der Auftraggeber Kenntnis über die mittels Videoüberwachung aufgezeichneten Vorgänge hat (beispielsweise, weil Sicherheitspersonal vor Ort war), ist über diese Situation keine Auskunft zu erteilen, wenn die Bildmaterialien nicht ausgewertet wurden. Dies führt *Löffler* zufolge zu einer Privilegierung von Bilddaten gegenüber sonstigen Daten auf Kosten der Betroffenenrechte. Die Videoüberwachung an öffentlichen Orten dient unter anderem der Kriminalitätsbekämpfung – diese stellt in der Regel ein gegenüber dem Auskunftsanspruch des Einzelnen überwiegendes Interesse dar. Unter Verweis auf eine allgemeine Kriminalitätsbekämpfung müsste nicht einmal dann Auskunft erteilt werden, wenn das Videomaterial ausgewertet wurde – dem Gesetzgeber kann jedoch nicht unterstellt werden, dass dieser Bestimmungen ohne Anwendungsbereich schaffen wollte, sodass eine Auskunftserteilung nur ausnahmsweise zum Schutz überwiegender öffentlicher Interessen unterbleiben kann.[343]

§ 50b sieht vor, dass aufgezeichnete Daten aus der Videoüberwachung nach spätestens 72 Stunden zu löschen sind – sofern diese nicht zu Beweissicherungszwecken benötigt werden. Sollte die geplante Aufbewahrungsdauer 72 Stunden übersteigen, darf die DSB die Videoüberwachung nur registrieren, wenn dies aus besonderen Gründen erforderlich ist. Im Anlassfall[344] führte der Auftraggeber an, dass die Daten aus der Videoüberwachung lediglich für 48 Stunden dezentral in den einzelnen Fahrzeugen gespeichert und anschließend überschrieben

[341] *Gerhartl,* Kein Auskunftsrecht bei Videoüberwachung?, ecolex 2015, 1112-1114.
[342] Vgl Art-29-Datenschutzgruppe, WP 89, 7, 17, 23 und 24.
[343] *Löffler,* (K)Ein Auskunftsrecht bei (nicht ausgewerteten) Videoüberwachungen. Eine Besprechung von VwGH 29. 10. 2014, 2013/01/0127, jusIT 2015/27, 67-73.
[344] DSK 19.7.2013, K121.698/0004-DSB/2013.

werden – dementsprechend wird bei einem Auskunftsersuchen auf dem Postweg das Datenmaterial wohl regelmäßig bereits vernichtet sein, bevor das Auskunftsbegehren beim Auftraggeber eintrifft.

Zur Auskunftserteilung bei der Videoüberwachung wird vom Auskunftswerber eine Mitwirkung hinsichtlich der Eingrenzung des fraglichen Zeitraums eingefordert. Bei der Benennung von Anfangs- und Endpunkt können Abweichungen von einer halben Stunde bis einer Stunde als tolerierbar angesehen werden. Die Erteilung einer schriftlichen Auskunft wie in § 26 Abs 1 vorgesehen ist hier hinsichtlich der verarbeiteten Daten aus naheliegenden Gründen keine transparente Lösung. Daher besteht diesbezüglich grundsätzlich ein Anspruch auf Erhalt der Videoaufzeichnung, die übrigen Auskunftsbestandteile sind schriftlich zu erteilen. Freilich muss der Geheimhaltungsanspruch Dritter gewahrt bleiben. Erlauben diese die Übersendung der Aufzeichnung an den Betroffenen nicht, so muss auf die schriftliche Auskunftserteilung in Gestalt einer präzisen Beschreibung des verarbeiteten Verhaltens zurückgegriffen werden. Alternativ kann der Auftraggeber auch eine Kopie unter technischer Unkenntlichmachung der anderen Personen zur Verfügung stellen.[345] Um abschätzen zu können, ob durch die Auskunftserteilung in die Geheimhaltungsansprüche Dritter eingegriffen wird, muss der Auftraggeber *Gerhartl* zufolge jedoch berechtigt sein, die vorhandenen Daten auszuwerten – auf dieser Grundlage kann der Auftraggeber erst entscheiden, in welcher Form die Auskunft zu erteilen ist (Übersendung der Aufzeichnung, Möglichkeit der Einsichtnahme auf Lesegeräten des Auftraggebers oder schriftliche Beschreibung der Handlungsabfolge).[346]

Eine nahezu durchgehende Ablehnung der Auskunftserteilung bei Bild bzw Videodaten steht mE im Widerspruch zum ansonsten um Transparenz und Wahrung der Betroffenenrechte bemühten DSG. Dementsprechend wäre eine klarere Regelung des Auskunftsanspruchs bei Videoüberwachungen wünschenswert, da der Auftraggeber in anderen Bereichen (beispielsweise Briefverkehr, Kontobewegungen) zur vollständigen Auskunftserteilung verpflichtet ist – es scheint nicht nachvollziehbar, warum Videoüberwachungen anders behandelt werden sollen, zumal besondere Maßnahmen zum Schutz Dritter normiert wurden (etwa Auskunftserteilung durch Niederschrift der Geschehnisse).

4.14 Schema zur Auskunftserteilung

Zusammenfassend lässt sich damit an dieser Stelle festhalten, dass die bestehende Rechtslage (in Verbindung mit Kommentarliteratur, Spruchpraxis der DSB, Musterschreiben bzw Formularen) insgesamt gut geeignet ist, um die Rahmenbedingungen der Auskunftserteilung über

[345] ErlRV 472, BlGNR XXIV. GP, 20f.
[346] *Gerhartl,* Kein Auskunftsrecht bei Videoüberwachung?, ecolex 2015, 1112-1114.

personenbezogene Daten des Betroffenen darzustellen. Sowohl das Formular zum Auskunftsbegehren der DSB (siehe Anhang 1) als auch das von *Knyrim* empfohlene Musterschreiben zur Beantwortung des Auskunftsbegehrens (siehe Anhang 2) sind sinnvoll strukturiert und unterstützen den reibungslosen Ablauf. Es ist *Knyrim* beizupflichten, wenn er darauf hinweist, dass für Auftraggeber eine gewisse Systematik innerhalb der Organisation sicherlich wünschenswert und ökonomisch vorteilhaft ist, um Auskunftsbegehren rasch bearbeiten zu können[347]. *Haidinger* führt diesen Gedanken bezüglich der DS-GVO weiter und empfiehlt den Verantwortlichen, die Organisationsstruktur entsprechend der ab 2018 geltenden Gesetzeslage anzupassen und bereits vorab mit „friendly customers" hinsichtlich der Praxistauglichkeit zu testen.[348] Dies lässt sich schematisch darstellen (Rechtslage vor DS-GVO):

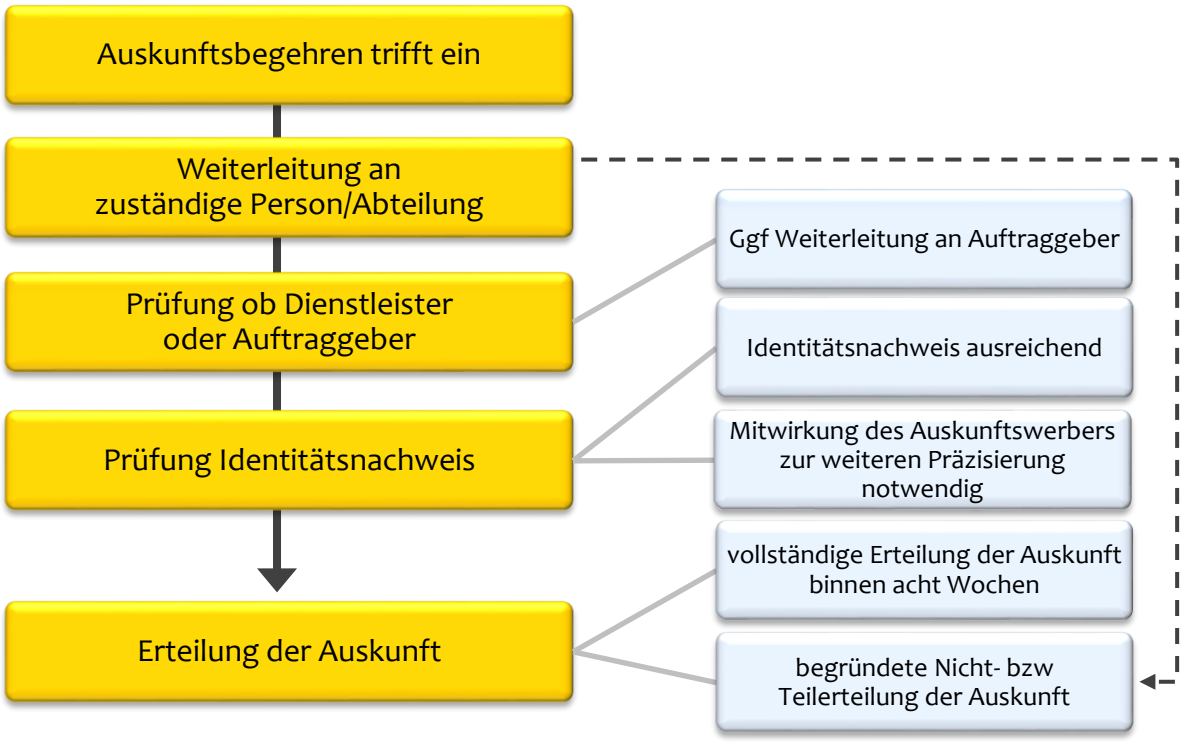

Abbildung 1: Schema zur Auskunftserteilung (erstellt von Joachim Galileo Fasching)

[347] *Knyrim*, Datenschutzrecht³, 326.
[348] *Haidinger*, Die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch (Art 15-21 DSGVO), in Knyrim (Hrsg.), DS-GVO, 125 und 135.

5 Rechtsschutz und Verwaltungsstrafrecht

In den vorangehenden Kapiteln wurde gezeigt, wie ein Auskunftsbegehren aufgebaut sein sollte und welche Inhalte vonseiten des Auftraggebers an den Betroffenen zu übermitteln sind. Obwohl die im Gesetz genannte Achtwochenfrist mE großzügig ist[349], kann es vorkommen, dass der Betroffene innerhalb dieser Frist keine oder keine vollständige Auskunft vom Auftraggeber erhält. Für die Durchsetzung des Auskunftsrechts (im privaten und öffentlichen Bereich) ist die monokratische Datenschutzbehörde nach den Verfahrensvorschriften des AVG zuständig. Im DSG sind das Kontroll- und Ombudsmannverfahren (§ 30 „Kontrollbefugnisse der DSB“), das (förmliche) Beschwerdeverfahren (§ 31 „Beschwerde an die DSB“), die datenschutzrechtliche Klage vor den Zivilgerichten (§ 32 „Anrufung der Gerichte“) sowie Verwaltungsstrafbestimmungen (§ 52) verankert. Im Rahmen dieser Diplomarbeit wurde ein persönliches Gespräch mit Dr. Matthias Schmidl (stellvertretender Leiter der Datenschutzbehörde) geführt, die Erkenntnisse daraus fließen ebenfalls in den folgenden Abschnitt ein.[350]

Für jede Verfahrenseinleitung kommt § 13 AVG zur Anwendung. Nach Abs 1 sind Anträge, Gesuche, Anzeigen, Beschwerden und sonstige Mitteilungen, sofern in den Verwaltungsvorschriften nicht anderes bestimmt ist, bei der Behörde schriftlich, mündlich oder telefonisch einzubringen. Schriftliche Anbringen können in jeder technisch möglichen Form übermittelt werden. Bei der DSB sollten alle Anbringen schriftlich oder mittels E-Mail (dsb@dsb.gv.at) gestellt werden (Internet www.dsb.gv.at). Rechtsmittel und Anbringen, die an eine Frist gebunden sind oder durch die der Lauf einer Frist bestimmt wird, sind schriftlich einzubringen. Mängel schriftlicher Anbringen ermächtigen die Behörde nicht zur Zurückweisung. Die Behörde hat vielmehr von Amts wegen unverzüglich deren Behebung zu veranlassen und kann dem Einschreiter die Behebung des Mangels mit der Wirkung auftragen, dass das Anbringen nach fruchtlosem Ablauf einer gleichzeitig zu bestimmenden, angemessenen Frist zurückgewiesen wird. Wird der Mangel rechtzeitig behoben, so gilt das Anbringen als ursprünglich richtig eingebracht. Zur Entgegennahme mündlicher oder telefonischer Anbringen ist die Behörde, außer bei Gefahr im Verzug, nur während der für den Parteienverkehr bestimmten Zeit, zur Entgegennahme schriftlicher Anbringen nur während der Amtsstunden verpflichtet. Die Amtsstunden und die für den Parteienverkehr bestimmte Zeit sind bei der Behörde im Internet oder durch Anschlag kundzumachen. Bei Anbringen, die außerhalb der Amtsstunden bei der Behörde eingebracht werden, beginnen die behördlichen Entscheidungsfristen erst mit dem Wiederbeginn der

---

[349] Die verpflichtende Auskunftserteilung binnen vier Wochen – wie im § 25 Abs 1 DSG 1978 idF BGBl Nr. 565/1978 normiert – wäre mE eine ausreichende Frist, sofern der Auftraggeber nicht die Mitwirkungsobliegenheit des Betroffen beansprucht. Vgl *Jahnel,* Datenschutzrecht, 262 (dieser stellt auf die automationsunterstützte Datenabfrage ab, welche rasch die gewünschte Auskunft liefern sollte und verweist auf Art 12 lit a RL 95/46/EG, in welchem die Auskunft „ohne unzumutbare Verzögerung“ zu erteilen ist) und *Duschanek,* ZfV 2000, 526(534).

[350] *Schmidl,* Das datenschutzrechtliche Recht auf Auskunft – ein Überblick, ZIIR 2014, 21-26.

Amtsstunden zu laufen. Die Behörde ist nicht verpflichtet, Anbringen, die sich auf keine bestimmte Angelegenheit beziehen, in Verhandlung zu nehmen. Anbringen können schließlich in jeder Lage des Verfahrens zurückgezogen werden. Außerdem kann der verfahrenseinleitende Antrag in jeder Lage des Verfahrens geändert werden. Durch die Antragsänderung darf die Sache ihrem Wesen nach nicht geändert und die sachliche oder örtliche Zuständigkeit nicht berührt werden.[351]

Die Verfahren vor der DSB können jeden Auftraggeber des privaten und öffentlichen Bereichs treffen – von der Zuständigkeit sind jedoch die Gesetzgebung (insb der Nationalrat und die Landtage mit ihren jeweiligen Unterorganen wie Ausschüssen, Rechnungshöfen oder Ombudsstellen) und die Gerichtsbarkeit ausgenommen. Die DSB thematisiert hierbei ein Verfahrensproblem: ihre Zuständigkeit für ganz Österreich. Da der gesetzliche Grundsatz der Sparsamkeit (§ 39 Abs 2 AVG) gilt, werden Ermittlungen außerhalb eines Radius von ca 50 Kilometern rund um Wien meistens durch ersuchte Behörden im Amtshilfeweg durchgeführt. Damit gewinnt die DSB allerdings keinen unmittelbaren Eindruck zB von technischen Systemen, Orten und Personen.[352] Die DSB kann selbst keine Strafen verhängen, jedoch eine (Verwaltungs-)Strafanzeige erheben, welche gemäß § 52 Abs 5 DSG durch die Bezirksverwaltungsbehörde im Sprengel des Auftraggebers zu entscheiden ist – sollte der Auftraggeber keinen Sitz in Österreich haben, so ist die BVB am Sitz der DSB zuständig.[353]

Die DSB ist insb für die Behandlung von Eingaben von Personen zuständig, die eine Verletzung in ihren Datenschutzrechten (Auskunft, Richtigstellung, Löschung, Geheimhaltung) geltend machen.[354] Die Tätigkeitsbereiche der DSB umfassen ua Individualbeschwerden, KOV, Rechtsauskünfte, Genehmigungen, Verfahren vor BVwG sowie Auskünfte Schengen. Wie in untenstehender Abbildung (Auszug aus dem Datenschutzbericht 2015) ersichtlich, wurden im Jahr 2015 insgesamt 147 Individualbeschwerden eingebracht, diese umfassen das KOV (§ 30) und das Beschwerdeverfahren (§ 31). 2015 wurden 147 Anliegen bearbeitet (95 Bescheide und 52 Einstellungen).[355]

[351] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/112 in § 30 Anm 5.
[352] DSB Newsletter 2/2015, 2.
[353] Vgl *Dohr/Pollirer/Weiss/Knyrim*, DSG², 402 in § 52 Anm 19.
[354] *DSB*, Datenschutzbericht 2015, 6.
[355] *DSB*, Datenschutzbericht 2015, 8.

Art der Tätigkeit	Eingangsstücke			Erledigungen		
	2013	2014	2015	2013	2014	2015
Individualbeschwerden	224	224	147	107	220	147
Erledigungsart der Individualbeschwerden	224	224	147	73 Bescheide 34 Einstellungen	117 Bescheide 103 Einstellungen	95 Bescheide 52 Einstellungen
Kontroll- Ombudsmannverfahren nach § 30 DSG 2000 (Verfahren über Antrag)	309	399	332	326	400	357
Kontroll- Ombudsmannverfahren nach § 30 DSG 2000 (amtswegiges Prüfverfahren)	79	98	67	80	88	97
Rechtsauskünfte	1133	2261	2152	1133	2261	2123

Abbildung 2: Datenschutzbericht 2015 der DSB[356]

Gemäß § 37 Abs 6 sind Entscheidungen der DSB von grundsätzlicher Bedeutung für die Allgemeinheit von der DSB unter Beachtung der Erfordernisse der Amtsverschwiegenheit in geeigneter Weise zu veröffentlichen. Die DSB publiziert diese unter anderem im Rechtsinformationssystem des Bundes (RIS)[357], im vierteljährlich erscheinenden Newsletter[358] sowie basierend auf § 37 Abs 5 DSG im nunmehr jährlich erscheinenden Datenschutzbericht[359]. Dabei sind die Erfordernisse der Amtsverschwiegenheit zu berücksichtigen, das bedeutet, dass Namen und Firmen, Rechtsformen und Produktbezeichnungen, Adressen (inkl. URLs, IP- und E-Mail-Adressen), Aktenzahlen (und dergleichen), etc., sowie deren Initialen und Abkürzungen aus Pseudonymisierungsgründen abgekürzt und/oder verändert sein können. Die DSB hat auf einer früheren Version ihrer Webseite einige nützliche Tipps rund um Rechtsschutz bei Datenschutzverletzungen veröffentlicht.[360]

§ 34 Abs 1 DSG sieht für die Behandlung einer Eingabe nach § 30, einer Beschwerde nach § 31 oder einer Klage nach § 32 eine subjektive Verjährungsfrist von einem Jahr ab Kenntnis

[356] *DSB*, Datenschutzbericht 2015, 9.
[357] Abrufbar unter https://www.ris.bka.gv.at/Dsk/.
[358] Abrufbar unter https://www.dsb.gv.at/web/datenschutzbehorde/newsletter.
[359] Abrufbar unter https://www.dsb.gv.at/dokumente.
[360] Abrufbar unter http://web.archive.org/web/20160406141343/http://www.dsb.gv.at/site/6189/default.aspx.

von einem beschwerenden Ereignis sowie eine objektive Frist von drei Jahren, nachdem das Ereignis behauptetermaßen stattgefunden hat, vor. § 34 Abs 1 spricht von der Kenntnis eines „beschwerenden Ereignis“ als Auslöser der Präklusionsfrist. Damit kann im Fall der Nichtreaktion auf das Begehren (Unterlassung) eines Auskunfts- oder Löschungswerbers nur das Versäumen der achtwöchigen Frist des § 26 Abs 4 oder des § 27 Abs 4 gemeint sein, im Fall der Reaktion (Ablehnung, Negativauskunft, inhaltliche Auskunft, Löschungsbestätigung) jedoch der Zugang der behauptet rechtswidrigen Äußerung des datenschutzrechtlichen Auftraggebers[361].

Die Anwendungserfahrung, insb vor der DSK, hat ergeben, dass die Statuierung von Verjährungsfristen (Abs 1) für die Geltendmachung der Interessen der Betroffenen nach dem DSG sachlich geboten ist: Die Ermittlung von Sachverhalten, die lange zurückliegen, stößt erfahrungsgemäß auf erhebliche Schwierigkeiten und verhindert eine verlässliche Beurteilung des Vorliegens von Datenschutzverletzungen. Auch im eigenen Interesse sollten die Betroffenen daher dazu angehalten werden, behauptete Datenschutzverletzungen möglichst frühzeitig bei der DSB oder bei Gericht anhängig zu machen.[362] Auf Präklusionsfristen muss von Amts wegen, also bei feststehendem Sachverhalt, ohne Einwendung Bedacht genommen werden; die Verjährung dagegen muss mittels Einrede geltend gemacht werden.[363]

5.1 Kontroll- und Ombudsmannverfahren nach § 30 DSG

Bei dem KOV nach § 30 DSG handelt es sich um ein formfreies Verfahren auf Grundlage des Art 28 Abs 4 DSRL, das mediativen Charakter (soft law) hat. Die DSB bezeichnet das KOV als „Allrounder“ (es sind alle datenschutzrechtlich relevanten Sachverhalte einer Prüfung im Rahmen des KOV zugänglich[364]) unter den Werkzeugen zur Durchsetzung des Rechts auf Datenschutz, da damit auch die Verletzung von Pflichten durch den Auftraggeber geltend gemacht werden können. Das Verfahren endet mit einer Empfehlung an den Auftraggeber (beispielsweise Verstärkung der Datensicherheitsmaßnahmen) oder mit einer bloßen Mitteilung an die Beteiligten, dass keine Rechts- oder Pflichtenverletzung vorliegt.[365] Die DSB hat dabei für die Befolgung der Empfehlung eine angemessene Frist zu setzen – wird dieser Empfehlung innerhalb der gesetzten Frist nicht entsprochen, so kann die DSB je nach Art des Verstoßes von Amts wegen weitere Maßnahmen setzen.[366] Dieser Verfahrenstyp ist auch dann zulässig, wenn die DSB alternativ zur förmlichen Rechtsdurchsetzung (Beschwerdeverfahren nach § 31 DSG) zuständig wäre – und zwar unabhängig vom geltend gemachten Recht (Pflicht) bzw dem

[361] DSK 15.4.2011, K121.673/0008-DSK/2011; DSK 15.4.2011, K121.674/0008-DSK/2011.
[362] ErlRV 1613 BlgNR XX. GP, 50.
[363] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 247-250 in § 34 Anm 2 und 3.
[364] *Jahnel*, Datenschutzrecht, 512 in 9/29.
[365] DSB Newsletter 2/2015, 1f.
[366] Ausführlicher zu Empfehlungen und deren Durchsetzung *Jahnel*, Datenschutzrecht, 516-519 in 9/35-9/38.

angesprochenen Auftraggeber. Das Verfahren wird auf Antrag eines Betroffenen oder von Amts wegen eingeleitet. Vorrangiges Ziel ist dabei die Herstellung des rechtmäßigen Zustandes ohne Anrufung der Gerichte – gegebenenfalls wird eine Empfehlung der DSB ausgesprochen und veröffentlicht. Ein Bescheid kann – mit Ausnahme von Mandatsbescheiden nach § 30 Abs 6a – in diesem Verfahren nicht erlassen werden.[367] Nach § 30 Abs 6a kann die DSB eine Datenanwendung bei „Gefahr im Verzug" mit Mandatsbescheid (abgekürztes Verfahren!) gem § 57 Abs 1 AVG untersagen. Dagegen kann binnen zwei Wochen bei der DSB das Rechtsmittel der Vorstellung erhoben werden, dem allerdings keine aufschiebende Wirkung zukommt. Dieses Rechtsmittel ist nicht aufsteigend und es hat die DSB binnen zwei Wochen das Ermittlungsverfahren einzuleiten, ansonsten tritt der Mandatsbescheid außer Kraft. Andernfalls steht gegen den die Vorstellung erledigenden Bescheid die Beschwerde an das BVwG zu.[368]

Die DSB kann auf Grundlage einer (anonymen) Eingabe oder von Amts wegen tätig werden. Auch ein Einschreiten auf Ersuchen anderer Ämter (zB des Arbeitsinspektorats bei Videoüberwachung am Arbeitsplatz) kommt immer wieder vor. Im privaten Bereich macht das KOV lediglich dann Sinn, wenn die Verfahrensbeteiligten bereit sind, die Schlichtung durch die DSB zu akzeptieren – andernfalls weist die DSB mit Nachdruck auf die Möglichkeit der gerichtlichen Klage nach § 32 DSG 2000 hin.[369] Die Konsequenzen der Nichtbefolgung einer Empfehlung der Kontrollstelle sind in Abs 4 (nunmehr Abs 6) näher geregelt.[370] Anlässlich jeder zulässigen Eingabe nach § 30 Abs 1 bzw jedes begründeten Verdachts hat die Datenschutzkommission nunmehr den Registerstand zu überprüfen, entspricht dieser nicht dem Gesetz, sind Maßnahmen nach den §§ 22 und 22a zu ergreifen. Somit führt das Verfahren nach § 30 im Fall eines Verdachts der Nichterfüllung der Meldepflicht zu den §§ 22 und 22a. Der Ausspruch einer Empfehlung scheint in diesen Fällen wenig zweckmäßig und entfällt daher künftig. Eine Empfehlung ist weiters nicht mehr erforderlich, wenn die Datenanwendung schon wegen „Gefahr im Verzug" untersagt worden ist.[371]

Der § 30 normiert keinen Anspruch auf eine bescheidmäßige Erledigung des Anbringens. Die Ausübung des Aufsichtsrechts durch die Behörde kann zwar angeregt, aber nicht erzwungen werden.[372] Dieser weniger formstrenge Verfahrenstyp ist vom Gesetzgeber für allgemeine Rügen (beispielsweise behauptete Pflichtenverletzung durch den Auftraggeber) und inhaltlich weniger bestimmte „Beschwerden" vorgesehen worden.[373] Eine Einschau beim Auftraggeber

[367] *DSB,* Datenschutzbericht 2015, 18.
[368] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/118e(210/118f) in § 30 Anm zu E7.
[369] DSB Newsletter 2/2015, 2.
[370] ErlRV 1613 BlgNR XX. GP, 49.
[371] ErlRV 472, BlGNR XXIV. GP, 12.
[372] DSK 18.5.2004, K211.496/0003-DSK/2004.
[373] DSK 26.2.2002, K120.783/004-DSK/2002 und DSK 11.10.2002, K120.814/008-DSK/2002.

(Dienstleister) darf grundsätzlich nur innerhalb der Betriebszeiten vorgenommen werden, um der Verpflichtung zur möglichsten Schonung zu entsprechen.[374] In der Praxis beauftragt die DSB mit dieser Einschau Dritte, etwa Universitätsinstitute für Informatik.[375]

Ungeachtet des in § 30 Abs 1 verwendeten Begriffs „jedermann" muss es sich um einen Betroffenen im Sinne des § 4 Z 3 handeln.[376] Der Einschreiter muss eine ihn betreffende Rechts- oder Pflichtenverletzung eines Auftraggebers behaupten. Die DSB ist gemäß § 30 Abs 7 verpflichtet, den Einschreiter, der die Ausübung dieser Befugnisse durch seine Eingabe angeregt hat, darüber zu informieren, wie mit seiner Eingabe verfahren wurde (dh bspw, ob die DSB überhaupt nähere Ermittlungen durchgeführt hat oder durchführen wird oder die in § 30 Abs 6 vorgesehenen Maßnahmen zur Anwendung bringen wird).[377]

Die DSB stellt auf ihrer Webseite[378] ein Formular zur Verfügung, mit dem eine Rechts- bzw Pflichtenverletzung durch einen Auftraggeber im privaten oder öffentlichen Bereich vorgebracht werden kann. Als Beispiele für eine Rechtsverletzung werden Verletzung des Rechts auf Geheimhaltung, Verletzung des Anspruchs auf Richtigstellung, Löschung oder Auskunft oder Nichtbeachtung des Widerspruchs gegen Datenverwendung genannt. In den Bereich der Pflichtenverletzung fallen beispielsweise Führung der DVR-Nummer, Offenlegung seiner Identität, Meldepflicht beim DVR, Offenlegung nicht-meldepflichtiger Datenanwendungen, Teilnehmen an oder Betreiben eines Informationsverbundsystems ohne Vorabkontrolle durch die DSB, Betreiben einer Datenanwendung mit sensiblen oder strafrechtlich relevanten Daten oder einer Datenanwendung zur Auskunftserteilung über Kreditwürdigkeit ohne Vorabkontrolle durch die DSB, Verstoß gegen Informationspflicht bei Datenermittlung oder keine ausreichenden Datensicherheitsmaßnahmen.

Aus dem Datenschutzbericht 2014 geht hervor, dass – wie auch in den Jahren zuvor – der zahlenmäßig größte Anwendungsbereich des KOV die Videoüberwachung war. Als Fälle werden besonders erwähnt: Empfehlung betreffend die Meldung an den Jugendwohlfahrtsträger aufgrund des Verdachts auf Vernachlässigung, Misshandlung, Quälen oder sexuellen Missbrauch (nur bei einem hinreichend konkreten Verdacht dürfen personenbezogene Daten auf Basis des § 54 ÄrtzeG übermittelt werden)[379], Empfehlung betreffend die Verwendung der So-

---

[374] ErlRV 1613 BlgNR XX. GP, 49.
[375] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/113 in § 30 Anm 13. Ausführlicher zum Einschauverfahren *Jahnel*, Datenschutzrecht, 514f in 9/32-9/34.
[376] AB 2028 der Beilagen XX. GP, 3 zu § 30.
[377] DSK 25.6.2004, K120.877/0017-DSK/2004.
[378] https://www.dsb.gv.at/at.gv.bka.liferay-app/documents/22758/115215/Druckformular_Ombudsmanneingabe_07-2016.pdf/9260b511-52b5-4bc7-bfc2-e2faa3c2ec44, abgerufen am 02. September 2016.
[379] DSB 29.1.2014, DSB-K215.309/0001-DSB/2014.

zialversicherungsnummer zur Erstellung eines Benutzer-Accounts (der Nachweis der „Echtheit“ einer Person wäre auch mit der Ärzteausweisnummer bzw der Bürgerkarte möglich)[380] sowie Empfehlung zur Verwendung von Wählerdaten aus dem Wählerverzeichnis hinsichtlich einer vom Bürgermeister selbst finanzierten Befragung der Gemeindebürger zum geplanten Flüchtlings- und Asylwerberheim (die Verwendung personenbezogener Daten durch ein Organ der Gebietskörperschaft bedarf einer gesetzlichen Grundlage)[381].

Im Datenschutzbericht 2015 werden folgende Fälle hervorgehoben: Empfehlung zur Durchführung einer Befragung über arbeitsbedingte psychische Belastungen mit anschließender Auswertung (die Befragungsergebnisse ließen Rückschlüsse auf einzelne Mitarbeiter zu)[382], Empfehlung zur unzulässigen Übermittlung einer Hausverbotsliste (der Fanordner wurde via Geste auf einen auffälligen Fußballfan hingewiesen)[383] sowie Empfehlung wegen Änderung der Rechtsform samt Namen und Wegfall des Zwecks und Rechtsgrundlage der Datenanwendung (im DVR waren fehlerhafte bzw gesetzwidrige Informationen über das Unternehmen gespeichert)[384]. Zudem ist auch ein Mandatsbescheid zur Videoüberwachung ergangen, in welchem festgehalten wurde, dass „eine Videoüberwachung hinsichtlich allgemein zugänglicher Flächen in einem Mehrparteienwohnhaus etwa zur Abschreckung von Einbrechern (Schutzzweck) oder zur Identifizierung eines Sachbeschädigers (Beweissicherungszweck) zulässig sei, nicht jedoch, um mit Hilfe der Videoüberwachung Beweise für eine vertragswidrige Nutzung des Mietgegenstandes (zB Nichtgebrauch, unerlaubte Untervermietung) zu sammeln oder ganz allgemein Daten zum Privatleben der Mieter zu erheben“.[385]

Im Jahr 2016 sind einige weitere Empfehlungen durch die DSB ausgesprochen worden, unter anderem zum Umgang mit sensiblen personenbezogenen Daten, zur effektiven Zugangskontrolle bei Patientendaten, Einschränkung einer Videoüberwachung auf Echtzeitüberwachung, deutlichere Kennzeichnung einer Videoüberwachung, zur Speicherung von Nutzerprofilen ehemaliger Bediensteter sowie zur Speicherung von Fotos und Personalien bei Baustellenkontrollen (Aufdeckung von Schwarzarbeit und illegaler Gewerbeausübung).

---

[380] DSB 23.5.2014, DSB-D213.131/0002-DSB/2014. Vgl die DSB-Empfehlung vom 19.7.2013, DSB-K210.741/0016-DSK/2013, wonach die Sozialversicherungsnummer nicht als „genereller Identifikator“ verwendet werden dürfe.

[381] DSB 28.11.2014, DSB-D215.548/0007-DSB/2014.

[382] DSB 30.3.2015, DSB-D215.611/0003-DSB/2014.

[383] DSB 1.4.2015, DSB-D215.529/0002-DSB/2015.

[384] DSB 1.7.2015, DSB-D215.814/0003-DSB/2015.

[385] *DSB*, Datenschutzbericht 2015, 18 mit Verweis auf DSB 22.8.2014, DSB-D215.463/0006-DSB/2014. Der Mandatsbescheid wurde nach einem Rechtsmittel der Auftraggeber der (unzulässigen) Videoüberwachung aufgehoben, da sich herausgestellt hatte, dass die Anlage inzwischen bereits entfernt worden war.

5.2 Beschwerdeverfahren nach § 31 DSG

Eine Beschwerde kann gemäß § 31 Abs 1 bei der DSB erhoben werden, wenn man in seinem Recht auf Auskunft (§ 26 oder § 50 Abs 1 dritter Satz) oder auf Darlegung einer automatisierten Einzelentscheidung (§ 49 Abs 3) verletzt wurde. Dabei darf es sich jedoch nicht um Verwendung von Daten für Akte im Dienste der Gesetzgebung oder der Gerichtsbarkeit handeln.[386] Sofern der Anspruch nicht nach § 32 Abs 1 vor einem Gericht geltend zu machen ist oder sich gegen ein Organ im Dienste der Gesetzgebung oder der Gerichtsbarkeit richtet, können gemäß § 31 Abs 2 auch Verletzungen im Recht auf Geheimhaltung (§ 1 Abs 1) bzw Richtigstellung oder Löschung (§§ 27 und 28) vor der DSB geltend gemacht werden. Jedermann, der Betroffener iSd § 4 Z 3 ist, darf dabei als Beschwerdeführer auftreten.[387] In einem Beschwerdeverfahren machte der Beschwerdegegner (BMI) geltend, dass das Auskunftsverlangen Tätigkeiten des BMI/BIA betreffe, die der Gerichtsbarkeit zuzuordnen seien und daher der Beurteilung durch die DSB entzogen seien. Ein Auskunftsbegehren an das BMI ist jedoch ein solches an ein Verwaltungsorgan und unterliegt daher auch der Prüfungskompetenz der DSB.[388]

Eine „Popularklage“ (Klage, die von jemandem erhoben wird, der nicht allein davon betroffen ist) vor der DSB ist nach geltender Rechtslage nicht zulässig und ihre Behandlung daher nicht möglich, da Rechtsverletzungen behauptende Anbringen an die DSB – sowohl die weniger formellen Eingaben gemäß § 30 Abs 1 als auch die formellen Beschwerden nach § 31 Abs 1 und 2 – nur von Personen gemacht werden können, die behaupten, in ihrer Rechtssphäre von den Handlungen eines datenschutzrechtlichen Auftraggebers betroffen zu sein.[389]

Durch die DSG-Novelle 2010 wurde der Begriff „Auftraggeber“ aus § 31 Abs 1 und 2 gestrichen (ob jemandem diese Rolle zukommt, wird oft erst im Verfahren entschieden) – damit ist klar, dass auch gegen Dienstleister zur Durchsetzung des § 26 Abs 10 vorgegangen werden kann.[390]

Die Datenschutzbehörde empfiehlt auf ihrer Webseite[391] die Verwendung eines Formulars, um eine Verletzung des § 31 DSG geltend zu machen; dieses Formular ist im Anhang 4 abgebildet. Die Beschwerde hat dabei gemäß § 31 Abs 3 zu enthalten:

1. die Bezeichnung des als verletzt erachteten Rechts,
2. soweit dies zumutbar ist, die Bezeichnung des Rechtsträgers oder Organs, dem die behauptete Rechtsverletzung zugerechnet wird (Beschwerdegegner),

---

[386] Vgl DSK 10.7.2009, K121.535/0004-DSK/2009.
[387] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/124 in § 31 Anm 3.
[388] DSK 28.6.2006, K121.075/0013-DSK/2006.
[389] DSK 30.3.2012, K121.765/0008-DSK/2012; DSK 9.8.2013, K121.933/0029-DSK/2013.
[390] ErlRV 472, BlGNR XXIV. GP, 12f.
[391] http://www.dsb.gv.at/DocView.axd?CobId=30482, abgerufen am 09. August 2016.

3. den Sachverhalt, aus dem die Rechtsverletzung abgeleitet wird,
4. die Gründe, auf die sich die Behauptung der Rechtswidrigkeit stützt,
5. das Begehren, die behauptete Rechtsverletzung festzustellen und
6. die Angaben, die erforderlich sind, um zu beurteilen, ob die Beschwerde rechtzeitig eingebracht ist.

Wie aus § 31 Abs 3 Z 2 hervorgeht, ist die Anführung des korrekten Beschwerdegegners nicht zwingend notwendig.[392] Damit wird der Tatsache Rechnung getragen, dass es häufig schwierig ist, den datenschutzrechtlich verantwortlichen Auftraggeber zu benennen. Eine DSB-Beschwerde darf nicht zurückgewiesen werden, wenn zwar die bekämpfte Datenverwendung eindeutig bestimmt, der dafür verantwortliche Auftraggeber aber nicht ausdrücklich angeführt wird. In diesen Fällen hat die DSB den Auftraggeber amtswegig zu bestimmen.[393] Einem unvertretenen Beschwerdeführer ist es nicht zumutbar, die Vorschriften des § 31 Abs 3 vollständig einzuhalten, es genügt daher, wenn die Beschwerde die Begriffe „Verdacht Datenschutzverletzung“ und „persönliche Daten“ beinhaltet – allfällige zusätzliche erforderliche Informationen hat die DSB im Rahmen der Manuduktionspflicht des § 13 Abs 3 AVG einzuholen.[394]

§ 31 Abs 4 zufolge sind einer Beschwerde nach Abs 1 außerdem das zu Grunde liegende Auskunftsverlangen (der Antrag auf Darlegung oder Bekanntgabe) und eine allfällige Antwort des Beschwerdegegners anzuschließen (Korrespondenz mit dem Auftraggeber). Einer Beschwerde nach Abs 2 sind außerdem der zu Grunde liegende Antrag auf Richtigstellung oder Löschung und eine allfällige Antwort des Beschwerdegegners anzuschließen. Auskunfts- bzw Löschungsverlangen müssen ohnehin stets vorliegen, um die entsprechenden Rechte erfolgreich geltend machen zu können[395].

Zur fristgerechten Einbringung der Beschwerde ist § 34 DSG[396] zu beachten, daher sind die Anbringen gemäß § 13 Abs 1 AVG schriftlich zu erheben. Die Eingabe des Betroffenen ist dabei kostenfrei nach § 53 Abs 1 DSG, jedoch kann die DSB gemäß § 35 AVG gegen Personen, die offenbar mutwillig die Tätigkeit der Behörde in Anspruch nehmen oder in der Absicht einer Verschleppung der Angelegenheit unrichtige Angaben machen, eine Mutwillensstrafe bis zu 726 Euro verhängen. Ebenso gilt es, die in § 31 Abs 3 genannten Minimalkriterien anzuführen, denn wenn diese fehlen, kann nach § 13 Abs 3 AVG vorgegangen werden. Eine Behandlung von Anbringen, die Abs 3 und 4 nicht genügen, kann allenfalls im Verfahren nach § 30 erfolgen. Die Intention dahinter ist, dass es der DSB damit möglich ist, Beschwerden, die nicht

[392] Vgl DSK 11.3.2005, K120.991/0006-DSK/2005.
[393] *Ennöckl,* Die DSG-Novelle 2010, ÖJZ 2010/35, 293 (295).
[394] DSK 20.7.2011, K121.704/0011-DSK/2011.
[395] VwGH 6.6.2007, 2001/12/0004 = VwSlg 17215 A/2007.
[396] Siehe Begriff Verjährungsfrist, 67.

einmal die genannten Minimalanforderungen aufweisen, nicht inhaltlich behandeln zu müssen.[397] Im Verfahren vor der DSB kommt mangels einer bestehenden Anspruchsnorm im Sinne von § 74 Abs 2 AVG keinem Beteiligten, weder dem Beschwerdeführer noch den Beschwerdegegnern, ein Anspruch auf Kostenersatz zu.[398]

Gemäß § 13 Abs 3 AVG ermächtigen Mängel schriftlicher Anbringen die Behörde nicht zur sofortigen Zurückweisung. Die Behörde hat vielmehr von Amts wegen unverzüglich deren Behebung zu veranlassen und kann dem Einschreiter die Behebung des Mangels mit der Wirkung auftragen, dass das Anbringen nach fruchtlosem Ablauf einer gleichzeitig zu bestimmenden, angemessenen Frist zurückgewiesen wird. Wird der Mangel rechtzeitig behoben, so gilt das Anbringen als ursprünglich richtig eingebracht. Ein Auskunftsbegehren nach § 26 DSG ist notwendige Voraussetzung für das Entstehen einer datenschutzrechtlichen Auskunftspflicht des Auftraggebers und gerade die in der Beschwerde vorzunehmende Konkretisierung, worin die Unrichtigkeit der erteilten Auskunft bestehen soll, sind für die Behandlung einer Beschwerde wegen einer behaupteten Verletzung im Recht auf (richtige) Auskunft wesentlich. Da die Beschwerde im vorliegenden Fall in Bezug auf die behauptete Verletzung im Recht auf Auskunft somit zur Behandlung nicht geeignet war, war die Beschwerde zurückzuweisen.[399] Eine verfrühte Einleitung des Beschwerdeverfahrens schadet nicht[400], jedoch kann die behauptete Verletzung im Recht auf Auskunft erst nach Ablauf der Frist von acht Wochen festgestellt werden.[401]

Grundsätzlich hat die DSB unter Bedachtnahme auf allfällige konkrete Verwaltungsvorschriften von Amts wegen (Offizialmaxime) vorzugehen und im Rahmen des AVG (Erforschung der materiellen Wahrheit bei freier Beweiswürdigung und Unbeschränktheit der Beweismittel sowie der Mittelbarkeit des Verfahrens) den Gang des Ermittlungsverfahrens zu bestimmen. Dabei hat sich die Behörde bei allen Verfahrensanordnungen von Rücksichten auf möglichste Zweckmäßigkeit, Raschheit, Einfachheit und Kostenersparnis leiten zu lassen. Nachdem durch den verfahrenseinleitenden Antrag (es besteht nach dem AVG keine Anwaltspflicht) die Verwaltungssache, also der Prozessgegenstand, allenfalls nach einem Verbesserungsverfahren, festgesetzt wurde, hat die DSB im Rahmen des Ermittlungsverfahrens (§ 37 AVG) den für die Erledigung der Verwaltungssache maßgebenden Sachverhalt festzustellen und den Parteien (Recht auf Gehör und auf Akteneinsicht) Gelegenheit zur Geltendmachung ihrer Rechte und rechtlichen Interessen zu geben. Nach einer Antragsänderung hat die Behörde das Ermittlungsverfahren nur insoweit zu ergänzen, als dies im Hinblick auf seinen Zweck notwendig

[397] ErlRV 472, BlGNR XXIV. GP, 13.
[398] DSK 16.5.2008, K121.353/0008-DSK/2008; ebenso DSK 20.1.2010, K120.939/0003-DSK/2010.
[399] DSK 16.12.2009, K121.565/0006-DSK/2009; DSK 20.1.2010, K121.575/0002-DSK/2010.
[400] DSB 16.7.2015, DSB-D122.349/0004-DSB/2015.
[401] DSK 24.2.2010, K121.573/0003-DSK/2010.

ist. Wenn die Sache zur Entscheidung reif ist, kann die Behörde das Ermittlungsverfahren für geschlossen erklären (§ 39 Abs 1 bis 3 AVG).[402]

Der Auskunftsanspruch kann ohne nähere Begründung durch den Auskunftswerber geltend gemacht werden, ebenso ist im § 31 Abs 3 keine explizite Begründung, warum man den Auskunftsanspruch durchsetzen möchte, gefordert. In einem Praxisfall wurde ich von der DSB aufgefordert, meine Hintergründe für das Auskunftsbegehren offenzulegen („Machen Sie bitte Angaben, ob der Hintergrund des Auskunftsverlangens bzw Ihrer Beschwerde z.B. in einem Mißbrauchsverdacht durch Dritte, Mehrfachabbuchungen oder Ähnlichem liegt."). Die Beantwortung dieser Frage war Gegenstand eines Mangelbehebungsauftrags – und damit war ich zur Antwort verpflichtet, wenn ich das Beschwerdeverfahren vor der DSB reibungslos fortführen wollte. Diese Form der Begründungspflicht gegenüber dem Auftraggeber oder der DSB stellt mE eine unzulässige Einschränkung des Auskunftsanspruchs dar.

Die DSG-Novelle 2010 hat eine Klarstellung in § 31 Abs 5 bewirkt, die der bisher geübten Praxis entspricht: Die der DSB durch § 30 Abs 2 bis 4 eingeräumten Kontrollbefugnisse kommen ihr auch in Beschwerdeverfahren nach § 31 Abs 1 und 2 gegenüber dem Beschwerdegegner zu. Ebenso besteht auch hinsichtlich dieser Verfahren die Verschwiegenheitspflicht nach § 30 Abs 5. § 31 Abs 6 sieht aus Gründen der Verfahrensökonomie vor, dass ein Kontrollverfahren nach § 30 Abs 1 nicht parallel zu einem Beschwerdeverfahren über denselben Gegenstand geführt werden soll. Freilich können über den Beschwerdegegenstand hinausgehende Verdachtsmomente (insb im Hinblick auf Verpflichtungen, die nicht mit subjektiven Betroffenenrechten korrespondieren) von der DSB nach § 30 weiterverfolgt werden.[403]

Die Vollzugspraxis hat zahlreiche Probleme bei der Auslegung der bisherigen spärlichen Regelungen des § 31 Abs 1 und 2 gezeigt. Zunächst war lange nicht klar, welchen Charakter die Bescheide der DSB haben[404]. Durch Rsp des VwGH ist dies nunmehr weitgehend klargestellt[405]. An dieser orientiert sich § 31 Abs 7: demnach ist eine Rechtsverletzung jedenfalls festzustellen. Nur bei Auftraggebern des privaten Bereichs ist darüber hinaus ein – vollstreckbarer – Leistungsauftrag zu erteilen, der so zu formulieren ist, dass die festgestellte Rechtsverletzung beseitigt wird. Der Leistungsauftrag ist je nach dem Beschwerdebegehren bzw den die Feststellung der Rechtswidrigkeit tragenden Gründen im Einzelfall zu formulieren. Es wird sich im Regelfall nicht auf ein konkret verarbeitetes Datum beziehen, weil die DSB die Rechtmäßigkeit der Auskunftserteilung nur ex post prüft und sie nicht an Stelle des Auftraggebers Auskunft zu erteilen hat. Somit wird der Leistungsauftrag in der Regel allgemeiner formuliert

---

[402] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/125 in § 31 Anm 16.
[403] ErlRV 472, BlGNR XXIV. GP, 13.
[404] Ausführlicher dazu *Jahnel*, Datenschutzrecht, 523 in 9/43.
[405] Vgl VwGH 28.3.2006, 2004/06/0125 = VwSlg 16873 A/2006; VwGH 27.6.2006, 2005/06/0366.

sein (zB „Der Beschwerdegegner hat innerhalb von zwei Wochen (neuerlich) Auskunft über die zur Person des Beschwerdeführers verarbeiteten Daten aus der Datenbank xy zu erteilen oder zu begründen, warum die Auskunft nicht erteilt wird.“).[406]

Die DSB hat jedenfalls binnen sechs Monaten über die behauptete Rechtsverletzung zu entscheiden, ansonsten ist eine Säumnisbeschwerde an das BVwG gemäß § 39 Abs 1 DSG möglich. Es kann dabei zur Zurückweisung (beispielsweise wurden Fristen nach § 34 Abs 1 nicht gewahrt), zur Erteilung eines konkreten Mangelbehebungsauftrags nach § 13 Abs 3 AVG, zur formlosen Einstellung des Beschwerdeverfahrens (bspw aufgrund Klaglosstellung nach § 31 Abs 8) oder zu einem Bescheid mit (teilweise) stattgebendem oder (teilweise) abweisendem Spruch kommen. Wie auch aus dem Formular der DSB im Anhang 4 hervorgeht, sollte im privaten Bereich bei der Beschwerde nach § 31 gleichzeitig der Antrag gestellt werden, dem Gegner durch Bescheid aufzutragen, die entsprechende Auskunftserteilung durchzuführen (§ 31 Abs 7), ansonsten stellt die DSB nämlich nur fest, dass eine Verletzung im Recht auf Auskunft vorliegt.[407]

Der vollstreckbare Leistungsauftrag gegenüber Auftraggebern im privaten Bereich ist durch die Bestimmung des § 5 VVG mit Zwangsstrafe bedroht, da es sich hierbei um eine unvertretbare Leistung handelt. Die Vollstreckung erfolgt dabei gemäß § 1 Abs 2 lit a VVG durch die örtlich zuständige BVB.[408] Gegenüber Auftraggebern des öffentlichen Bereichs wäre ein Leistungsauftrag nicht vollstreckbar, da das zu einer Erzwingung unvertretbarer Leistungen im VVG vorgesehene Zwangsmittel, die Verhängung von Zwangsstrafen, gemäß § 5 Abs 4 VVG gegenüber einer Körperschaft öffentlichen Rechts nicht zulässig ist.[409] Werden die Rechte auf Auskunft, Löschung oder Richtigstellung vom Betroffenen gegenüber einer Verwaltungsbehörde oder einem anderen datenschutzrechtlich Verantwortlichen (Auftraggeber) des öffentlichen Bereichs geltend gemacht, so wird nicht durch einen in Form eines Bescheids ergehenden Verwaltungsakt sondern durch eine bloße Mitteilung entschieden. Diese bis auf die Schriftlichkeit nicht formgebundene Mitteilung des Auftraggebers ist daher nicht von den Verwaltungsgerichten sondern von der Datenschutzbehörde zu überprüfen. Die verwaltungsgerichtliche Kontrolle beginnt erst nach einem Zwischenschritt in Form eines Bescheids der Datenschutzbehörde. Dieses Abweichen von dem in Art 130 Abs 2 Z 1 des Bundes-Verfassungsge-

[406] ErlRV 472, BlGNR XXIV. GP, 12.
[407] DSK 22.5.2013, K121.935/0006-DSK/2013; vgl *Dohr/Pollirer/Weiss/Knyrim*, DSG², 210/72O in § 26 Anm zu E 64.
[408] *Jahnel*, Datenschutzrecht, 506 in 9/20 und 524 in 9/44. Ausführlich zur Vollstreckung DSK 27.9.2005, K073.025/0007-DSK/2005.
[409] DSK 10.8.2007, K073.028/0004-DSK/2007.

setzes angelegten System ist durch Unionsrecht bedingt (Art 28 der Richtlinie 95/46/EG; Garantie des Bestehens einer unabhängigen Kontrollstelle für Datenschutz in Art 8 Abs 2 der Charta der Grundrechte der EU).[410]

§ 31 Abs 8 sieht eine besondere verfahrensrechtliche Regelung für den in der Praxis regelmäßig auftretenden Fall vor, dass ein Beschwerdeführer während des Auskunfts-, Richtigstellungs- oder Löschungsbeschwerdeverfahrens klaglos gestellt wird, dh die mit der Beschwerde verfolgte Auskunft erteilt oder die Löschung/Richtigstellung durchgeführt wird. Wurde die Beschwerde in einem solchen Fall nicht ausdrücklich zurückgezogen (§ 13 Abs 7 AVG), so musste dennoch ein abweisender Bescheid erlassen werden, auch wenn auf Grund des Unterbleibens einer Stellungnahme des Beschwerdeführers im Parteiengehör zu vermuten war, dass dieser kein Interesse an der Weiterverfolgung seines Anspruches hat. Nun ist es der DSB möglich, in derartigen Fällen das Verfahren formlos (dh ohne Bescheiderlassung, wohl aber unter Verständigung des Beschwerdeführers) einzustellen, wenn der Beschwerdeführer nicht ausdrücklich auf einer Fortsetzung beharrt. Diese § 33 Abs 1 VwGG nachgebildete Ergänzung des verfahrensrechtlichen Instrumentariums des AVG scheint im Hinblick auf das kontradiktorisch ausgestaltete Beschwerdeverfahren vor der DSB zweckmäßig. Die formlose Einstellung ist auch nicht präjudiziell, eine neue Beschwerdeerhebung innerhalb der Frist des § 34 Abs 1 daher jederzeit möglich. Besonders Bedacht genommen wird in der Bestimmung auch auf die immer wieder vorkommende wesentliche Änderung des Verfahrensgegenstandes (§ 13 Abs 8 AVG) in einer derartigen Konstellation. Wenn etwa zunächst Beschwerde erhoben wurde, weil auf ein Auskunftsbegehren überhaupt nicht reagiert worden ist und während des Verfahrens eine Auskunft erteilt wird, die der Beschwerdeführer aber als unvollständig oder falsch ansieht, so ändert er bei einem entsprechenden Vorbringen den Verfahrensgegenstand wesentlich ab[411]. Solche Fälle werden nunmehr als (konkludente) Zurückziehung der ursprünglichen Beschwerde und gleichzeitige Einbringung einer weiteren Beschwerde mit dem geänderten Gegenstand gewertet. Damit beginnt auch die Entscheidungsfrist neu zu laufen. Die nach § 31 Abs 3 erforderlichen Inhalte müssen sich in einem derartigen Fall schlüssig aus einer Zusammenschau von alter und neuer Beschwerde ergeben, ansonsten ist die neue Beschwerde mangelhaft.[412]

Damit ist klargestellt, dass eine verspätete Auskunftserteilung (nach Ablauf der achtwöchigen Frist, jedoch vor Feststellung der Rechtsverletzung durch die DSB) für den Auftraggeber keine weiteren Konsequenzen nach sich zieht. Im Entscheidungszeitpunkt liegt kein tauglicher Beschwerdegrund (mehr) vor, da durch die tatsächliche Auskunftserteilung der Zweck des in § 26

[410] *DSB*, Datenschutzbericht 2015, 14.
[411] Vgl DSK 20.7.2007, K121.289/0006-DSK/2007.
[412] ErlRV 472, BlGNR XXIV. GP, 13.

normierten Auskunftsanspruchs erfüllt wurde.[413] Diese Konstellation ist zwar aus Sicht der möglichst minimalen Inanspruchnahme der DSB korrekt, könnte aber zu einer „Zermürbung" des Auskunftswerbers führen, da die Auftraggeber zunächst behaupten können, das Auskunftsbegehren nicht erhalten zu haben[414] und die im § 26 Abs 4 normierte Frist zur Auskunftserteilung von acht Wochen nicht zwingend einhalten müssen, da ihnen bei verspäteter Auskunftserteilung (vor Entscheidungszeitpunkt der DSB über die Beschwerde des Auskunftswerbers) keine Konsequenzen drohen. ME wäre an dieser Stelle zu überlegen, ob nicht doch ein Feststellungsinteresse des Auskunftswerbers an der Rechtsverletzung im Zeitpunkt der Beschwerdeerhebung (nach fruchtlosem Verstreichen der achtwöchigen Frist zur Auskunftserteilung) besteht, das in einer möglichen Verwaltungsstrafe für den säumigen Auftraggeber resultiert.[415]

Zur Wahrung der Übersichtlichkeit des § 31 wurden im Zuge der DSG-Novelle 2010 mit dem Beschwerdeverfahren zusammenhängende Instrumente in § 31a geregelt. Der bisherige § 31 Abs 3 (in der Praxis bedeutungslos) scheint im Hinblick darauf nicht mehr erforderlich, weil der neue § 30 Abs 6a, auf den in Abs 2 verwiesen wird, der DSB zumindest die gleichen Möglichkeiten gibt. Hinsichtlich des Bestreitungsvermerks wird nunmehr in § 31a Abs 3 im Hinblick auf eine Beschleunigung dieser Möglichkeit vorgesehen, dass darüber mit Mandatsbescheid entschieden werden kann. Der bisherige § 31 Abs 4 findet sich in § 31a Abs 4 unverändert wieder. Es wird lediglich zusätzlich angeordnet, dass die ersten beiden Sätze im Verfahren nach § 30 sinngemäß anzuwenden sind.[416]

Wie bereits in den vorangehenden Abschnitten skizziert, gab man mir bei einigen meiner Auskunftsbegehren nicht innerhalb der gesetzlich vorgesehenen Frist die erwartete Auskunft. Dabei traten folgende Mängel auf: entweder wurde keine Auskunft binnen acht Wochen oder eine unzulässige Negativauskunft oder eine unvollständige bzw unrichtige Auskunft erteilt. In diesen Fällen ist es möglich, mithilfe der Datenschutzbehörde den Auftraggeber zur vollständigen Erteilung der Auskunft aufzufordern. In den Anhängen 1-4 sind Formulare zum Auskunftsbegehren, zur Auskunftserteilung sowie zur Einleitung des KOV und des Beschwerdeverfahrens vor der Datenschutzbehörde ergänzt. In weiterer Folge werden die konkreten Mängel der einzelnen Auskunftsbegehren sowie die Vorgehensweise der DSB im Rahmen des Beschwerdeverfahrens nach § 31 thematisiert.

---

[413] Vgl ua DSK 1.7.2003, K120.698/002-DSK/2003; DSK 18.5.2004, K120.899/0004-DSK/2004; DSK 7.6.2005, K120.912/0008-DSK/2005; DSK 11.10.2006, K121.214/0006-DSK/2006; DSK 15.6.2007, K121.285/0011-DSK/2007; DSK 22.10.2008, K121.387/0020-DSK/2008; DSK 5.12.2008, K121.413/0011-DSK/2008; DSK 30.9.2011, K121.729/0008-DSK/2011.

[414] DSK 22.4.2005, K120.879/0003-DSK/2005.

[415] Die Praxis dieser Form der Verfahrensbeendigung wegen Klaglosstellung wurde jedoch vom BVwG in zwei Entscheidungen (Erkenntnisse vom 17.11.2015, W214 2014069-1 und W214 2107281-1) bestätigt.

[416] ErlRV 472, BlGNR XXIV. GP, 13f.

Meine Beschwerde gegen eine deutschsprachige Chatplattform mit einer .at-Domain und Hauptsitz in Deutschland wurde von der DSB mangels eigener Zuständigkeit an den Landesbeauftragten für den Datenschutz Baden-Württemberg weitergereicht. Dort teilte man mir in einer Stellungnahme mit, dass im Dezember 2015 ein Treffen der Aufsichtsbehörden aus Bayern, Hamburg, Berlin und Baden-Württemberg zum Thema Datenschutz bei Datingportalen stattgefunden hat[417]. Der Auskunftsanspruch kann nicht allein mit der Begründung abgelehnt werden, dass keine Namen und Anschriften gespeichert wurden. Gerade bei Anbietern von Onlineportalen ist die zweifelsfreie Zuordnung von Betroffenem und Pseudonym (Nickname) schwierig. Die Chatplattform wurde durch den Landesbeauftagten für den Datenschutz Baden-Württemberg aufgefordert, eine Downloadmöglichkeit der personenbezogenen Daten (wie beispielsweise Facebook sie anbietet) zu implementieren. Da die Umsetzung jedoch einige Zeit in Anspruch nimmt (Kommunikation zwischen Rechtsabteilung und Programmierer, Planung und Finanzierung der Schnittstelle, Sicherheitstests, Kommunikation gegenüber den Nutzern), wurde mir die gewünschte Auskunft bis dato (14 Monate nach der Initialanfrage) nicht erteilt.

Mein Auskunftsbegehren gegenüber meiner ehemaligen Schule wurde nach einer Beschwerde an die DSB durch den Landesschulrat zufriedenstellend beantwortet. Zunächst war mir lediglich mitgeteilt worden, dass personenbezogene Daten über mich in zwei Anwendungen gespeichert werden, jedoch nicht welche konkreten Daten dies sind.

Das Auskunftsbegehren gegenüber einem ehemaligen Arbeitgeber während des Studiums wurde von diesem nicht entsprechend ernst genommen, bzw erhielt ich drei Monate nach der Initialanfrage die Auskunft, dass diese irrtümlich als Spam beurteilt worden war, da ich direkt auf die Anwendbarkeit des Datenschutzgesetzes verwiesen habe. Hierzu ist festzuhalten, dass mangelndes Fachwissen rund um das Auskunftsbegehren nicht nur vonseiten des Auftraggebers, sondern auch vonseiten der Betroffenen einen wesentlichen Einfluss auf die Arbeit der DSB haben. Vielen Betroffenen ist nicht hinreichend klar, dass sie im indirekten Kontakt (zB via Formular, E-Mail, Kundenkarten) deutlich mehr sensible und intime Informationen über sich preisgeben, als sie dies im direkten Dialog tun würden. Persönliche Ansprache unmittelbar nach der Registrierung („Vervollständige dein Profil, damit ...“), Unerfahrenheit im Umgang mit der Preisgabe personenbezogener Daten („Offensichtlich tun dies die anderen auch, also wird dies richtig sein ...“) sowie vermeintliche Pflichtangaben (bei Facebook: „Freund X möchte gerne mehr über dich erfahren. Gib ... an!“) sind nur einige der von Auftraggebern gewählten Methoden, um mehr personenbezogene Daten als notwendig zu erhalten.

[417] Pressemitteilung des Landesbeauftragten für den Datenschutz Baden-Württemberg vom 11. Dezember 2015, abrufbar unter: http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/02/Augen-auf-bei-der-Partnersuche-im-Netz.pdf#, abgerufen am 11. Oktober 2016.

Facebook bietet die Auskunft über personenbezogene Daten über ein „self-service tool“ zum Download an. Der diesbezüglich kontaktierte Mitarbeiter hat mir jedoch mitgeteilt, dass die Daten, die ich bereits zur Löschung vorgemerkt hätte, darin nicht enthalten sind. Auf die Frage, wie ich an Daten herankomme, die ich zwar zur Löschung vorgesehen habe, die Facebook aber weiterhin speichert, wurde mir abstrakt das zuvor Beschriebene wiederholt: es gebe ein self-service tool und man weist darauf hin, dass man dort als Betroffener nicht die vollständige Auskunft erhalten könne. Abgesehen davon war bei der Verwendung des self-service tools von Facebook klar ersichtlich, dass nur ausgewählte Datenkategorien, aber mit Sicherheit nicht der vollständige Datensatz zu meiner Person beauskunftet wurde. Den Klagsweg über Irland, EuGH und österreichische Gerichte wie Maximilian Schrems zu beschreiten, ohne jedoch vollständige Auskunft von Facebook zu erhalten, ist derzeit kein Thema für mich. Diesbezüglich wird die DS-GVO ab 2018 wesentliche Veränderungen mit sich bringen, die es dem Betroffenen erleichtern, von Auftraggebern mit Hauptsitz in einem anderen EU-Mitgliedsstaat die gewünschte Auskunft über die gespeicherten personenbezogenen Daten zu erhalten. Schrems setzt sich für den Grundrechtsschutz ein (vgl Art 8 EMRK, Achtung des Privat- und Familienlebens sowie des Briefverkehrs) und konnte dabei mit seiner Klage vor dem EuGH erreichen, dass das Safe-Harbor-Abkommen mit den USA für ungültig erklärt wurde.[418] Die EU-Kommission erarbeitete daraufhin mit den USA das Folgeabkommen „Privacy Shield“, um es Auftraggebern zu ermöglichen, weiterhin personenbezogene Daten von europäischen Bürgern in die USA übermitteln zu können.[419] Schrems kritisierte das Privacy Shield-Abkommen, da es ebenso wie das Safe-Harbor-Abkommen zuvor keinen ausreichenden Schutz vor Massenüberwachung durch US-amerikanische Geheimdienste (beispielsweise NSA/National Security Agency) biete. Im Grunde besage Privacy Shield, dass US-Recht weiterhin Vorrang habe.[420]

5.3 Datenschutzrechtliche Klage vor den Zivilgerichten nach § 32 DSG

Ansprüche gegen Auftraggeber des privaten Bereichs wegen der Verletzung der Rechte des Betroffenen auf Geheimhaltung, auf Richtigstellung oder auf Löschung sind gemäß § 32 Abs 1 vom Betroffenen auf dem Zivilrechtsweg geltend zu machen.[421] Dabei ist folgende Konstellation denkbar: ein Auskunftswerber stellt ein Auskunftsbegehren an den Auftraggeber. Die DSB hilft dem Betroffenen im Beschwerdeverfahren nach § 31 dabei, die gewünschten Auskünfte zu erhalten. Diese Informationen können dem Betroffenen als Entscheidungsgrundlage die-

[418] EuGH 6.10.2015, C-362/14 (Schrems/Data Protection Commissioner).
[419] http://europa.eu/rapid/press-release_IP-16-2461_de.htm, abgerufen am 11. Oktober 2016.
[420] https://netzpolitik.org/2016/privacy-shield-da-steht-genauso-drin-us-recht-hat-vorrang/, abgerufen am 11. Oktober 2016.
[421] DSK 12.12.2007, K121.324/0008-DSK/2007.

nen, ob er den Prozessweg beschreiten möchte (im Beschwerdeverfahren fallen für den Betroffenen lediglich eigene Kosten an, da die entsprechende Eingabe gemäß § 53 Abs 1 von Gebühren befreit ist).[422,423] § 33 regelt etwaige Schadenersatzansprüche, die auf einer schuldhaften Verwendung von Daten entgegen dem DSG durch den Auftraggeber oder Dienstleister basieren.

Gemäß § 32 Abs 4 ist für Klagen und Anträge auf Erlassung einer einstweiligen Verfügung nach DSG in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht zuständig, in dessen Sprengel der Kläger (Antragsteller) seinen gewöhnlichen Aufenthalt oder Sitz hat. Klagen (Anträge) können aber auch bei dem Landesgericht erhoben werden, in dessen Sprengel der Beklagte seinen gewöhnlichen Aufenthalt oder Sitz oder eine Niederlassung hat. Die Zuständigkeit der Gerichte zur Entscheidung über subjektive Rechte darf nicht im Wege der Untersuchungs- und Kontrollrechte nach § 30 DSG umgangen werden.[424]

Die DSB weist dabei darauf hin, dass aufgrund des besonderen Gerichtsstands (Zuständigkeit des Gerichtshofs erster Instanz, unabhängig vom Streitwert) in diesem Verfahren die Pflicht besteht, sich durch einen Rechtsanwalt vertreten zu lassen. Einkommens- und vermögensschwache Mitbürgerinnen und Mitbürger können bei Gericht die Gewährung der Verfahrenshilfe (Gebührenbefreiung, Beigabe eines Rechtsanwalts) beantragen.[425] Der Instanzenzug führt nach dem Urteil des Landesgerichts zum OLG und OGH.

Zusammenfassend lässt sich festhalten, dass die drei unterschiedlichen Verfahrenstypen (KOV, Beschwerdeverfahren, Klage vor Zivilgerichten) dem Betroffenen ausreichend Möglichkeiten bieten, seine datenschutzrechtlichen Anliegen gegenüber dem Auftraggeber bzw Dienstleister durchzusetzen. Der Vorteil des Kontroll- und Ombudsmannverfahrens nach § 30 liegt im informellen Charakter (keine Verfahrensregeln bzw Formalitäten), jedoch kann die DSB keinen vollstreckbaren Bescheid – sondern lediglich eine Empfehlung – aussprechen. Im Beschwerdeverfahren nach § 31 erhält der Betroffene eine Entscheidung binnen sechs Monaten, muss dabei aber hinreichend am förmlichen Verwaltungsverfahren mitwirken. § 32 bietet dem Betroffenen die Möglichkeit, sein Recht auf Geheimhaltung, Richtigstellung oder Löschung gegenüber privaten Auftraggebern durchzusetzen. Dabei trägt der Betroffene jedoch das Kostenrisiko und unterliegt der Anwaltspflicht.[426]

---

[422] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 215 in § 32 Anm 3.

[423] DSK 23.8.2002, K120.819/003-DSK/2002; DSK 24.11.2010, K121.646/0011-DSK/2010; DSK 21.10.2011, K121.755/0005-DSK/2011; DSK 1.2.2013, K121.930/0004-DSK/2013; DSK 30.4.2013, K121.955/0005-DSK/2013; DSK 6.9.2013, K121.959/0010-DSK/2013.

[424] DSK 18.5.2004, K211.496/0003-DSK/2004.

[425] https://www.dsb.gv.at/rechte-der-betroffenen, abgerufen am 29. September 2016.

[426] Vgl https://www.dsb.gv.at/rechte-der-betroffenen, abgerufen am 30. September 2016.

5.4 Anfechtung beim BVwG/VwGH/VfGH/EuGH

Seit der Verwaltungsgerichtsbarkeits-Novelle 2012 kann gegen den Bescheid der DSB Beschwerde beim BVwG erhoben werden. Dies erfolgt in unionsrechtskonformer Umsetzung der Art 22 und 28 DSRL. Damit wurde auch der VwGH entlastet, der nach dem Durchlauf des administrativen Instanzenzugs (Ausschöpfung der Berufungs- und Einspruchsmöglichkeiten im Verwaltungsverfahren) angerufen werden konnte.[427] Die DSB stellte fest, dass dadurch die Bedeutung der Rechtsprechung der DSB für die verbindliche Auslegung und Weiterentwicklung des Datenschutzrechts reduziert wurde, daher wurde auch die Anzahl der im RIS dokumentierten Entscheidungen verringert. Das BVwG misst dabei insb der sorgfältigen Durchführung des Ermittlungsverfahrens zur Feststellung des für die Entscheidung wesentlichen Sachverhalts durch die DSB einen hohen Stellenwert zu.[428]

Gemäß Art 133 Abs 4 und 9 B-VG kann gegen Entscheidungen des BVwG in Datenschutzangelegenheiten nur dann zulässigerweise Revision an den Verwaltungsgerichtshof erhoben werden, wenn sie von der Lösung einer Rechtsfrage abhängt, der grundsätzliche Bedeutung zukommt, insb weil das Erkenntnis (der Beschluss) von der Rsp des VwGH abweicht, eine solche Rsp fehlt oder die zu lösende Rechtsfrage in der bisherigen Rsp des VwGH nicht einheitlich beantwortet wird. Revision können auch Parteien, die Auftraggeber des öffentlichen Bereichs sind, erheben. Soweit das BVwG keine ordentliche Revision zulässt, ist – bei Behauptung des Vorliegens einer Rechtsfrage, der grundsätzliche Bedeutung zukommt – die Einbringung einer außerordentlichen Revision an den VwGH möglich. Weiters steht den Parteien die Möglichkeit offen, wegen behaupteter Verletzung eines verfassungsgesetzlich gewährleisteten Rechts gegen ein Erkenntnis oder einen Beschluss des BVwG eine Beschwerde an den Verfassungsgerichtshof zu erheben. Gemäß Art 267 AEUV haben die Gerichte die Möglichkeit, dem Europäischen Gerichtshof Fragen zu Interpretation europäischen Rechts vorzulegen, die sie zu ihrer Entscheidungsfindung für erforderlich halten. Höchstgerichte haben in einem derartigen Fall sogar die Verpflichtung, derartige Fragen dem EuGH vorzulegen. Daher hat das BVwG in Datenschutzangelegenheiten die Möglichkeit, dem EuGH derartige Fragen vorzulegen, während etwa VwGH oder VfGH gegebenenfalls sogar dazu verpflichtet wären, bevor sie eine Entscheidung treffen.[429]

---

[427] *Souhrada-Kirchmayer*, Gerichtlicher Rechtsschutz gegen eine Aufsichtsbehörde (Art 78) in Knyrim (Hrsg.), DS-GVO, 328; ErlRV 1618 BlgNR XXIV. GP, 3.
[428] *DSB*, Datenschutzbericht 2014, 14.
[429] *Souhrada-Kirchmayer*, Gerichtlicher Rechtsschutz gegen eine Aufsichtsbehörde (Art 78) in Knyrim (Hrsg.), DS-GVO, 331.

5.5 Verwaltungsstrafbestimmungen nach § 52 DSG

Entsprechend Art 24 DSRL sind im DSG Sanktionen für die Ahndung von Verstößen vorgesehen.[430] Die DSB kann selbst keine Strafen verhängen, jedoch eine (Verwaltungs-)Strafanzeige erheben, welche gemäß § 52 Abs 5 DSG durch die Bezirksverwaltungsbehörde im Sprengel des Auftraggebers zu entscheiden ist – sollte der Auftraggeber keinen Sitz in Österreich haben, so ist die BVB am Sitz der DSB zuständig.[431]

Gemäß § 52 Abs 1 Z 3 stellt die Nichtbeauskunftung von Daten entgegen einem Bescheid bzw Urteil einen Verwaltungsstrafbestand dar, welcher mit einer Geldstrafe von bis zu 25.000 Euro zu ahnden ist. Dabei handelt es sich um einen Strafrahmen, der nicht ausgeschöpft werden muss.[432] Als Schuldform genügt hier Fahrlässigkeit, also die Verwirklichung eines der angeführten Tatbilder – zwar ohne dies direkt zu wollen, jedoch unter Außerachtlassung der möglichen Sorgfalt. Fahrlässigkeit wird dabei angenommen, dem Täter steht es jedoch frei, diese Vermutung durch Glaubhaftmachung seiner Schuldlosigkeit zu widerlegen. Kann der Mangel des Verschuldens nicht erwiesen werden, so geht dies zu Lasten des Täters.[433]

Die (teilweise) Nichterteilung der Auskunft mangels Verfügbarkeit der Information über die Herkunft der Daten bedeutet eine Verletzung des Rechts auf Geheimhaltung. Daneben begeht der Auftraggeber auch gemäß § 52 Abs 2 Z 4 eine Verwaltungsübertretung, wenn er die gemäß § 14 erforderlichen Sicherheitsmaßnahmen (Protokollierungspflicht) gröblich außer Acht lässt.[434]

---

[430] ErlRV 1613 BlgNR XX. GP, 54.
[431] Vgl *Dohr/Pollirer/Weiss/Knyrim*, DSG², 402 in § 52 Anm 19.
[432] ErlRV 742 BlgNR XXI. GP, 23.
[433] *Dohr/Pollirer/Weiss/Knyrim*, DSG², 401 in § 52 Anm 6 und 8.
[434] *Jahnel*, Datenschutzrecht, 384 in 7/29.

6 Ausblick auf die Datenschutz-Grundverordnung und DSG 2018

Die Datenschutz-Grundverordnung (DS-GVO 2016/679) trat am 25. Mai 2016 in Kraft, gilt ab 25. Mai 2018 und löst die bislang geltende RL 95/46/EG ab. In weiterer Folge werden die wesentlichen Änderungen, die sich durch die Geltung der DS-GVO ab 2018 ergeben, skizziert. In Art 12ff der DS-GVO werden die Modalitäten für die Ausübung der Betroffenenrechte (insbesondere das Auskunftsrecht) geregelt, eng damit ist die Datenportabilität nach Art 20 verknüpft. Art 25 legt die Rahmenbedingung für Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen fest, Art 55 enthält Strafbefugnisse, das One-Stop-Shop-Prinzip ist eine grundlegende Neuregelung, zudem wird mit Art 68 ein „Europäischer Datenschutzausschuss“ geschaffen und in Art 83 Abs 5 der bisherige Strafrahmen deutlich angehoben. Darüber hinaus kann jedes nationale Gericht in Zukunft in bestimmten Fällen verpflichtet sein, den EuGH im Rahmen einer Vorabentscheidung zu befassen – siehe dazu die Ausführungen in ErwGr 143 der DS-GVO.

ErwGr 39 DS-GVO formuliert die Leitgedanken, die bei der Verarbeitung personenbezogener Daten zu berücksichtigen sind. Der Betroffene (vgl Art 4 Z 1: identifizierte oder identifizierbare natürliche Person) soll dabei im Rahmen des Transparenzgebots leicht zugänglich und verständlich und in klarer und einfacher Sprache alle Informationen und Mitteilungen zur Verarbeitung der personenbezogenen Daten erhalten können. Dies führt einerseits zum Auskunftsanspruch in Art 15, andererseits sind damit auch Informationen über die Identität des Verantwortlichen (dabei ist mE das Impressum ausreichend[435]) sowie der Zweck der Verarbeitung gemeint. Explizit genannt ist dabei auch das Recht der Betroffenen, darüber aufgeklärt zu werden, wie sie ihre diesbezüglichen Rechte geltend machen können. Bemerkenswert ist ebenso der Gedanke der Datensparsamkeit bzw gar Datenvermeidung (Beschränkung der Speicherfrist sowie des Umfangs, der für die Verarbeitung notwendig ist). In meiner Masterthesis („Blockchain-Technologie: Anwendungsbereiche und ausgewählte Rechtsfragen“) werde ich mich mit Datenschutzeinstellungen auseinandersetzen, dabei geht es um die Frage, ob der Betroffene den Unternehmen, denen er die Datenverarbeitung erlaubt, via Blockchain im Sinne von privacy by design/default (Art 25 DS-GVO) obligatorische Rahmenbedingungen vorgeben könnte, innerhalb derer er die Datenverwendung gestattet.[436]

Art 15 DS-GVO enthält die Neuregelung des Auskunftsanspruchs des Betroffenen. Der Auftraggeber hat künftig explizit auf das Bestehen des Beschwerderechts bei einer Aufsichtsbehörde hinzuweisen. Abs 3 geht auf die elektronische Einbringung des Auskunftsbegehrens ein, wodurch insgesamt ein rascherer und kostengünstigerer Ablauf zu erwarten ist (durch die

[435] AA *Illibauer,* Informationsrecht und Modalitäten für die Ausübung der Betroffenenrechte, in Knyrim (Hrsg.), DS-GVO, 116.
[436] Näheres dazu in *BfDI*, Datenschutz-Grundverordnung, 22f.

Funktion „Lesebestätigung anfordern“ bei der Einbringung mittels E-Mail ist ein verbindlicher Zeitpunkt bekannt, der den Fristenlauf des Auskunftsbegehrens determiniert). *Haidinger* weist darauf hin, dass sich durch die DS-GVO zwei Punkte jedenfalls ändern: gemäß Art 15 Abs 3 hat der Verantwortliche ausdrücklich Kopien (E-Mails, Datenbankauszüge) der personenbezogenen Daten zur Verfügung zur stellen[437], zudem sind gemäß Art 15 Abs 1 lit d die Speicherfristen explizit zu beauskunften (Auftraggeber haben sich derzeit kaum mit derartigen Überlegungen auseinandergesetzt, weil oftmals ausreichend Speicherplatz für eine prinzipiell unbeschränkte Aufbewahrungsdauer vorhanden ist).[438] Im Unterschied zum DSG kann der Betroffene künftig gemäß Art 12 Abs 1 auch eine mündliche Auskunftserteilung verlangen, sofern er seine Identität entsprechend nachweist. Bei der Datenverarbeitung im Zusammenhang mit Kindern muss darauf geachtet werden, dass die Sprache und Darstellung (vgl ErwGr 58, Verwendung visueller Elemente wie Symbole, Icons udgl) der Informationen entsprechend angepasst wird.

Die Unentgeltlichkeit der Auskunftserteilung wird in Art 12 Abs 5 normiert. Demnach sind Informationen gemäß den Art 13 und 14 sowie alle Mitteilungen und Maßnahmen gemäß den Art 15 bis 22 und Art 34 unentgeltlich zur Verfügung zu stellen. Allerdings kann der Verantwortliche bei offenkundig unbegründeten oder — insbesondere im Fall von häufiger Wiederholung — exzessiven Anträgen einer betroffenen Person entweder ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder sich gänzlich weigern, aufgrund des Antrags tätig zu werden. Bei einem eher statischen Datenbestand wird ein Auskunftsersuchen pro Kalenderjahr wohl als verhältnismäßig einzustufen sein.[439] Der Verantwortliche hat den Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen. Es ist dabei ebenso wie bei der mündlichen Auskunftserteilung empfehlenswert, alle relevanten Tatsachen zu dokumentieren. Bei der gänzlichen Verweigerung der Auskunftserteilung ist wohl dennoch eine mit der Negativauskunft vergleichbare Information an den Betroffenen zu richten.

Art 11 thematisiert den Identitätsnachweis des Betroffenen bei Datenverarbeitungen, die keine Identifizierung des konkreten Nutzers erfordern. Der Verantwortliche ist dabei nicht verpflichtet, Informationen hinsichtlich der Identifizierung des Betroffenen aufzubewahren (ErwGr 64) oder einzuholen (ErwGr 57). Sofern der Verantwortliche nachweisen kann, dass er den Betroffenen nicht identifizieren kann, so entfällt dessen Auskunftsanspruch. Denkbar sind hierbei

[437] Bisher lehnte die DSB dies ausdrücklich ab: DSK 22.5.2013, K121.925/0007-DSK/2013.
[438] *Haidinger,* Die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch (Art 15-21 DSGVO), in Knyrim (Hrsg.), DS-GVO, 127f.
[439] *Haidinger,* Die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch (Art 15-21 DSGVO), in Knyrim (Hrsg.), DS-GVO, 126.

ua folgende Datenverarbeitungen: Dienstenutzung via Wertkarte (Telefonie, Internet), Gutscheine für Online-Angebote (zB Glücksspiel, Nutzung von Musik- und Videostreamingplattformen), Smart-Anwendungen (Smart Home/Meter, Cars, Watch, TV uvm – hierbei ist nur der abstrakte Nutzerkreis bekannt, wie beispielsweise der Haus- oder Autoeigentümer und dessen Bekanntenkreis – jedoch ist die Identifizierbarkeit eines konkreten Betroffenen nicht möglich). Dies könnte tendenziell zu Missbrauch führen, wenn der Verantwortliche nicht an dem konkreten Nutzerprofil sondern abstrakt am Profiling von verschiedenen Nutzergruppen interessiert ist, um diesen Gruppen maßgeschneiderte Angebote liefern zu können. Dies führt insgesamt zu einer unbefriedigenden Situation, weil der Betroffene keinen Auskunftsanspruch hat, welche Daten über ihn verarbeitet werden, weiters ist die Nachvollziehbarkeit der Herkunft und der Empfänger der Daten nicht gegeben. Da künftig wohl weitaus mehr Datenverarbeitungen ohne Identifizierung des konkret Betroffenen als derzeit zu erwarten sind, ist zu hinterfragen, ob dies eine positive Weiterentwicklung des Datenschutzrechts darstellt. Die Auskunftserteilung kann jedoch nur verweigert werden, wenn der Verantwortliche glaubhaft macht, dass er nicht in der Lage ist, die betroffene Person zu identifizieren – das bedeutet in weiterer Konsequenz, dass er jede Möglichkeit der Identifizierung nutzen müsste. Dabei ist zu berücksichtigen, dass eine unbefugte Herausgabe von personenbezogenen Daten an Nicht-Betroffene zu empfindlichen Strafen führen kann.[440] Es ist zu bezweifeln, ob dies die Klügste aller denkbaren Lösungen darstellt, da damit letztendlich wie beim Diskurs mit dem Telekommunikationsdiensteanbieter dieser rückwirkend leicht darstellen kann, dass er nicht mehr zweifelsfrei feststellen kann, ob ich im fraglichen Zeitraum die Datenanwendung ausschließlich benutzt habe. Umgekehrt wäre auch möglich gewesen, den Verantwortlichen von vornherein zu verpflichten, jeweils eine plattforminterne Lösung bereitzustellen, welche die Erforderlichkeit der eindeutigen Identifizierbarkeit des Betroffenen auf die Kenntnis der Zugangsdaten verschiebt (vgl auch ErwGr 64).

Als Frist für die Auskunftserteilung ist in Art 12 Abs 3 ein Monat ab Eingang des Auskunftsbegehrens normiert, diese Frist kann bei entsprechender Komplexität auf insgesamt drei Monate erweitert werden (die Fristerweiterung ist dem Betroffenen vorab mitzuteilen). Die Negativauskunft (der Verantwortliche erteilt dem Betroffenen keine Auskunft, vgl Art 12 Abs 4) ist ebenfalls unverzüglich, jedoch innerhalb eines Monats zu erteilen und hat die Gründe für die Verweigerung sowie die Möglichkeit der Beschwerde bei der Aufsichtsbehörde bzw eines gerichtlichen Rechtsbehelfs zu beinhalten.

Art 20 normiert neben dem Auskunftsanspruch über die verarbeiteten personenbezogenen Daten die Möglichkeit der Datenübertragbarkeit von einem Verantwortlichen zu einem anderen

[440] *Illibauer,* Informationsrecht und Modalitäten für die Ausübung der Betroffenenrechte, in Knyrim (Hrsg.), DS-GVO, 118.

Verantwortlichen. Dabei ist etwa an den Wechsel Social Media-Anbieter, Versicherung, Hausbank, Telefonie- oder Internetdiensteanbieter zu denken. Offen bleibt laut *Haidinger* dabei jedoch, wie genau die Datenübertragbarkeit bei Datenanwendungen aussieht, deren Inhalt vom Betroffenen nicht bereitgestellt, sondern verursacht wurde (beispielsweise Bewegungsdaten – eventuell überwiegt hier der Grundsatz der Datensparsamkeit, sodass derartige Informationen nicht an den neuen Verantwortlichen zu übertragen sind). Der Konflikt zum geistigen Eigentum Dritter (Arten der Datenkategorien, durch den Verantwortlichen vorgenommene Bewertungen) steht dabei ebenso zur Debatte.[441]

Die Aufsichtsbehörde (aktuell: „Datenschutzbehörde“) ist künftig gemäß Art 55 DS-GVO für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr mit dieser Verordnung übertragen wurden, im Hoheitsgebiet ihres eigenen Mitgliedstaats zuständig. Damit erhält sie voraussichtlich auch eine Strafbefugnis, die bisher bei den Bezirksverwaltungsbehörden angesiedelt war. Sollte ein Auftraggeber die Rechte der betroffenen Person (also beispielsweise den Auskunftsanspruch) missachten, so hat die Aufsichtsbehörde gemäß Art 83 Abs 5 DS-GVO eine Geldbuße von bis zu 20 Millionen Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs zu verhängen, je nachdem, welcher der Beträge höher ist. Dies führt zu einem Spannungsverhältnis mit österreichischem Verfassungsrecht, da der VfGH in stRsp die Auffassung vertritt, dass Art 91 Abs 2 und 3 B-VG (Anklageprinzip) die Verhängung hoher Geldstrafen (ab etwa € 200.000,-) den ordentlichen Gerichten vorbehalten ist.[442] Dementsprechend sollte der österreichische Gesetzgeber von der Ausnahmebestimmung des Art 83 Abs 9 DS-GVO Gebrauch machen und die Verhängung der Geldbußen zur Gänze den Gerichten überantworten. Die Geldbußen sollen im Einzelfall wirksam, verhältnismäßig und abschreckend sein (Art 83 Abs 1), sodass sich die Verantwortlichen bereits vor Aufnahme der Datenverarbeitung intensiv damit befassen, wie diese aus Sicht des Datenschutzes konzipiert werden muss (insbesondere können Flüchtigkeitsfehler wie das Versenden einer E-Mail an mehrere Empfänger zu hohen Geldbußen führen). Falls sich der Verantwortliche künftig nicht an der DS-GVO orientiert, drohen somit nicht bloß Imageschäden und Ablenkung von der Arbeitsleistung, sondern eben auch existenzgefährdende Geldbußen und sonstige Sanktionen (Verwarnung, vgl ErwGr 148 und 150).[443]

---

[441] *Haidinger,* Die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch (Art 15-21 DSGVO), in Knyrim (Hrsg.), DS-GVO, 134.

[442] Vgl insb VfSlg 12.151/1989 und *Öhlinger/Eberhard*, Verfassungsrecht[11] (2016) Rz 627 mwN. Der VfGH hat seine Auffassung auch nach Einführung der Verwaltungsgerichtsbarkeit erster Instanz nicht in Frage gestellt (vgl etwa VfGH 10.3.2015, G 203/2014 ua).

[443] *Illibauer,* Geldbußen und andere Sanktionen, in Knyrim (Hrsg.), DS-GVO, 337 und 342f.

Eine weitere wesentliche Veränderung ist die engere Zusammenarbeit der nationalen Aufsichtsbehörden im sogenannten Kohärenzverfahren nach Art 64 DS-GVO (erhöhter Koordinationsaufwand mit federführender Behörde). Zudem wird der sogenannte „One-Stop-Shop-Mechanismus" umgesetzt, demnach ist für Unternehmen mit mehreren Niederlassungen die Aufsichtsbehörde am Hauptsitz zuständig. Damit bekommen die Unternehmen einen zentralen Ansprechpartner und werden dadurch gegenüber den bisherigen Regelungen erheblich entlastet.[444] Die DS-GVO bewirkt eine Verschiebung der Aufgaben der DSB, da diese künftig im Vorfeld von Datenverarbeitungen mitzuwirken hat bzw einzubinden ist (etwa bei der Datenschutz-Folgeabschätzung, Bestellung eines Datenschutzbeauftragten, Zertifizierung). Bislang war der Hauptaufgabenbereich der DSB in der Durchsetzung subjektiver Rechte (Auskunft, Richtigstellung, Löschung, Widerspruch) angesiedelt.[445]

Art 68 DS-GVO (siehe auch ErwGr 139) normiert ein neues Gremium, und zwar den „Europäischen Datenschutzausschuss". Dessen Kernaufgabe ist entsprechend Art 70 DS-GVO die Sicherstellung der einheitlichen Anwendung der DS-GVO in den Mitgliedsstaaten. Dies kann sich unter anderem in Beratung, Ausarbeitung von Leitlinien, Akkreditierung von Zertifizierungsstellen und in der Abgabe von Stellungnahmen äußern. Dieses Gremium ist mit der aktuellen „Art 29-Gruppe" vergleichbar.

Das DSG wird zwar mit der DS-GVO grundlegend geändert, behält aber weiterhin wesentliche innerstaatliche Regelungen bei, insbesondere zur Struktur der unabhängigen Aufsichtsbehörde (DSB). Die DS-GVO sieht vor, dass das DSG ab 2018 die Bestimmungen der Art 51 ff beinhaltet, und zwar durch die Umsetzungsverpflichtung in Art 51 Abs 4. Weiters können die Mitgliedsstaaten gemäß Art 83 Abs 7 Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.

Auch in Deutschland gibt es schon konkrete Pläne zur grundlegenden Reform des BDSG 2018, im inoffiziellen Referentenentwurf des Bundesministeriums des Innern (der Entwurf wurde mittlerweile zurückgezogen und neu erstellt) finden sich ua Bestimmungen zu Betroffenenrechten, Ausgestaltung der unabhängigen Datenschutzaufsichtsbehörden, Rechtsschutzmöglichkeiten und Verhängung von Geldbußen.[446]

---

[444] Näheres dazu in *BfDI*, Datenschutz-Grundverordnung, 19f.

[445] *Flendrovsky*, Die Aufsichtsbehörden, in Knyrim (Hrsg.), DS-GVO, 290.

[446] *Bundesministerium des Innern* (Referentenentwurf), Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Datenschutz-Grundverordnung und zur Umsetzung der Richtlinie (EU) 2016/680, abrufbar unter https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/09/Entwurf-ABDSG-E-08.2016.pdf, abgerufen am 13. Oktober 2016.

Gerade im Bereich Rechtsinformatik bzw Informationsrecht wird deutlich, wie weit die Gesetzgebung den tatsächlichen Gegebenheiten nachsteht – Auftraggeber könnten mit geringem Aufwand den Auskunftsanspruch aushebeln. Eine denkbare Herangehensweise wäre (wie in der DSB-Entscheidung zum Online-Banking gezeigt), dass der Auftraggeber dem Betroffenen einen Fernzugang zu einem Account gewährt (ErwGr 63), wo diesem unstrukturiert dessen personenbezogene Daten zur Verfügung gestellt werden (der Betroffene hat keinen Anspruch darauf, die Daten in einer bestimmten Form zu erhalten). Die Datenschutzthematik könnte sich auch dahingehend weiterentwickeln, dass die Betroffenen von den „Auftraggebern" dazu verpflichtet werden, in einer Datenanwendung ihre Stammdaten zentral zu pflegen (beispielsweise im Smart Car oder im Smart TV), der Betroffene gewährt den „Auftraggebern" einzeln oder gebündelt Zugriff auf die Daten – in diesem Fall würde die Auftraggeberposition jedoch wegfallen, da der Betroffene selbst seine Daten speichert und an Dienstleister weitergibt (der Betroffene allein würde im soeben geschilderten Szenario entscheiden, wer welche Daten in seinem Auftrag verarbeiten darf). Bei Facebook und anderen Onlineplattformen ist allmählich der Paradigmenwechsel erkennbar, denn der Auftraggeber ist letztendlich der Betroffene selbst (er entscheidet, ob er personenbezogene Daten von sich auf seiner Pinnwand postet – und via Privatsphäre-Einstellungen kann er entscheiden, wem er darauf Zugriff gewährt). Algorithmen bzw die konkrete technische Umsetzung der Datenverarbeitung durch Auftraggeber oder Dienstleister sind nicht zu beauskunften, sondern lediglich die verwendeten Basisdaten – und über diese verfügt der Betroffene, sobald er seine eigene Pinnwand in der Onlineplattform aufruft.

Gärtner hat in seiner Dissertation gezeigt, welche Bedeutung Datenanwendungen für Unternehmen haben und wie gefährlich gestohlene Daten damit sein können. Es gilt, einen vernünftigen Kompromiss zu erzielen, damit einerseits Betroffene Auskunft über ihre Daten erhalten, Unternehmen zur Einhaltung von Datensicherheitsmaßnahmen verpflichtet werden, andererseits die Unternehmen aber ihre Geschäftstätigkeiten möglichst flüssig weiterführen können. Wenn Vertrauen gegenüber seinen Geschäftspartnern an Bedeutung verliert und zunehmend durch Scoring-Algorithmen (Bonitätsdatenbank, Social-Media-Accounts) ersetzt wird, so sind die Verbraucherinteressen entsprechend zu berücksichtigen, um diese nicht durch die faktische Übermacht der Unternehmen zu benachteiligen.[447]

Zusammenfassend lässt sich festhalten, dass der Rechtsschutz bei Auskunftsbegehren mE ausreichend geregelt ist, jedoch ist die DS-GVO dahingehend zu begrüßen, dass diese auf aktuelle Entwicklungen (unter anderem globale Wirtschaftsprozesse, elektronische Auskunftserteilung, empfindliche Strafrahmen) eingeht und damit das Datenschutzrecht weiterent-

[447] *Gärtner*, Harte Negativmerkmale auf dem Prüfstand des Datenschutzrechts.

wickelt. Das Ziel der DS-GVO ist ein informierter Betroffener, der seine Rechte einfacher wahrnehmen und durchsetzen kann. Dabei ist unter anderem die Verwendung von Bildsymbolen denkbar (Art 12 Abs 7 und ErwGr 58), um dem Betroffenen die Informationen präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache zur Verfügung stellen zu können. In diesem Sinne ist aus Sicht der Aufsichtsbehörden und der europäischen Institutionen darauf zu achten, dass die Gesetzeslage regelmäßig an die eingangs geschilderten wirtschaftlichen Rahmenbedingungen in der Europäischen Union angepasst und dabei die historisch gewachsenen Datenschutzstandards beibehalten werden.

Persönliche Anmerkungen

Die vorliegende Arbeit habe ich aus einem starken persönlichen Interesse heraus verfasst; zum einen wollte ich wissen, welche Datenkategorien Firmen und staatliche Stellen über mich speichern – denn dies ist schließlich die Voraussetzung, um Richtigstellung oder Löschung begehren zu können. Mir war dabei von vornherein klar, dass nicht alle Auskünfte vollständig oder ordnungsgemäß erteilt werden würden, da hier oftmals wirtschaftliche Interessen diametral entgegenstehen (beispielhaft dafür Facebook und andere Chatplattformen). Zum anderen wollte ich mir ein vielfach immer noch stiefmütterlich behandeltes Thema erarbeiten, da ich nach wie vor darin die Idee sehe, mit einem bewussten und sparsamen Umgang mit persönlichen Daten zu einer Gesellschaft mit Chancengleichheit beizutragen.

Meine Eltern haben mich schon früh für den Datenschutz sensibilisiert, da sie mir bereits während meiner Schulzeit im Streit um das Bildungsdokumentationsgesetz (dort wurde die Sozialversicherungsnummer eines jeden Schülers abgespeichert, um dessen schulischen und studentischen Werdegang abbilden zu können – dies wäre beispielsweise ebenso gut mit einem bereichsspezifischen Kennzeichen möglich, dabei wird eben nicht die SV-Nummer verwendet) gezeigt haben, wie man sich mit persönlichem Engagement für eine Veränderung der Gesetzeslage einbringen kann.

In meiner juristischen und beruflichen Praxis nehme ich vielfach Sorglosigkeit im Umgang mit persönlichen Daten und Informationen wahr: dies reicht von Social Media, über E-Commerce, diverse „smarte“ Anwendungen (Smartphone, Smart Cars, Smart Meter, Smart TV, Smart Home, Smart Watch) bis hin zur Preisgabe und Übermittlung von Daten an Dritte (in diesem Zusammenhang sei beispielhaft NSA/Snowden genannt – vor mittlerweile drei Jahren wurden die Datentransfers bekannt, geändert hat sich seitdem aber vergleichsweise wenig). Wir stehen an einem ökonomischen und gesellschaftlichen Scheideweg, und wenn der „gläserne Mensch“ (Stichworte: polizeiliches Staatsschutzgesetz, massenhafte Überwachung privater Kommunikation entgegen Artikel 8 EMRK, langfristige Dokumentation von individuellem Fehlverhalten) nicht zur Realität werden sollen, müssen wir uns weiterhin dafür vehement einsetzen, personenbezogene und sensible Daten zu schützen.

Anhang 1 – Formular Auskunftsbegehren

Die Datenschutzbehörde empfiehlt auf ihrer Webseite[448] die Verwendung des nachfolgenden Formulars, um ein Auskunftsbegehren an den Auftraggeber zu richten:

Ersuchen um Auskunft gemäß § 26 DSG 2000

Stand: 1. Januar 2014

Absender:

Name:

Anschrift, Straße: .....

Anschrift, Postleitzahl, Ort: .....

.....

An:

Name/Firma:

Anschrift, Straße: .....

Anschrift, Postleitzahl, Ort: .....

.....

_____
Ort / Datum

Sehr geehrte Damen und Herren:

Hiermit ersuche ich um Auskunft gemäß § 26 Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999.

448 https://www.dsb.gv.at/documents/22758/115215/Druckformular-Ersuchen_um_Auskunft_Par_26_DSG.pdf/b285b27a-278b-4dc2-8113-61a587fe5c61, abgerufen am 02. September 2016.

X

Bitte wählen Sie ☒ aus!

☐	Ich ersuche um Auskunft über alle zu meiner Person gespeicherten Daten.
☐	Ich ersuche um Auskunft über meine Daten aus einer bestimmten Datenanwendung, nämlich _
☐	Ich ersuche um Auskunft über meine Daten im Zusammenhang mit einem bestimmten Ereignis, nämlich _

Mehrfachnennungen ☒ möglich!

☐	Ich ersuche um Auskunft über den logischen Ablauf einer automatisierten Entscheidungsfindung (§ 49 Abs. 3 DSG 2000, zB Bonitätsprüfung) _

☐	Bitte erteilen Sie mir auch Auskunft über Ihre Dienstleister.

Bitte wählen Sie ☒ aus!

☐	Als Beweis meiner Identität lege ich eine Kopie eines amtlichen Lichtbildausweises bei.
☐	Ich erbringe folgenden sonstigen Identitätsnachweis:_ _

Gemäß § 26 Abs. 7 DSG 2000 dürfen Sie meine Daten während des Auskunftsverfahrens bei Strafe (§ 52 Abs. 1 Z 4 DSG 2000, Geldstrafe bis zu 25 000 Euro) nicht löschen.

Unterschrift: ___________________________________

<u>Beilage</u>

Anhang 2 – Musterschreiben Auskunftserteilung

Knyrim empfiehlt, für die jeweiligen Anfragen von Betroffenen Musterschreiben zu konzipieren, um rascher auf Auskunftsersuchen reagieren zu können. Folgende beispielhafte Struktur dient dabei als Grundgerüst:

„„„Sehr geehrte ...
Zu Ihrem Auskunftsersuchen nach § 26 DSG teilen wir mit wie folgt:

1. [Im Fall einer Negativauskunft] Wir haben keine Daten Ihrer Person in unserer Datenanwendung [Bezeichnung der Datenanwendung] gespeichert. Bitte geben Sie uns nähere Details bekannt, aufgrund derer Sie vermuten, in unserer Datenanwendung gespeichert zu sein.
2. Wir verarbeiten folgende Daten von Ihnen: [Aufzählung sämtlicher Daten, die über den Betroffenen gespeichert sind.]
3. Diese Daten haben wir [zB aufgrund Ihrer eigenen Angaben/aus dem Telefonbuch/vom Adressverlag XY] erhalten.
4. Wir haben diese Daten [zB an niemanden/ an ... und ... übermittelt].
5. Wir verarbeiten Ihre Daten zum Zweck der [zB Durchführung Ihrer Bestellung/Bewerbung unserer XYZ-Produkte].
6. Die Rechtsgrundlage für die Verarbeitung Ihrer Daten durch uns ist [zB unsere Gewerbeberechtigung für das ... Gewerbe].
7. Für die Verarbeitung Ihrer Daten haben wir die Firma [...] als Dienstleister iSd § 10 DSG 2000 beauftragt.)““[449]

Sollte der Identitätsnachweis fehlen bzw mangelhaft sein, so empfiehlt *Knyrim* folgendes Musterschreiben:

„„„Sehr geehrte ...
Wir beziehen uns auf Ihr Schreiben vom [Datum]. Gemäß Auskunftsrecht nach § 26 Datenschutzgesetz (DSG 2000) kann jede Person oder jede Personengemeinschaft vom Auftraggeber einer Datenanwendung Auskunft darüber verlangen, ob und welche Daten über sie verarbeitet werden. Dabei muss sichergestellt sein, dass die angeforderten Daten ausschließlich an die betroffene Person zugestellt werden. Wir sind somit verpflichtet, die Identität des Auskunftswerbers zu überprüfen. Wir ersuchen Sie daher, eine Kopie Ihres Reisepasses, Personalausweises oder Führerscheins an uns zu übermitteln.

Nach Einlangen der Unterlagen werden wir innerhalb der Frist von acht Wochen Ihr Ansuchen beantworten.““[450]

[449] *Knyrim*, Datenschutzrecht³, 324.
[450] *Knyrim*, Datenschutzrecht³, 323.

Anhang 3 – Formular für Kontroll- und Ombudsmannverfahren

Die Datenschutzbehörde empfiehlt auf ihrer Webseite[451] die Verwendung des nachfolgenden Formulars, um eine Verletzung des § 30 DSG geltend zu machen:

Eingabe an die Datenschutzbehörde im Kontroll- und Ombudsmannverfahren (§ 30 Abs. 1 DSG 2000)

Stand: 4. Juli 2016

Einschreiter/in:

Name:

Anschrift, Straße: .....

Anschrift, Postleitzahl, Ort: .....

E-Mail-Adresse: .....

Telefon: .....

Fax: .....

Ich ersuche versandbereite Dokumente entsprechend Zustellgesetz unmittelbar elektronisch an

folgende E-Mail-Adresse auszufolgen:

Fettgedruckte Angaben werden **unbedingt** benötigt. Nach dem Gesetz können Anbringen auf jede technisch mögliche Weise eingebracht werden, also nicht nur per Post sondern auch per Fax oder E-Mail. Jede Nachricht reist aber auf Gefahr des Senders, was bedeutet, dass Sie im Streitfall belegen müssen, dass die Nachricht den richtigen Empfänger erreicht hat. Die Datenschutzbehörde behält es sich aber vor, bei Anbringen ohne Unterschrift (betrifft insbesondere E-Mails ohne elektronische Signatur) bei Zweifel zur Klärung der Identität eine unterschriebene Bestätigung des Senders zu verlangen. Daher – sowie für Zwecke der Zustellung nachweispflichtiger Sendungen (RSa- und RSb-Briefe) – ist die Angabe einer Postadresse (kein Postfach!) notwendig. Andere Korrespondenz kann gerne auf elektronischem Wege erfolgen. Durch Gebrauch von E-Mail oder Fax stimmen Sie nach dem Gesetz auch dem Empfang von Nachrichten auf diesem Wege zu. Die Datenschutzbehörde weist Sie darauf hin, dass Ihre Eingabe im Kontroll- und Ombudsmannverfahren sowie alle Ihre anderen Eingaben dem Antragsgegner zur Kenntnis gebracht werden müssen.

Bitte schicken Sie Ihre Eingabe nur einmal! Bitte ☒ ankreuzen!

---

[451] https://www.dsb.gv.at/at.gv.bka.liferay-app/documents/22758/115215/Druckformular_Ombudsmanneingabe_07-2016.pdf/9260b511-52b5-4bc7-bfc2-e2faa3c2ec44, abgerufen am 02. September 2016.

An die Datenschutzbehörde

Hohenstaufengasse 3

1010 Wien

REPUBLIK ÖSTERREICH

- via Fax 53115 / 202690
- via E-Mail dsb@dsb.gv.at

Ich wende mich an die Datenschutzbehörde, um eine mich betreffende Rechts- bzw Pflichtenverletzung durch einen Auftraggeber im

☐	Privaten Bereich (Beschwerdegegner ist zB Unternehmen, Privatperson, Verein, politische Partei)
☐	Öffentlichen Bereich (Beschwerdegegner ist zB eine Behörde, amtliche Dienststelle, Gemeinde, Kammer, gesetzlich anerkannte Kirche oder Religionsgesellschaft)

zu rügen.

Dies betrifft folgenden Auftraggeber:

Name (Firma): .....

Adresse: .....

DVR-Nr. (falls vergeben und bekannt): .....

Art der Rechtsverletzung:

☐	Verletzung meines **Rechts auf Geheimhaltung** schutzwürdiger personenbezogener Daten (§ 1 DSG 2000)
☐	Verletzung meines Anspruchs auf **Richtigstellung** von Daten (§ 27 DSG 2000)
☐	Verletzung meines Anspruchs auf **Löschung** von Daten (§ 27 DSG 2000)
☐	Verletzung meines Anspruchs auf **Auskunft** über eigene Daten (§ 26 DSG 2000)
☐	Nichtbeachtung meines **Widerspruchs** gegen Datenverwendung (§ 28 DSG 2000)
☐	Sonstiges, nämlich: _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Art der Pflichtenverletzung:

☐	Der Auftraggeber hat keine DVR-Nummer geführt oder in sonstiger Weise gegen die Pflicht zur Offenlegung seiner Identität verstoßen.
☐	Der Auftraggeber hat gegen die Meldepflicht beim Datenverarbeitungsregister verstoßen.
☐	Der Auftraggeber hat gegen die Pflicht zur Offenlegung nicht-meldepflichtiger Datenanwendungen verstoßen.
☐	Der Auftraggeber nimmt an einem Informationsverbundsystem teil oder betreibt es, ohne sich der Vorabkontrolle durch die Datenschutzbehörde unterzogen zu haben.
☐	Der Auftraggeber betreibt eine Datenanwendung mit sensiblen Daten (Angaben zur rassischen oder ethnischen Herkunft, politischen Meinung, Gewerkschaftszugehörigkeit, religiösen oder philosophischen Überzeugungen, zur Gesundheit und zum Sexualleben), ohne sich der Vorabkontrolle durch die Datenschutzbehörde unterzogen zu haben.
☐	Der Auftraggeber betreibt eine Datenanwendung zur Auskunftserteilung über Kreditwürdigkeit, ohne sich der Vorabkontrolle durch die Datenschutzbehörde unterzogen zu haben.
☐	Der Auftraggeber betreibt eine Datenanwendung mit strafrechtlich relevanten Daten, ohne sich der Vorabkontrolle durch die Datenschutzbehörde unterzogen zu haben.
☐	Der Auftraggeber hat bei der Ermittlung von Daten gegen die Informationspflicht verstoßen.
☐	Der Auftraggeber hat keine ausreichenden Datensicherheitsmaßnahmen ergriffen.
☐	Sonstiges, nämlich: _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

(Bitte schildern Sie in einigen kurzen Sätzen, worauf sich Ihre Annahme einer Rechts- oder Pflichtenverletzung gründet:)

Zur Bescheinigung meines Vorbringens schließe ich an:

☐	(Urkunden-)Kopien wie Briefe, Computerausdrucke, Screenshots etc. (Anzahl der Beilagen : _ _ _ _ _ _ _)
☐	Sonstiges, nämlich: _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Ich ersuche die Datenschutzbehörde, mein Vorbringen zu prüfen und mich über die unternommenen Schritte zu informieren.

Datum:

Unterschrift: .....

.....

Folgenden Hinweis sollten Sie bitte beachten:

Gegen Personen, die Identitäten fälschen oder mutwillig (ohne Grund und Anlass, zur „Beschäftigung“ der Behörde) Beschwerden einbringen, wird straf- und verfahrensrechtlich (Mutwillensstrafe bis zu Euro 726,--) vorgegangen.

Anhang 4 – Formular für eine Auskunftsbeschwerde

Die Datenschutzbehörde empfiehlt auf ihrer Webseite[452] die Verwendung des nachfolgenden Formulars, um eine Verletzung des § 31 DSG geltend zu machen:

Beschwerde an die Datenschutzbehörde
(Auskunftsrecht, § 31 Abs. 1 DSG 2000)

Stand: 4. Juli 2016

Beschwerdeführer:

Name: .....

Anschrift, Straße: .....

Anschrift, Postleitzahl, Ort: .....

E-Mail-Adresse: .....

Telefon: .....

Fax: .....

Ich ersuche versandbereite Dokumente entsprechend Zustellgesetz unmittelbar elektronisch an folgende E-Mail-Adresse auszufolgen:

Fettgedruckte Angaben werden **unbedingt** benötigt. Nach dem Gesetz können Anbringen auf jede technisch mögliche Weise eingebracht werden, also nicht nur per Post sondern auch per Fax oder E-Mail. Jede Nachricht reist aber auf Gefahr des Senders, was bedeutet, dass Sie im Streitfall belegen müssen, dass die Nachricht den richtigen Empfänger erreicht hat. Die Datenschutzbehörde behält es sich aber vor, bei Anbringen ohne Unterschrift (betrifft insbesondere E-Mails ohne elektronische Signatur) bei Zweifel zur Klärung der Identität eine unterschriebene Bestätigung des Senders zu verlangen. Daher – sowie für Zwecke der Zustellung nachweispflichtiger Sendungen (RSa- und RSb-Briefe) – ist die Angabe einer Postadresse (kein Postfach!) notwendig. Andere Korrespondenz kann gerne auf elektronischem Wege erfolgen. Durch Gebrauch von E-Mail oder Fax stimmen Sie nach dem Gesetz auch dem Empfang von Nachrichten auf diesem Wege zu. Die Datenschutzbehörde weist Sie darauf hin,

[452] https://www.dsb.gv.at/documents/22758/115215/Druckformular_Auskunftsbeschwerde_07-2016.pdf/dbcadcfa-b470-44e7-8161-f6e405173557, abgerufen am 12. Oktober 2016.

dass diese Beschwerde sowie alle Ihre Eingaben dem Beschwerdegegner zur Kenntnis gebracht werden müssen.

Bitte schicken Sie Ihre Eingabe nur einmal! Bitte ☒ ankreuzen!

An die Datenschutzbehörde
Hohenstaufengasse 3
1010 Wien
REPUBLIK ÖSTERREICH

- via Fax 53115 / 202690
- via E-Mail dsb@dsb.gv.at

Beschwerde wegen Verletzung des Rechts auf Auskunft über eigene personenbezogene Daten gemäß § 26 DSG 2000 im

☐	Privaten Bereich (Beschwerdegegner ist zB Unternehmen, Privatperson, Verein, politische Partei)
☐	Öffentlichen Bereich (Beschwerdegegner ist zB eine Behörde, amtliche Dienststelle, Gemeinde, Kammer, gesetzlich anerkannte Kirche oder Religionsgesellschaft)

gegen den Auftraggeber (Beschwerdegegner):

Name (Firma): .....

Adresse: .....

DVR-Nr. (falls vergeben und bekannt): .....

------- ab hier bitte eine der Beschwerdevarianten wählen ------

Variante A: Das Auskunftsbegehren wurde nicht beantwortet:

Das Auskunftsbegehren wurde gestellt:

☐	per Post mit eingeschriebenem Brief
☐	per Post mit gewöhnlichem Brief

☐	per einfacher E-Mail
☐	per E-Mail-Attachment (Scan mit Wiedergabe einer Unterschrift)
☐	per E-Mail mit sicherer elektronischer Signatur
☐	per Fax
☐	auf folgende sonstige Weise: _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Ich habe das Auskunftsbegehren am _ _ _ _ _ _ _ _ _ _ _ _ an den Auftraggeber geschickt.

Bitte beachten Sie, dass eine Beschwerde wegen Verletzung des Auskunftsrechts kann erst erhoben werden, wenn nicht innerhalb der gesetzlichen Frist (**8 Wochen ab Eingang beim Auftraggeber**) Auskunft erteilt wurde oder behauptet wird, dass die erteilte Auskunft unvollständig oder unrichtig ist. Ein an die Datenschutzbehörde an Stelle des Auftraggebers gerichtetes Auskunftsersuchen ist ebenso unzulässig wie zwecklos.

War das Auskunftsbegehren auf bestimmte Datenanwendungen beschränkt?

☐	Ja, auf folgende: _
☐	Nein

Welchen Identitätsnachweis haben Sie dem Auftraggeber erbracht?

☐	Kopie eines amtlichen Lichtbildausweises
☐	Sonstiger Identitätsnachweis, nämlich: _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Hat der Auftraggeber um Ihre Mitwirkung ersucht oder bestimmte Auskünfte von Ihnen verlangt?

☐	Nein
☐	Ja, nämlich folgendes: _

Variante B: das Auskunftsbegehren wurde beantwortet, ich halte die Auskunft aber für

☐	unvollständig
☐	unrichtig

Dafür führe ich folgende Gründe an:

------- ab hier bitte wieder in jedem Fall ausfüllen -------

Als Beweismittel für mein Vorbringen schließe ich an:

☐	Kopie meines Auskunftsbegehrens
☐	Kopie des Aufgabescheins der Post
☐	Sonstige Korrespondenz mit dem Auftraggeber
☐	Kopie der erhaltenen Auskunft
☐	Sonstiges, nämlich: _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

Folgende weitere Beweismittel kann ich anführen:

☐	Meine Einvernahme als Partei
☐	Weitere Beweispersonen (Zeugen, bitte Namen und möglichst eine Adresse, an der die Person geladen werden kann, angeben): _
☐	Sonstiges, nämlich: _

Antrag an die Datenschutzbehörde:

Durch das Verhalten des Beschwerdegegners erachte ich mich in meinem Recht auf Auskunft gemäß § 26 Abs. 1 DSG 2000 verletzt. Ich beantrage,

☐ bei Beschwerde gegen Auftraggeber des öffentlichen Bereichs	die Datenschutzbehörde möge mit Bescheid diese Rechtsverletzung feststellen.
☐ bei Beschwerde gegen Auftraggeber des privaten Bereichs	die Datenschutzbehörde möge mit Bescheid ☐ diese Rechtsverletzung feststellen ☐ und dem Auftraggeber des privaten Bereichs auf Antrag zusätzlich die Reaktion auf das Auskunftsbegehren in jenem Umfang auftragen, der erforderlich ist, um die festgestellte Rechtsverletzung zu beseitigen.

Datum:

Unterschrift: .....

.....

Folgende Hinweise sollten Sie bitte beachten:

Gegen Personen, die Identitäten fälschen oder mutwillig (ohne Grund und Anlass, zur „Beschäftigung“ der Behörde) Beschwerden einbringen, wird straf- und verfahrensrechtlich (Mutwillensstrafe bis zu Euro 726,--) vorgegangen.

Literaturverzeichnis

Agentur der Europäischen Union für Grundrechte, & Europarat. (2014). Handbuch zum Europäischen Datenschutzrecht. Luxemburg: Amt für Veröffentlichungen der Europäischen Union.

Anspruch auf Auskunftserteilung nach dem DatenschutzG: Inhalt, Aktiv- und Passivlegitimation. (1986). Juristische Blätter, S 663f.

Anwendungsbereich des KSchG / Unzulässige Vertragsklauseln. (1999). Österreichisches Recht der Wirtschaft, S 458f.

Artikel-29-Datenschutzgruppe. (2004). Stellungnahme 4/2004 zum Thema Verarbeitung personenbezogener Daten aus der Videoüberwachung (WP 89).

Auer, M. (2011). Das Grundrecht auf Datenschutz im Unternehmen. Wien: Verlag Österreich.

Auskunft über Daten - Verweigerung ideeller Schaden? (1989). Wirtschaftsrechtliche Blätter, S 66f.

Auskunftsanspruch des Überwachten gegen Privatdetektiv? (2014). Österreichisches Recht der Wirtschaft, S 398.

Auskunftspflicht nach § 25 Datenschutzgesetz. (2000). ecolex, S 578.

Auskunftsrecht gegenüber Behörde - Bekanntgabe der Identität des Auskunftswerbers. (1992). EDV & Recht, S 191-194.

Bauer, L. & Reimer, S. (2009). Grundrecht auf Datenschutz. Handbuch Datenschutzrecht. Wien: Facutas.wuv Universitätsverlag.

Bednar, K. (1980). Rechtliche Probleme des Datenschutzgesetzes. Österreichische Juristen-Zeitung, S 281(282).

Bundesministerium des Innern, (13. Oktober 2016). Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Datenschutz-Grundverordnung und zur Umsetzung der Richtlinie (EU) 2016/680. Von https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/09/Entwurf-ABDSG-E-08.2016.pdf abgerufen

Bydlinski, P. (2014). Verbotene Überwachung durch einen Detektiv: Nur Unterlassungs- oder auch Auskunftspflichten? Österreichische Juristen Zeitung, S 744-746.

Dammann, U., & Simitis, S. (1997). EG-Datenschutzrichtlinie : Kommentar. Baden-Baden: Nomos-Verlagsgesellschaft.

Datenschutz: "Adreßverwaltung". (1993). ecolex, S 380.

Datenschutz: Umfang und Inhalt der Auskunftspflicht. (1986). Österreichisches Recht der Wirtschaft, S 306-308.

Datenschutzbehörde. (2015). Datenschutzbericht 2014. Wien: BM.I Digitalprintcenter.

Datenschutzbehörde. (2015). DSB Newsletter 2/2015. Wien: Österreichische Datenschutzbehörde.

Datenschutzbehörde. (2016). Datenschutzbericht 2015. Wien: BM.I Digitalprintcenter.

Datenschutzbehörde. (2. September 2016). Eingabe an die Datenschutzbehörde im Kontroll- und Ombudsmannverfahren. Von https://www.dsb.gv.at/at.gv.bka.liferay-app/documents/22758/115215/Druckformular_Ombudsmanneingabe_07-2016.pdf/9260b511-52b5-4bc7-bfc2-e2faa3c2ec44 abgerufen

Datenschutzbehörde. (2. September 2016). Ersuchen um Auskunft gemäß § 26 DSG 2000. Von https://www.dsb.gv.at/documents/22758/115215/Druckformular-Ersuchen_um_Auskunft_Par_26_DSG.pdf/b285b27a-278b-4dc2-8113-61a587fe5c61 abgerufen

Datenschutzbehörde. (9. August 2016). Formular für eine Auskunftsbeschwerde. Von http://www.dsb.gv.at/DocView.axd?CobId=30482 abgerufen

Datenschutzbehörde. (30. September 2016). Rechte der Betroffenen. Von https://www.dsb.gv.at/rechte-der-betroffenen abgerufen

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. (2016). Datenschutz-Grundverordnung. Bonn: Appel & Klinger Druck und Medien GmbH.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, (12. September 2016). Datenschutz-Wiki des BfDI. Von https://www.bfdi.bund.de/bfdi_wiki/index.php/Auskunftsrecht abgerufen

Dohr, W., Pollirer, H.-J., Weiss, E. M., & Knyrim, R. (2002). Datenschutzrecht² (20. Ergänzungslieferung, Juli 2016). Wien: Manz'sche Verlags- und Universitätsbuchhandlung GmbH.

Drobesch, H., & Grosinger, W. (2000). Das neue österreichische Datenschutzgesetz. Wien: Juridica-Verlag.

Drobesch, H., & Grosinger, W. (2000). Das neue österreichische Datenschutzgesetz - Datenschutzgesetz, Verordnungen, datenschutzrechtliche Bestimmungen, mit ausführlichen Erläuterungen. Wien: Manz Crossmedia GmbH & Co KG.

Duschanek, A. (2000). Neuerungen und offene Fragen im Datenschutzgesetz 2000. Verwaltung aktuell, S 526 (534).

Duschanek, A., & Rosenmayr-Klemenz, C. (2000). Datenschutzgesetz 2000 - Gesetzestext samt Einführung und Kurzkommentag. Wien: MANZ CROSSMEDIA GmbH & Co KG.

Ennöckl, D. (2010). Die DSG-Novelle 2010. Österreichische Juristen Zeitung, S 293 (295).

Erläuterungen zur RV 1613 der XX. GP (Bundesgesetz über den Schutz personenbezogener Daten - Datenschutzgesetz 2000). (1999).

Erläuterungen zur RV 1618 der XXIV. GP (Verwaltungsgerichtsbarkeits-Novelle 2012). (2012).

Erläuterungen zur RV 472 der XXIV. GP.

Erläuterungen zur RV 742 der XXI. GP (2. Euro-Umstellungsgesetz - Bund). (2001).

Gärtner, S. (2011). Harte Negativmerkmale auf dem Prüfstand des Datenschutzrechts (Dissertation). Hamburg: Dr. Kovač.

Gerhartl, A. (2014) Kein Auskunftsrecht bei Videoüberwachung?. ecolex, S 1112-1114.

Grabenwarter, C. (2009). Europäische Menschenrechtskonvention - ein Studienbuch. Wien: Manz'sche Verlags- und Universitätsbuchhandlung GmbH.

Jahnel, D. (2008). Auskunftsrecht und Identitätsnachweis. jusIT, S 225.

Jahnel, D. (2008). Keine Feststellung einer Rechtsverletzung bei verspäteter Auskunft. jusIT, S 72.

Jahnel, D. (28. August 2009). VwGH: Auskunftsrecht auch hinsichtlich nicht direkt suchbarer Daten. jusIT, S 153.

Jahnel, D. (2009). VwGH: Auskunftsrecht hinsichtlich Abfragen und Übermittlungen aus dem Abgabeninformationssystem. jusIT, S 152.

Jahnel, D. (2010). Datenschutzrecht - Grundrecht auf Datenschutz, Zulässigkeitsprüfung, Betroffenenrechte, Rechtsschutz. Wien: Jan Sramek Verlag KG.

Jahnel, D., & Knyrim, R. (2008). Willkürliche Abweisung eines Auskunftsbegehrens - Auskunftspflicht bezüglich aller vorhandenen Daten. jusIT, S 25f.

Knyrim, R. (2016). Datenschutz-Grundverordnung - Das neue Datenschutzrecht in Österreich und der EU. Wien: Manz'sche Verlags- und Universitätsbuchhandlung GmbH.

Knyrim, R. (2015). Datenschutzrecht³ - Praxishandbuch für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmen, Outsourcen, Werben uvm. Wien: Manz'sche Verlags- und Universitätsbuchhandlung GmbH.

Kotschy, W. (2008). Datenschutzrechtliche Fragen der Videoüberwachung. In A. Bammer, G. Holzinger, M. Vogl, & G. Wenda, Rechtsschutz Gestern - Heute - Morgen / Festgabe Machacek/Matscher. Graz: Neuer Wissenschaftlicher Verlag.

Landgericht-Berlin. (17. Dezember 2015). Landgericht Berlin 17.12.2015, 20 O 172/15. Von https://www.berlin.de/gerichte/presse/pressemitteilungen-der-ordentlichen-gerichtsbarkeit/2016/20-o-172-15_urteil-vom-17-12-2015.pdf abgerufen

Löffler, M. (2015). (K)Ein Auskunftsrecht bei (nicht ausgewerteten) Videoüberwachungen. Eine Besprechung von VwGH 29. 10. 2014, 2013/01/0127, jusIT, S 67-73.

Molterer, W., & Scheibner, H. (26. Jänner 2005). IA 515 BlgNR XXII. GP.

Öhlinger, T.; & Eberhard, H. (2016). Verfassungsrecht. Wien: facultas Universitätsverlag.

Passadelis, N., Rosenthal, D. & Thür, H. (2015). Datenschutzrecht - Beraten in Privatwirtschaft und öffentlicher Verwaltung. Basel: Helbing Lichtenhahn Verlag.

Preiß, T. (2015). Die Bedeutung der Risikoanalyse für den Rechtsschutz bei automatisierten Verwaltungsstrafverfahren (Dissertation). Wien.

Rechtsinformationssystem im Bundeskanzleramt. (27. Mai 2016). Bundesgrundsatzgesetz vom 15. Mai 1987 über die Auskunftspflicht der Verwaltung der Länder und Gemeinden (Auskunftspflicht-Grundsatzgesetz). Von https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000915&ShowPrintPreview=True abgerufen

Richtlinie 95/46/EG des Europäischen Parlaments und des Rats vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. (24. Oktober 1995).

Schmidl, M. (2014). Das datenschutzrechtliche Recht auf Auskunft – ein Überblick. Zeitschrift für Informationsrecht, S 21-26.

Schrems, M. (25. Mai 2016). europe vs. facebook. Von http://www.europe-v-facebook.org/DE/Anzeigen/anzeigen.html abgerufen

Schweizer, R. J. (2015). Geschichte und Zukunft des Datenschutzrechts. In N. Passadelis, D. Rosenthal, & H. Thür, Datenschutzrecht / Beraten in Privatwirtschaft und öffentlicher Verwaltung. Basel: Helbing Lichtenhahn Verlag.

Stärker, L. (2008). Datenschutzgesetz. Wien: Verlag Österreich.

Stelzer, M. (2004). Datenschutz im Gentechnikrecht : Studie über den allfälligen Anpassungsbedarf der datenschutzrechtlichen Bestimmungen des Gentechnikgesetzes. Wien: Bundesministerium für Gesundheit u. Frauen, Sektion IV.

Stelzer, M., & Bernert, I. (2004). Datenschutz im Gentechnikrecht - Studie über den allfälligen Anpassungsbedarf der datenschutzrechtlichen Bestimmungen des Gentechnikgesetzes. Wien: Bundesministerium für Gesundheit und Frauen, Sektion IV.

Thanner, T. (2010). Datenschutzgesetz. Graz: Neuer Wissenschaftlicher Verlag.

Thiele, C. (2014). OGH: Kein Auskunftsanspruch gegen Detektiv über Auftraggeber. jusIT, S 140.

Thienel, K., & Singer, C. (1987). Zeitschrift für Verwaltung, S 257 (258).

Unzulässigkeit von AGB-Klauseln - Verstoß gegen das Transparenzgebot (I). (1999). ecolex, S 464f.

Verfassungsausschuss. 1024 der Beilagen zu den Stenographischen Protokollen des Nationalrates XIV. GP. Von https://www.parlament.gv.at/PAKT/VHG/XIV/I/I_01024/imfname_316411.pdf abgerufen

Verfassungsausschuss. (01. Juli 1999). 2028 der Beilagen zu den Stenographischen Protokollen des Nationalrates XX. GP, Bericht des Verfassungsausschusses.

von Danwitz, T. (2015). Die Grundrechte auf Achtung der Privatsphäre und auf Schutz personenbezogener Daten, Datenschutz und Datensicherheit, S 581(584f).

Judikaturverzeichnis

Bundesverwaltungsgericht

BVwG 17.11.2015, W214 2014069-1/15E.

BVwG 3.12.2015, W214 2113213-1.

Datenschutzbehörde

DSB 29.1.2014, DSB-K215.309/0001-DSB/2014.

DSB 13.3.2014, DSB-D121.220/0005-DSB/2014.

DSB 23.5.2014, DSB-D213.131/0002-DSB/2014.

DSB 22.8.2014, DSB-D215.463/0006-DSB/2014.

DSB 5.9.2014, DSB-D122.105/0015-DSB/2014.

DSB 24.9.2014, DSB-D121.891/0002-DSB/2014.

DSB 1.10.2014, DSB-D122.020/0012-DSB/2014.

DSB 27.10.2014, DSB-D122.215/0004-DSB/2014.

DSB 28.11.2014, DSB-D215.548/0007-DSB/2014.

DSB 3.3.2015, DSB-D122.272/0004-DSB/2014.

DSB 3.3.2015, DSB-D122.273/0002-DSB/2015.

DSB 9.3.2015, DSB-D122.299/0003-DSB/2015.

DSB 11.3.2015, DSB-D122.319/0002-DSB/2015.

DSB 30.3.2015, DSB-D215.611/0003-DSB/2014.

DSB 1.4.2015, DSB-D215.529/0002-DSB/2015.

DSB 1.7.2015, DSB-D215.814/0003-DSB/2015.

DSB 16.7.2015, DSB-D122.349/0004-DSB/2015.

DSB 10.3.2016, DSB-D122.322/0001-DSB/2016.

DSB 15.4.2016, DSB-D122.418/0002-DSB/2016.

DSB 12.5.2016, DSB-D122.515/0004-DSB/2016.

DSB 15.7.2016, DSB-D122.453/0008-DSB/2016.

Datenschutzkommission

DSK 27.4.2000, 120.694/4-DSK/00.

DSK 31.8.2000, 120.701/3-DSK/00.

DSK 10.11.2000, 120.707/7-DSK/00.

DSK 23.3.2001, K210.380/001-DSK/2001.

DSK 24.4.2001, K120.737/002-DSK/2001.

DSK 24.4.2001, K202.010/002-DSK/2001.

DSK 21.8.2001, K120.734/014-DSK/2001.

DSK 23.11.2001, K120.748/022-DSK/2001.

DSK 26.2.2002, K120.760/004-DSK/2002.

DSK 26.2.2002, K120.783/004-DSK/2002.

DSK 4.6.2002, K120.810/005-DSK/2002.

DSK 20.8.2002, K120.800/010-DSK/2002.

DSK 23.8.2002, K120.819/003-DSK/2002.

DSK 3.9.2002, K120.790/010-DSK/2002.

DSK 11.10.2002, K120.814/008-DSK/2002.

DSK 25.3.2003, K120.744/001-DSK/2003.

DSK 1.7.2003, K120.698/002-DSK/2003.

DSK 1.7.2003, K120.842/009-DSK/2003.

DSK 1.7.2003, K501.349-040/003-DVR/2003.

DSK 2.9.2003, K120.743/004-DSK/2003.

DSK 12.9.2003, K202.028/006-DSK/2003.

DSK 14.11.2003, K120.819/006-DSK/2003.

DSK 14.11.2003, K120.871/004-DSK/2003.

DSK 20.1.2004, K120.888/001-DSK/2004.

DSK 27.2.2004, K120.761/0002-DSK/2004.

DSK 27.2.2004, K120.867/0001-DSK/2004.

DSK 12.3.2004, K120.892/0003-DSK/2004.

DSK 4.5.2004, K120.905/0008-DSK/2004.

DSK 18.5.2004, K120.899/0004-DSK/2004.

DSK 18.5.2004, K211.496/0003-DSK/2004.

DSK 25.6.2004, K120.877/0017-DSK/2004.

DSK 3.8.2004, K120.921/0006-DSK/2004.

DSK 8.10.2004, K120.826/0002-DSK/2004.

DSK 12.11.2004, K120.902/0017-DSK/2004.

DSK 16.11.2004, K120.959/0009-DSK/2004.

DSK 7.12.2004, K120.928/0009-DSK/2004.

DSK 14.1.2005, K120.970/0002-DSK/2005.

DSK 15.2.2005, K120.981/0002-DSK/2005.

DSK 11.3.2005, K120.969/0002-DSK/2005.

DSK 11.3.2005, K120.991/0006-DSK/2005.

DSK 5.4.2005, K120.873/0003-DSK/2005.

DSK 5.4.2005, K120.972/0004-DSK/2005.

DSK 5.4.2005, K120.986/0008-DSK/2005.

DSK 22.4.2005, K120.879/0003-DSK/2005.

DSK 20.5.2005, K120.862/0011-DSK/2005.

DSK 20.5.2005, K120.897/0003-DSK/2005.

DSK 20.5.2005, K120.908/0009-DSK/2005.

DSK 20.5.2005, K120.983/0009-DSK/2005.

DSK 7.6.2005, K120.912/0008-DSK/2005.

DSK 7.6.2005, K120.976/0003-DSK/2005.

DSK 7.6.2005, K121.008/0007-DSK/2005.

DSK 21.6.2005, K120.839/0005-DSK/2005.

DSK 30.6.2005, K120.977/0005-DSK/2005.

DSK 30.6.2005, K121.015/0009-DSK/2005.

DSK 2.8.2005, K121.034/0006-DSK/2005.

DSK 2.8.2005, K121.038/0006-DSK/2005.

DSK 27.9.2005, K073.025/0007-DSK/2005.

DSK 11.10.2005, K121.036/0014-DSK/2005.

DSK 16.12.2005, K121.049/0023-DSK/2005.

DSK 5.4.2006, K202.046/0012-DSK/2006.

DSK 31.5.2006, K121.108/0008-DSK/2006.

DSK 31.5.2006, K121.133/0007-DSK/2006.

DSK 28.6.2006, K121.075/0013-DSK/2006.

DSK 9.8.2006, K121.102/0012-DSK/2006.

DSK 9.8.2006, K121.109/0006-DSK/2006.

DSK 26.9.2006, K121.150/0014-DSK/2006.

DSK 29.9.2006, K213.000/0005-DSK/2006.

DSK 11.10.2006, K121.214/0006-DSK/2006.

DSK 20.10.2006, K121.154/0014-DSK/2006.

DSK 20.10.2006, K121.155/0015-DSK/2006.

DSK 2.2.2007, K121.225/0001-DSK/2007.

DSK 21.3.2007, K121.245/0009-DSK/2007.

DSK 21.3.2007, K121.255/0005-DSK/2007.

DSK 21.3.2007, K121.258/0003-DSK/2007.

DSK 21.3.2007, K507.515-023/0002-DVR/2007.

DSK 12.4.2007, K121.142/0003-DSK/2007.

DSK 7.5.2007, K121.280/0007-DSK/2007.

DSK 23.5.2007, K121.259/0013-DSK/2007.

DSK 15.6.2007, K121.285/0011-DSK/2007.

DSK 20.7.2007, K121.289/0006-DSK/2007.

DSK 10.8.2007, K073.028/0004-DSK/2007.

DSK 10.8.2007, K121.276/0014-DSK/2007.

DSK 3.10.2007, K121.278/0018-DSK/2007.

DSK 3.10.2007, K121.290/0015-DSK/2007.

DSK 24.10.2007, K121.273/0016-DSK/2007.

DSK 12.12.2007, K121.324/0008-DSK/2007.

DSK 18.1.2008, K121.326/0002-DSK/2008.

DSK 18.1.2008, K121.327/0002-DSK/2008.

DSK 6.2.2008, K121.328/0003-DSK/2008.

DSK 29.2.2008, K121.334/0005-DSK/2008.

DSK 29.2.2008, K121.344/0002-DSK/2007.

DSK 29.2.2008, K121.362/0006-DSK/2008.

DSK 2.4.2008, K121.345/0005-DSK/2008.

DSK 25.4.2008, K121.340/0006-DSK/2008.

DSK 16.5.2008, K121.323/0007-DSK/2008.

DSK 16.5.2008, K121.353/0008-DSK/2008.

DSK 30.5.2008, K121.356/0005-DSK/2008.

DSK 26.9.2008, K121.381/0008-DSK/2008.

DSK 22.10.2008, K121.386/0009-DSK/2008.

DSK 22.10.2008, K121.387/0020-DSK/2008.

DSK 5.12.2008, K121.385/0007-DSK/2008.

DSK 5.12.2008, K121.410/0008-DSK/2008.

DSK 5.12.2008, K121.413/0011-DSK/2008.

DSK 21.1.2009, K121.407/0001-DSK/2009.

DSK 21.1.2009, K121.414/0003-DSK/2009.

DSK 21.1.2009, K121.415/0002-DSK/2009.

DSK 25.2.2009, K121.394/0006-DSK/2009.

DSK 25.2.2009, K121.427/0003-DSK/2009.

DSK 25.2.2009, K121.492/0004-DSK/2009.

DSK 20.3.2009, K121.493/0007-DSK/2009.

DSK 8.5.2009, K121.470/0007-DSK/2009.

DSK 5.6.2009, K121.488/0007-DSK/2009.

DSK 5.6.2009, K121.525/0004-DSK/2009.

DSK 10.7.2009, K121.495/0013-DSK/2009.

DSK 10.7.2009, K121.535/0004-DSK/2009.

DSK 18.9.2009, K121.514/0008-DSK/2009.

DSK 18.9.2009, K121.517/0020-DSK/2009.

DSK 18.9.2009, K121.521/0007-DSK/2009.

DSK 16.10.2009, K121.533/0017-DSK/2009.

DSK 18.11.2009, K121.526/0028-DSK/2009.

DSK 16.12.2009, K120.973/0015-DSK/2009.

DSK 16.12.2009, K121.541/0012-DSK/2009.

DSK 16.12.2009, K121.550/0017-DSK/2009.

DSK 16.12.2009, K121.565/0006-DSK/2009.

DSK 20.1.2010, K120.939/0003-DSK/2010.

DSK 20.1.2010, K121.575/0002-DSK/2010.

DSK 20.1.2010, K121.578/0002-DSK/2010.

DSK 24.2.2010, K121.573/0003-DSK/2010.

DSK 19.3.2010, K121.593/0009-DSK/2010.

DSK 27.8.2010, K121.616/0012-DSK/2010.

DSK 27.8.2010, K121.628/0015-DSK/2010.

DSK 24.11.2010, K121.632/0008-DSK/2010.

DSK 24.11.2010, K121.646/0011-DSK/2010.

DSK 17.12.2010, K121.636/0010-DSK/2010.

DSK 15.4.2011, K121.673/0008-DSK/2011.

DSK 15.4.2011, K121.674/0008-DSK/2011.

DSK 18.5.2011, K121.652/0022-DSK/2011.

DSK 17.6.2011, K121.691/0015-DSK/2011.

DSK 20.7.2011, K121.704/0011-DSK/2011.

DSK 20.7.2011, K212.469/0008-DSK/2011.

DSK 2.9.2011, K121.715/0010-DSK/2011.

DSK 30.9.2011, K121.729/0008-DSK/2011.

DSK 21.10.2011, K121.733/0009-DSK/2011.

DSK 21.10.2011, K121.755/0005-DSK/2011.

DSK 24.2.2012, K121.751/0006-DSK/2012.

DSK 30.3.2012, K121.765/0008-DSK/2012.

DSK 25.5.2012, K121.791/0008-DSK/2012.

DSK 27.6.2012, K121.803/0008-DSK/2012.

DSK 14.12.2012, K121.877/0011-DSK/2012.

DSK 1.2.2013, K121.930/0004-DSK/2013.

DSK 20.2.2013, K121.906/0003-DSK/2013.

DSK 10.4.2013, K121.924/0006-DSK/2013.

DSK 30.4.2013, K121.955/0005-DSK/2013.

DSK 22.5.2013, K121.925/0007-DSK/2013.

DSK 22.5.2013, K121.935/0006-DSK/2013.

DSK 14.6.2013, K212.780/0004-DSK/2013.

DSK 19.7.2013, K121.698/0004-DSB/2013.

DSK 9.8.2013, K121.933/0029-DSK/2013.

DSK 6.9.2013, K121.605/0003-DSK/2013.

DSK 6.9.2013, K121.959/0010-DSK/2013.

DSK 6.9.2013, K121.964/0015-DSK/2013.

DSK 6.9.2013, K121.979/0014-DSK/2013.

DSK 25.10.2013, K122.023/0006-DSK/2013.

DSK 8.11.2013, K121.972/0008-DSK/2013.

DSK 22.11.2013, K121.974/0019-DSK/2013.

DSK 13.12.2013, K122.039/0008-DSK/2013.

DSK 13.12.2013, K202.128/0004-DSK/2013.

Europäischer Gerichtshof

EuGH 12.12.2013, C-486/12 (Vorabentscheidungsersuchen des Gerechtshof te 's-Hertogenbosch – Niederlande – in dem Verfahren auf Antrag von X).

EuGH 14.7.2014, C-141/12 (YS).

EuGH 1.10.2015, C-201/14 (Smaranda Bara u.a.).

EuGH 6.10.2015, C-362/14 (Schrems/Data Protection Commissioner).

Oberster Gerichtshof

OGH 10.7.1986, 6 Ob 12/85.

OGH 5.5.1988, 6 Ob 9/88.

OGH 25.2.1993, 6 Ob 6/93.

OGH 26.1.1995, 6 Ob 33/94.

OGH 27.1.1999, 7 Ob 170/98w.

OGH 28.10.1999, 3 Ob 132/99d.

OGH 28.6.2000, 6 Ob 148/00h.

OGH 13.4.2011, 15 Os 172/10y.

OGH 22.1.2014, 3 Ob197/13m.

Verfassungsgerichtshof

VfGH 27.9.1989, G6/89; G21/89; G23/89; G30/89; G67/89 = VfSlg 12151/1989.

VfGH 30.11.2005, B1158/03 - B200/04, B764/04, B574/04, B1325/04.

VfGH 2.10.2007, B227/05 = VfSlg 18230/2007.

VfGH 29.9.2012, B54/12ua = VfSlg 19673/2012.

VfGH 11.10.2012, B1369/11 = VfSlg 19691/2012.

VfGH 27.6.2014, G47/2012 ua = VfSlg 19892/2014.

VfGH 10.3.2015, G203/2014 ua.

Verwaltungsgerichtshof

VwGH 18.3.1992, 91/12/0007.

VwGH 23.2.2000, 2000/12/0026.

VwGH 21.10.2004, 2004/06/0086.

VwGH 22.11.2005, 2003/03/0041.

VwGH 28.3.2006, 2004/06/0125 = VwSlg 16873 A/2006.

VwGH 27.6.2006, 2005/06/0366.

VwGH 19.12.2006, 2005/06/0111 = VwSlg 17090 A/2006.

VwGH 23.1.2007, 2006/06/0039.

VwGH 6.6.2007, 2001/12/0004 = VwSlg 17215 A/2007.

VwGH 27.6.2007, 2007/04/0105.

VwGH 27.9.2007, 2006/06/0330.

VwGH 27.11.2007, 2006/06/0262.

VwGH 9.9.2008, 2004/06/0221 = VwSlg 17515 A/2008.

VwGH 28.4.2009, 2005/06/0194 = VwSlg 17680 A/2009.

VwGH 27.5.2009, 2007/05/0052 = VwSlg 17706 A/2009.

VwGH 8.9.2009, 2008/17/0152 = VwSlg 17729 A/2009.

VwGH 11.12.2009, 2009/17/0223.

VwGH 25.8.2010, 2009/03/0150.

VwGH 25.8.2010, 2009/03/0161.

VwGH 27.4.2012, 2010/17/0003 = VwSlg 18396 A/2012.

VwGH 15.11.2012, 2008/17/0096.

VwGH 28.5.2013, 2011/17/0066.

VwGH 29.10.2014, 2013/01/0127.

Zusammenfassung / Abstract

Zusammenfassung der Diplomarbeit „Auskunftsrecht nach § 26 Datenschutzgesetz 2000 in der Praxis inklusive Ausblick auf die Datenschutz-Grundverordnung (VO 2016/679) ab 25.05.2018“ von Joachim Galileo Fasching, LLB.oec., betreut durch Dr. Dietmar Jahnel

Der zentrale Aspekt der Diplomarbeit ist das datenschutzrechtliche Auskunftsrecht des Betroffenen gegenüber dem Auftraggeber einer Datenanwendung. Die Artikel 12 und 13 der Richtlinie 95/46/EG wurden im § 26 Datenschutzgesetz 2000 umgesetzt. Der Mehrwert liegt in einer ausführlichen und praxisnahen Erläuterung der Modalitäten des Auskunftsbegehrens. Eigene Erfahrungen leiten zur Durchsetzung des Auskunftsrechts bei der Datenschutzbehörde über, dabei wird insbesondere auf das Beschwerdeverfahren nach § 31 DSG eingegangen.

Die Arbeit behandelt neben Begriffsdefinitionen (ua „Auftraggeber“ und „Betroffener“ im Sinne des § 4 DSG) und höchstgerichtlicher Rechtsprechung (BVwG, OGH, VfGH, VwGH und EuGH) insbesondere die Bescheide und Empfehlungen der Datenschutzbehörde (vormals Datenschutzkommission). Abschließend folgt ein Ausblick auf die Veränderungen, die sich durch die ab dem 25. Mai 2018 geltende Datenschutz-Grundverordnung (Verordnung 2016/679) ergeben.

Abstract to diploma thesis „Request for information according to § 26 Austrian Data Protection Law 2000 in practice including preview on European General Data Protection Regulation (EU 2016/679) as from 25.05.2018“ from Joachim Galileo Fasching, LLB.oec., supervised by Dr. Dietmar Jahnel

The main content of the diploma thesis is the right of access (the processor has the right to be informed about the personal data the controller is processing about him in a personal data filing system) in the Austrian Data Protection Law 2000. The articles 12 and 13 of the directive 95/46/EC are transformed in § 26 DSG. The detailed and practically orientated expositions of structuring the right of access provide additional value. Own experiences lead over to the enforcement of the right of information through the Data Protection Authority, there you find more information concerning the appeal’s procedure (§ 31 DSG).

The thesis works on definitions (eg “controller” and “processor” in § 4 DSG), high courts’ decisions (BVwG, OGH, VfGH, VwGH and EuGH) and concentrates on regulations and recommendations of the Data Protection Authority. The diploma thesis is completed by an overview on the General Data Protection Regulation *(regulation 2016/679) which is applicable by 25 May 2018.*