www.jusletter-it.eu

Galileo Fasching

Auskunftsrecht nach § 26 DSG in der Praxis inklusive Ausblick auf die DS-GVO

The article's central aspect is the data protection related right of access by the data subject with respect to the ordering party of a data application. The articles 12 and 13 DPR have been implemented in § 26 DSG 2000. The added value lies within a detailed and practical explanation of the information request's modalities. Conclusively, a prospect on the changes resulting from the enforcement of the GDPR on 25 May 2018 is offered. (ah)

Category: Articles
Region: Austria
Field of law: Data Protection

Citation: Galileo Fasching, Auskunftsrecht nach § 26 DSG in der Praxis inklusive Ausblick auf die DS-GVO, in: Jusletter IT 24-Mai-2018

ISSN 1664-848X, https://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Inhaltsübersicht

1. Einleitung

[Rz 1] In der Diplomarbeit erfolgte nach den grundlegenden Definitionen (Grundrecht, räumlicher und sachlicher Anwendungsbereich mit Ausnahmen, personenbezogene Daten, Rollenverteilung, Datei und Datenanwendung) ein Überblick über die Umsetzung der Art. 12 und 13 der Richtlinie 95/46/EG (DSLR)[1] in § 26 Datenschutzgesetz 2000 (DSG). Der Schwerpunkt der gekürzten Fassung liegt auf den formalen und inhaltlichen Erfordernissen des Auskunftsbegehrens. An jenen Stellen, wo die Diplomarbeit ausführlicher auf die einzelnen Zusammenhänge eingeht, wird explizit auf die Vollversion verwiesen.

[Rz 2] Es ist darauf hinzuweisen, dass die hier hauptsächlich diskutierten Gesetzesstellen (DSRL, DSG) am 25. Mai 2018 von der Verordnung (EU) 2016/679 (DS-GVO)[2] abgelöst werden. Dennoch spielen die bisherigen Rechtsgrundlagen auch für das Verständnis der künftigen Gesetzeslage eine wesentliche Rolle, da sowohl das österreichische DSG i.d.F. Datenschutz-Anpassungsgesetz weiterhin in Art. 1 Abs. 3 und Art. 44 das Auskunftsrecht inhaltlich nahezu unverändert regelt als auch die DS-GVO auf die bisherige DSRL Bezug nimmt. Die Kernelemente der Auskunft (verarbeitete Datenkategorien, Zweck und Rechtsgrundlage der Verarbeitung, sowie Herkunft und Empfänger der Daten) sind beibehalten worden, durch die DS-GVO sind weitere Modalitäten (etwa Option der Auskunftserteilung via E-Mail, verpflichtende Information über Speicherdauer und Hinweis auf Beschwerderecht) ergänzt worden. Die auf Grundlage des § 26 DSG erstellte

[1] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281/31 vom 23. November 1995.

[2] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119/1 vom 4. Mai 2016.

Diplomarbeit ist weiterhin von zentraler Bedeutung, da sich für die Datenschutzbehörde (welche sich voraussichtlich stark an der bisherigen Rechtsprechung orientieren wird) sowie für die Unternehmen hinsichtlich des Auskunftsbegehrens gegenüber dem Betroffenen kaum etwas ändert. Im letzten Abschnitt dieses Beitrags («Ausblick auf die DS-GVO und DSG 2018») werden die Veränderungen zwischen der bisherigen und der neuen Rechtslage detailliert dargestellt.

[Rz 3] Anhand der bis zu dieser Stelle dargestellten Definitionen, Auslegungen und Entscheidungen ließ 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 DSG 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.
- Habe ich keinen Sitz oder Niederlassung in Österreich? Aufgrund des 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 DSG 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 DSG 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 DSG 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 i.V.m. Abs. 5 DSG 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 DSG 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 DSG 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 i.S.d. § 4 Z 6 und Z 9 DSG verarbeitet? Falls dies zutrifft, ist eine Reaktion auf Basis des in § 6 Abs. 1 DSG 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 i.S.d. § 4 Z 6 und Z 9 DSG verarbeite, da Echtzeitvideoüberwachungen, Akten, Aktenkonvolute u.dgl. nicht der Auskunftspflicht unterliegen. In den genannten Fällen besteht lediglich der Geheimhaltungsanspruch nach § 1 Abs. 1 DSG, nicht jedoch die Verpflichtung, Auskunft nach § 26 DSG zu erteilen.
- Werden Angaben, welche in öffentlichen Büchern einsehbar sind, abgefragt (z.B. Grundbuch)? Der Auskunftswerber ist in diesem Fall darauf hinzuweisen, dass diese Angaben entsprechend den besonderen Bestimmungen entgeltlich auszufolgen sind.

[Rz 4] Im nachfolgenden Abschnitt werden die inhaltlichen Erfordernisse des Auskunftsbegehrens näher analysiert.

2. Auslegung, Entscheidungen und Rechtsprechung zu § 26 DSG und praktische Hinweise

[Rz 5] Wie bereits eingangs dargestellt, sieht die Verfassungsbestimmung im § 1 Abs. 1 DSG die Geheimhaltung der personenbezogenen Daten vor. Der in § 1 Abs. 3 i.V.m. § 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.

[Rz 6] Die Besonderheit des Grundrechts auf Datenschutz ist die unmittelbare Drittwirkung – das bedeutet, dass dieses auch gegenüber Privaten durchsetzbar ist.[3] Ergänzend ist dabei darauf hinzuweisen, dass Art. 8 der Charta der Grundrechte der europäischen Union (GRC)[4] 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.

---

3 Kurt Bednar, Rechtliche Probleme des Datenschutzgesetzes, ÖJZ 1980, 281(282). Die Drittwirkung des Grundrechts auf Datenschutz wurde bereits im DSG 1978 normiert.

4 Charta der Grundrechte der europäischen Union, ABl. C 326/391 vom 30. März 2010, S. 393.

[Rz 7] 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. Schwerpunkte dieses Abschnitts stellen praktische Hinweise zur reibungslosen Auskunftserteilung sowie die Möglichkeit zur Beschwerde an die Datenschutzbehörde bei unvollständiger Auskunftserteilung dar.

[Rz 8] Das Bestehen des Auskunftsrechts ist nicht davon abhängig, dass der Betroffene eine Rechtswidrigkeit behauptet[5] oder Zweifel an der Richtigkeit der verwendeten Daten geltend macht.[6] Für das Auskunftsrecht und die Auskunftspflicht ist es unerheblich, ob der Betroffene seine Einwilligung zu dem Datenverkehr gegeben hat, über den er Auskunft begehrt.[7] Der Auskunftsanspruch ist jedoch durch das allgemeine Schikaneverbot[8] (Schädigungsabsicht bzw. unlautere Motive der Handlung überwiegend) begrenzt.[9] 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.[10]

2.1. Kostenersatz

[Rz 9] Die Auskunft ist gemäß § 26 Abs. 6 DSG unentgeltlich zu erteilen, wenn kumulativ folgende Voraussetzungen vorliegen:[11]

- Die Auskunft bezieht sich auf den aktuellen Datenbestand[12] 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.

[Rz 10] Details dazu finden sich ebenfalls in der vollständigen Version der Diplomarbeit.

2.2. Aufbau des Auskunftsbegehrens

[Rz 11] Besonderes Augenmerk sollten aus Sicht des Auskunftswerbers auf die formellen Kriterien des Auskunftsbegehrens gerichtet werden: Zunächst ist zu klären, in welcher Form (schrift-

5 Walter Dohr/Hans J. Pollirer/Ernst M. Weiss/Rainer Knyrim, Kommentar Datenschutzrecht, Manz Verlag, 2. Auflage, Wien 2017, 210/53 in § 26 Anm 5.

6 VwGH 19. Dezember 2006, 2005/06/0111 = VwSlg 17090 A/2006.

7 OGH 10. Juli 1986, 6 Ob 12/85, veröffentlicht in RdW 1986, 306–308 = JBl 1986, 663.

8 OGH 10. Juli 1986, 6 Ob 12/85, veröffentlicht in RdW 1986, 306–308 = JBl 1986, 663.

9 Dohr/Pollirer/Weiss/Knyrim (Fn. 5), 210/53 in § 26 Anm 5.

10 DSK 30. Mai 2008, K121.356/0005-DSK/2008.

11 Dohr/Pollirer/Weiss/Knyrim (Fn. 5), 210/57f in § 26 Anm 30.

12 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*»).

lich 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 Datenschutzkommission (DSK) von einem «rechtsgültigen» Auskunftsbegehren.[13] Es ist dabei jedenfalls erforderlich, dass aus der Anfrage hervorgeht, dass ein Auskunftsbegehren i.S.d. § 26 Abs. 1 DSG 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 (u.a. Reaktionspflicht, Erteilung einer Negativauskunft) geknüpft sind – im betreffenden Fall ging jedoch aus der Anfrage nicht hervor, dass es sich um ein Auskunftsbegehren handelte.[14]

2.3. Identitätsnachweis

[Rz 12] Es ist ratsam, das Auskunftsbegehren schriftlich (als eingeschriebenen Brief, Telefax[15], E-Mail[16]) 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.[17] Dohr/Pollirer/Weiss/Knyrim vertreten die Meinung, dass der zweifelsfreie Identitätsnachweis via Telefon, Fax oder E-Mail nicht erbracht werden könnte und das Auskunftsbegehren damit nicht den gesetzlichen Formvorschriften entspricht.[18] 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 DSG 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 Meldegesetz 1991 (MeldeG) keinen Wohnort.[19]

[Rz 13] Mit Zustimmung des Auftraggebers kann das Auskunftsbegehren gemäß § 26 Abs. 1 DSG 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.[20] Sollte der Auftraggeber der Meinung sein, dass der dem Auskunftsbegeh-

13 DSK 10. Juli 2009, K121.495/0013-DSK/2009.

14 DSK 22. Oktober 2008, K121.386/0009-DSK/2008; ebenso DSK 20. Januar 2010, K121.578/0002-DSK/2010; DSK 25. Februar 2009, K121.492/0004-DSK/2009.

15 VwGH 9. September 2008, 2004/06/0221 = VwSlg 17515 A/2008 = jusIT 2008/109, 225 mit Anm. Jahnel.

16 So Bescheidpraxis der DSK, u.a. in DSK 5. Juni 2009, K121.525/0004-DSK/2009; DSK 2. Februar 2007, K121.225/0001-DSK/2007; DSK 16. November 2004, K120.959/0009-DSK/2004.

17 VwGH 27. November 2007, 2006/06/0262.

18 Dohr/Pollirer/Weiss/Knyrim (Fn. 5), 210/53 f. in § 26 Anm 7.

19 DSK 29. Februar 2008, K121.344/0002-DSK/2007.

20 Dietmar Jahnel, Datenschutzrecht – Grundrecht auf Datenschutz, Zulässigkeitsprüfung, Betroffenenrechte, Rechtsschutz, Jan Sramek Verlag KG, Wien 2010, 375 in 7/19.

ren 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.[21]

[Rz 14] 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 nicht aus.[22] 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.[23] Die Zustellung (im öffentlichen Bereich beispielsweise in Form einer Zustellung zu eigenen Handen[24] oder über einen Zustelldienst[25]; im privaten Bereich beispielsweise in Form eines Einschreibens mit der Zusatzleistung «eigenhändig» oder «mit Rückschein»[26]) 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.[27] 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.[28] 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 i.S.d. Signaturgesetzes (SVG; in Kraft bis zum 30. Juni 2016) nachzuweisen.[29] Darunter fällt beispielsweise die Handysignatur. Der Auftraggeber hat die Eignung des

21 DSK 29. Februar 2008, K121.344/0002-DSK/2007; vgl. DSK 1. Februar 2013, K121.930/0004-DSK/2013.

22 VwGH 9. September 2008, 2004/06/0221 = VwSlg 17515 A/2008 = jusIT 2008/109, 225 mit Anm. Jahnel. Vgl. OGH 25. Februar 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.

23 DSK 10. Juli 2009, K121.495/0013-DSK/2009.

24 § 21 Zustellgesetz (ZustG).

25 § 35 ZustG.

26 Dohr/Pollirer/Weiss/Knyrim (Fn. 5), 210/54 in § 26 Anm. 8 mit Verweis auf die Tarifstruktur der Österreichischen Post AG: https://www.post.at/tarife_privat.php (alle Websites zuletzt besucht am 18. Mai 2018), Abschnitt «Einschreiben/Zusatzleistungen».

27 VwGH 9. September 2008, 2004/06/0221 = VwSlg 17515 A/2008 = jusIT 2008/109, 225 mit Anm. Jahnel.

28 DSK 2. Februar 2007, K121.225/0001-DSK/2007.

29 Jahnel (Fn. 20), 373 f. in 7/18.

vom Betroffenen gewählten Identitätsnachweises im Einzelfall zu prüfen.[30] 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.[31]

[Rz 15] 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.[32] 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.[33]

[Rz 16] 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[34]). Damit stehe dem Auftraggeber ein Instrument zur Verfügung, das Nachholen des Identitätsnachweises zu erwirken – und der datenschutzrechtliche Auftraggeber habe gemäß § 26 Abs. 4 DSG 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.[35] 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,[36] daher ist an den Nachweis der Bevollmächtigung durch den Betroffenen ein besonders strenger Maßstab anzulegen.[37] Es entfällt dabei auch die Pflicht des Auftraggebers, den Auskunftswerber zur nachträglichen Vorlage eines Identitätsnachweises aufzufordern.[38]

[Rz 17] 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 tatsächlich dienen könne. Auch der Umstand, dass auf einem Personalausweis ein Foto aufgebracht sei, könne wohl keinen wirkungsvollen Beitrag zur*

30 Jahnel (Fn. 20), 375 in 7/19.

31 DSK 2. September 2011, K121.715/0010-DSK/2011.

32 Dohr/Pollirer/Weiss/Knyrim (Fn. 5), 210/54 in § 26 Anm. 8.

33 DSK 21. März 2007, K121.258/0003-DSK/2007.

34 Siehe Begriff Mitwirkungsobliegenheit, 53.

35 VwGH 9. September 2008, 2004/06/0221 = VwSlg 17515 A/2008 = jusIT 2008/109, 225 mit Anm. Jahnel; ebenso DSK 10. April 2013, K121.924/0006-DSK/2013.

36 AB 2028 der Beilagen XX. GP, 3 zu § 26.

37 DSK 10. Juli 2009, K121.495/0013-DSK/2009.

38 DSK 25. Oktober 2013, K122.023/0006-DSK/2013; DSK 6. September 2013, K121.964/0015-DSK/2013.

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).[39]

[Rz 18] 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.[40]

[Rz 19] In einer aktuellen Entscheidung[41] 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 z.B. 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 des Telekommunikationsgesetzes 2003 (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 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.[42] 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.[43]

39 VwGH 9. September 2008, 2004/06/0221 = VwSlg 17515 A/2008 = jusIT 2008/109, 225 mit Anm. Jahnel.

40 DSK 2. Februar 2007, K121.225/0001-DSK/2007; DSK 2. August 2005, K121.034/0006-DSK/2005.

41 DSB 15. April 2016, DSB-D122.418/0002-DSB/2016.

42 Vgl. OGH 13. April 2011, 15 Os 172/10y.

43 DSB 15. April 2016, DSB-D122.418/0002-DSB/2016.

Insgesamt bleibt dabei jedoch offen, in welcher Form der «Nutzernachweis» gegenüber einem Telekommunikationsdiensteanbieter (bzw. weiteren ähnlich gelagerten Anbietern, wie z.B. 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.

2.4. Postversand

[Rz 20] 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.[44] 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 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.

2.5. Erteilung der Auskunft

[Rz 21] Im nächsten Abschnitt wird die Erteilung der Auskunft thematisiert. Das subjektive Recht auf Auskunft über eigene Daten gemäß § 26 Abs. 1 DSG umfasst den Anspruch, eine vollständige und richtige Auskunft im vom Gesetz umschriebenen Umfang über eigene Daten, die der Auftraggeber verarbeitet, vom Auftraggeber zu erhalten.[45] Weiters sind Informationen über die

44 Details dazu: https://www.post.at/privat_versenden_brief_oesterreich_zusatzleistungen.php#6359.

45 DSK 23. August 2002, K120.819/003-DSK/2002.

Herkunft (soweit verfügbar[46]), 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.[47]

2.5.1. Verarbeitete Daten

[Rz 22] Die Auskunft hat § 26 Abs. 1 DSG zufolge lediglich «verarbeitete Daten» i.S.d. § 4 Z 9 DSG 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 DSG kein «Ermitteln» und damit auch kein «Verarbeiten». Im konkreten Fall wurden Daten zu Kontrollzwecken abgefragt, aber nicht verarbeitet.[48] 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.[49] Dies hielt die DSB auch im Zusammenhang mit der Aufhebung der Vorratsdatenspeicherung[50] 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 DSG auch nicht zum Gegenstand der Feststellung gemacht werden, in diesem Recht in der Vergangenheit verletzt gewesen zu sein.[51]

[Rz 23] § 26 Abs. 1 DSG 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.[52] 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

46 Aus dem Gesetz geht keine ausdrückliche Pflicht hervor, die Herkunft von Daten zu dokumentieren. Auch besteht keine auf das DSG gegründete Pflicht, eine in den Jahren 2008 oder 2009 gesendete E-Mail zu archivieren und dem Beschwerdeführer in Kopie vorzulegen – so DSK 24. April 2012, K121.751/0006-DSK/2012.

47 Siehe Begriff Abkürzungen, 41.

48 DSK 20. Oktober 2006, K121.154/0014-DSK/2006.

49 Vgl. Heinz Drobesch/Walter Grosinger, Das neue österreichische Datenschutzgesetz, Manz Verlag, 2. Auflage, Wien 2000, Anm. 6 zu § 26, 204. Ebenso DSK 18. Januar 2008, K121.326/0002-DSK/2008: «[...] *darauf hinzuweisen, dass sich die Auskunftspflicht des § 26 DSG 2000* [...] *ausschließlich auf beim Auftraggeber (noch) gespeicherte Daten bezieht.*'

50 VfGH 27. Juni 2014, G 47/2012 u.a. = VfSlg 19892, Kundmachung BGBl. I Nr. 44/2014.

51 DSB 1. Oktober 2014, DSB-D122.020/0012-DSB/2014 bestätigt durch BVwG 17. November 2015, W214 2014069-1/15E.

52 DSK 28. Juni 2006, K121.075/0013-DSK/2006.

DSG 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 DSG in Frage kommen.[53] 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.[54] Der Auskunftsanspruch des Betroffenen umfasst nicht die Bekanntgabe, in welcher Form Daten konkret verarbeitet wurden (beispielsweise Abfragen, Benützen oder Ausgeben bzw. Ausdrucken von Daten).[55]

[Rz 24] 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.[56] 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 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.

[Rz 25] Für Protokolldaten, die ausschließlich durch sequentielle Suche (nicht automationsunterstütztes Lesen der Protokolle) aufgefunden werden können, besteht keine Auskunftsverpflichtung.[57] Der Auftraggeber müsste in diesem Fall einen unverhältnismäßigen Aufwand gemäß § 26 Abs. 2 DSG 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.[58] Reine Protokolldaten (z.B. zu welcher Uhrzeit wurde eine Eintragung vorgenommen) unterliegen ebenfalls nicht dem Auskunftsanspruch.[59]

53 DSK 23. August 2002, K120.819/003-DSK/2002.

54 DSK 25. Mai 2012, K121.791/0008-DSK/2012.

55 DSK 20. August 2002, K120.800/010-DSK/2002; VwGH 28. April 2009, 2005/06/0194 = VwSlg 17680 A/2009.

56 DSK 8. Oktober 2004, K120.826/0002-DSK/2004; DSK 7. Juni 2005, K120.912/0008-DSK/2005.

57 AB 2028 der Beilagen XX. GP, 3 zu § 26.

58 DSK 23. Mai 2007, K121.259/0013-DSK/2007.

59 DSK 2. August 2005, K121.038/0006-DSK/2005.

2.5.2. Allgemein verständliche Form

[Rz 26] Die im § 26 Abs. 1 DSG 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.[60] 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.[61] 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 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*»[62]. Auch verarbeitete Codes, deren Bedeutung dem Auftraggeber nicht mehr geläufig sein sollte, sind unter Offenlegung dieser Tatsache zu beauskunften.[63] 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 (u.a. sind Verfahren vor der DSB zwingend in deutscher Sprache zu führen[64]), und hindert Privatpersonen nicht daran, sich auch im Rechtsverkehr (etwa bei der Abfassung von Verträgen) im Konsens anderer Sprachen zu bedienen.[65]

[Rz 27] In einem Praxisfall bekam ich Zugriff auf Daten, die nicht verständlich aufbereitet waren. In diesem Datensatz wurden Metadaten von Telefongesprächen (Uhrzeit, Gesprächsdauer, gewählte Rufnummer u.v.m.) 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

60 DSK 5. April 2005, K120.986/0008-DSK/2005.

61 VwGH 27. Mai 2009, 2007/05/0052 = VwSlg 17706 A/2009, jusIT 2009/76, 153 mit Anm. Jahnel.

62 Dohr/Pollirer/Weiss/Knyrim (Fn. %), 210/55 in § 26 Anm. 17.

63 DSK 3. Oktober 2007, K121.290/0015-DSK/2007.

64 VwGH 23. Februar 2000, 2000/12/0026.

65 DSK 22. Mai 2013, K121.935/0006-DSK/2013.

bezieht, d.h. die Daten müssen für den Betroffenen in einer leicht lesbaren und einfach verständlichen Form aufbereitet werden.

[Rz 28] 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 wird.[66] Auch dauerhaft verarbeitete interne Personennummern, Personenkennzeichen und ähnliche Suchbegriffe sind dem Betroffenen der Vollständigkeit halber zu übermitteln[67] – m.E. fällt beispielsweise auch die Matrikelnummer eines Studenten unter diese Kategorie.

[Rz 29] 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.[68] In einem Praxisfall wurden von Seiten 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.

2.5.3. Konkrete Feldinhalte

[Rz 30] 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»[69]) wiedergegeben werden.[70] 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.[71] Das Auskunftsrecht nach § 26 DSG 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.[72] 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.[73] 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.

66 DSK 5. April 2005, K120.986/0008-DSK/2005.

67 DSK 12. November 2004, K120.902/0017-DSK/2004.

68 DSK 5. April 2005, K120.986/0008-DSK/2005.

69 DSK 27. Februar 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.

70 DSK 23. November 2001, K120.748/022-DSK/2001 und DSK 14. Dezember 2012, K121.877/0011-DSK/2012.

71 DSK 20. März 2009, K121.493/0007-DSK/2009.

72 DSK 18. Mai 2011, K121.652/0022-DSK/2011.

73 OGH 28. Oktober 1999, 3 Ob 132/99d = ecolex 2000, 578.

[Rz 31] Wie bereits zuvor zur Datenanwendung[74] ausgeführt, unterliegen der Auskunftspflicht nach § 26 DSG automationsunterstützt verarbeitete Daten sowie nach den Bestimmungen des § 58 DSG auch 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.[75] 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.[76]

2.5.4. Herkunft der Daten

[Rz 32] 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 (z.B. 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 DSG) treffen.[77] Dementsprechend sind beispielsweise der «Melder» von Bonitätsinformationen[78] 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 (u.U. auch unter welchen Modalitäten). Vor diesem Hintergrund ist ein überwiegendes Interesse des Beschwerdeführers oder Dritter an einer Geheimhaltung dieser Angaben nicht zu erkennen.[79]

[Rz 33] Sollte es dennoch nicht bzw. nur mit unverhältnismäßig hohem Aufwand möglich sein, die Herkunft der Daten zu eruieren, so kann eine Information diesbezüglich unterbleiben[80] – 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.[81] Der VfGH stellte fest, dass über vorhandene Daten, auch wenn sie nicht gespeichert werden mussten, grundsätzlich Auskunft zu geben ist.[82] Unklar ist, aus welchen Gründen das Wort «verfügbaren» vor Infor-

74 Siehe Begriff Datenanwendung, 14.

75 Dohr/Pollirer/Weiss/Knyrim (Fn. 5), 210/53 in § 26 Anm. 4.

76 DSK 25. Februar 2009, K121.427/0003-DSK/2009.

77 Dohr/Pollirer/Weiss/Knyrim (Fn. 5), 210/54 in § 26 Anm. 11.

78 DSK 3. Oktober 2007, K121.290/0015-DSK/2007.

79 VwGH 23. Januar 2007, 2006/06/0039 mit Verweis auf den zugrundeliegenden Bescheid DSK 16. Dezember 2005, K121.049/0023-DSK/2005.

80 DSK 12. November 2004, K120.902/0017-DSK/2004 und DSK 20. Mai 2005, K120.908/0009-DSK/2005 und DSK 10. August 2007, K121.276/0014-DSK/2007.

81 OGH 5. Mai 1988, 6 Ob 9/88; WBl 1989, 66. Vgl. JBl 1986, 663.

82 VfSlg 18.230/2007.

mationen 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.[83] 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.[84] 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.[85]

2.5.5. Empfänger bzw. Empfängerkreise von Übermittlungen

[Rz 34] 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 (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.[86]

[Rz 35] 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. [87] Der Empfängerkreis kann sich allerdings einerseits dadurch reduzieren, dass sich gemäß § 14 Abs. 3 DSG aus der Registrierung einer zu beauskunftenden Datenanwendung (bzw. aus einer zutreffenden Standard- oder Musteranwendung) ein «Empfängerkreis» ergibt, der keiner 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.[88] Der VfGH hält die Regelung des § 26 Abs. 1 DSG zur Auskunft über «*allfällige Empfänger oder Empfängerkreise von Übermittlungen*» auch unter dem Blickwinkel

83 ErlRV 472, BlGNR XXIV. GP, 11.

84 OGH 28. Oktober 1999, 3 Ob 132/99d = ecolex 2000, 578.

85 DSK 16. Dezember 2009, K121.550/0017-DSK/2009; ebenso DSK 22. November 2013, K121.974/0019-DSK/2013.

86 DSK 3. Oktober 2007, K121.290/0015-DSK/2007.

87 VwGH 19. Dezember 2006, 2005/06/0111 = VwSlg 17090 A/2006.

88 DSK 16. Dezember 2009, K120.973/0015-DSK/2009; VwGH 28. April 2009, 2005/06/0194 = VwSlg 17680 A/2009; ebenso DSK 17. Juni 2011, K121.691/0015-DSK/2011.

des Art. 18 des Bundes-Verfassungsgesetzes (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.[89]

[Rz 36] 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»[90] hierbei nicht denkbar, da diese Übermittlungsvorgänge jedenfalls rekonstruierbar sind.[91] 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.[92] 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 des Konsumentenschutzgesetzes [KSchG] normierte Transparenzgebot) für nichtig erklärt.[93]

[Rz 37] 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 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.[94] Die DSK sieht im Zusammenhang mit Gesundheitsdaten[95] und bei Bonitätsdaten[96] 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

89 VfGH 2. Oktober 2007, B227/05 = VfSlg 18230; siehe dazu die Anm. von Jahnel und Knyrim, jusIT 2008, 25.

90 OGH 5. Mai 1988, 6 Ob 9/88; WBl 1989, 66. Vgl. JBl 1986, 663.

91 OGH 10. Juli 1986, 6 Ob 12/85, veröffentlicht in RdW 1986, 306–308 = JBl 1986, 663.

92 Dohr/Pollirer/Weiss/Knyrim (Fn. 5), 210/54a in § 26 Anm. 13 und 14.

93 OGH 27. Januar 999, 7 Ob 170/98w; ecolex 1999, 464f = RdW 1999, 458. Näher dazu auch Rainer Knyrim, Datenschutzrecht – Praxishandbuch für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmen, Outsourcen, Werben uvm. Manz'sche Verlags- und Universitätsbuchhandlung GmbH, 3. Auflage, Wien 2015, 174–176 und 194.

94 VwGH 19. Dezember 2006, 2005/06/0111 = VwSlg 17090 A/2006 mit Verweis auf den zugrundeliegenden Bescheid DSK 15. Februar 2005, K120.981/0002-DSK/2005; ebenso DSK 2. September 2003, K120.743/004-DSK/2003.

95 DSK 3. Oktober 2007, K121.278/0018-DSK/2007.

96 U.a. VwGH 19. Dezember 2006, 2005/06/0111 = VwSlg 17090 A/2006; DSK 8. Mai 2009, K121.470/0007-DSK/2009; DSK 15. Februar 2005, K120.981/0002-DSK/2005; DSK 7. Mai 2007, K121.280/0007-DSK/2007; DSK 2. September 2003, K120.743/004-DSK/2003.

Datenvermietung durch einen Adressverlag und Direktmarketingunternehmen hingegen genügt die Anführung von «Werbetreibende» als Empfängerkreis.[97]

2.5.6. Verwendungszweck und Rechtsgrundlage

[Rz 38] Der Betroffene hat weiters gemäß § 26 Abs. 1 3. Satz DSG 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.[98] Ebenso ist die Rechtsgrundlage der Datenverwendung (Verarbeitung und Übermittlung der personenbezogenen Daten) Gegenstand der Auskunftserteilung. Diese «*gesetzliche Zuständigkeit bzw. rechtliche Befugnis*» ist i.S.d. §§ 7 ff. DSG zu beauskunften.[99] Im öffentlichen Bereich ergibt sich die Rechtsgrundlage aus der «gesetzlichen Zuständigkeit» i.S.d. § 7 Abs. 1 DSG, im privaten Bereich beruht die Rechtsgrundlage meist auf den Statuten, dem Gesellschaftsvertrag i.V.m. den Eintragungen im Firmenbuch oder auf dem Gewerbeschein i.V.m. dem Gewerberegister.[100] 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. DSG) geltend zu machen.[101] Hierbei liegt m.E. eine der besonderen Fallkonstellation der soeben zitierten Entscheidung zugrunde: Der Beschwerdeführer brachte darin vor, dass die 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 DSG (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 DSG (öffentliche Datenanwendung wie beispielsweise eine Online-Suchmaschine)[102] im Vordergrund. Das Widerspruchsrecht nach § 28 Abs. 1 DSG wird in der Praxis schwieriger durchsetzbar sein, da der Betroffene in diesem Fall überwiegende schutzwürdige Geheimhaltungsinteressen nachzuweisen hat.[103]

[Rz 39] Die klare Angabe von Zweck und Rechtsgrundlage der Datenverwendung ist ein obligatorischer Bestandteil der vollständigen datenschutzrechtlichen Auskunftserteilung.[104] Der Betrof-

97 DSK 14. Januar 2005, K120.970/0002-DSK/2005.

98 Anderer Ansicht jedoch Dohr/Pollirer/Weiss/Knyrim (Fn. 5), 210/55 in § 26 Anm. 15.

99 DSK 1. Juli 2003, K501.349-040/003-DVR/2003.

100 Dohr/Pollirer/Weiss/Knyrim (Fn. 5), 210/55 in § 26 Anm. 16.

101 DSK 5. April 2005, K120.972/0004-DSK/2005.

102 Diese Bestimmung wurde bereits als verfassungswidrig aufgehoben (vgl. VfGH 8. Oktober 2015, G264/2015), die Aufhebung tritt jedoch erst mit 31. Dezember 2016 in Kraft.

103 § 28 Abs. 1 DSG 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. September 2006, 6 Ob 167/06m).

104 DSK 23. November 2001, K120.748/022-DSK/2001 und DSK 14. Dezember 2012, K121.877/0011-DSK/2012.

fene 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.[105] 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.[106]

2.5.7. Dienstleister

[Rz 40] 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.[107]

2.5.8. Auskunftserteilung im Katastrophenfall

[Rz 41] Die Bestimmungen der § 48a Abs. 4 und 6 i.V.m. § 52 Abs. 1 Z 5 DSG 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 DSG genannte Zweckbestimmung soll klar stellen, dass Daten von Katastrophenopfern von den An-

105 DSK 21. März 2007, K121.255/0005-DSK/2007.

106 DSK 16. Mai 2008, K121.323/0007-DSK/2008.

107 DSK 6. Februar 2008, K121.328/0003-DSK/2008.

gehörigen nur zur persönlichen Information und um den Betroffenen Hilfe zu leisten verwendet werden dürfen, nicht aber für andere, z.B. kommerzielle Zwecke.[108]

2.6. Pflicht zur Reaktion

[Rz 42] Wie zuvor bereits geschildert, hat der Auskunftswerber Anspruch[109] auf eine Antwort vom Auftraggeber, diese kann nach § 26 Abs. 1 5. Satz DSG auch in Form einer Negativauskunft erteilt werden.[110] 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[111] – erst dann ist das Auskunftsbegehren i.S.d. § 26 Abs. 4 DSG als erfüllt anzusehen. Konsequenterweise sind im Falle einer Negativauskunft (keine Daten zum Auskunftswerber gespeichert) auch die durch den Auftraggeber herangezogenen Dienstleister nicht zu 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 DSG zu stützen[112].

[Rz 43] 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 §§ 863 f. des Allgemeinen bürgerlichen Gesetzbuches (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.[113] Mit Einverständnis des Betroffenen sind auch folgende Formen der Auskunftserteilung denkbar: Akteneinsicht, Abschrift, Ablichtung, automationsunterstützt (z.B. Hardcopy, Einsichtnahme über Bildschirm, Screenshots[114], E-Mail). Dabei ist, wie zuvor schon erwähnt, sicherzustellen, dass die Auskunft ausschließlich dem Auskunftswerber zukommt.[115]

2.7. Beschränkung der Auskunft

[Rz 44] Der Auskunftsanspruch ist in mehrfacher Hinsicht beschränkt, dabei ist gemäß § 1 Abs. 2 DSG 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

108 IA 515 BlGNR XXII. GP, 10.

109 Siehe Begriffe Auskunftsverweigerung, 52 und Pflicht zur Reaktion, 56.

110 ErlRV 472, BlGNR XXIV. GP, 11 und VwGH 27. Mai 2009, 2007/05/0052 = VwSlg 17706 A/2009, jusIT 2009/76, 153 mit Anm. Jahnel.

111 DSK 2. April 2008, K121.345/0005-DSK/2008; ebenso DSK 18. Januar 2008, K121.326/0002-DSK/2008 und DSK 20. Mai 2005, K120.897/0003-DSK/2005.

112 DSK 14. Dezember 1984, GZ 120.052 = ZfVB 1987, 257 (258).

113 DSK 23. Mai 2007, K121.259/0013-DSK/2007.

114 DSK 23. Mai 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.

115 Dohr/Pollirer/Weiss/Knyrim (Fn. 5), 210/55 in § 26 Anm. 19.

erkennbaren Rechtschutzinteresses[116] 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.[117] Soweit eine Datenanwendung von Gesetzes wegen durch den Betroffenen einsehbar ist, besteht lediglich das Einsichtsrecht nach § 26 Abs. 8 DSG, darüber hinaus besteht das Auskunftsrecht nach § 26 Abs. 1 DSG.[118] Der Betroffene hat keinen Anspruch auf konkrete Darstellung der Datenanwendung[119] oder auf Vorlage von Ausdrucken aus der Datenanwendung[120]. Fragen, wie beispielsweise «von wem Passwörter abgefragt wurden» oder «von wem die e-mail Adresse wieder eingerichtet wurde», sind ebenfalls nicht Gegenstand des Auskunftsrechts.[121] Sofern nicht der aktuelle Datenbestand Gegenstand des Auskunftsbegehrens ist, kann der Auftraggeber einen Kostenersatz vom Betroffenen verlangen.[122]

[Rz 45] § 26 Abs. 2 DSG 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.

[Rz 46] In der vollständigen Version der Diplomarbeit sind hierzu weitere Informationen enthalten (Schutz des Auskunftswerbers aus besonderen Gründen, überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten, öffentliche Interessen).

2.8. Mitwirkungspflicht des Auskunftswerbers

[Rz 47] Der Auskunftswerber hat gemäß § 26 Abs. 3 DSG am Auskunftsverfahren über Befragung in dem ihm zumutbaren Ausmaß mitzuwirken, um ungerechtfertigten und unverhältnismäßigen Aufwand beim Auftraggeber zu vermeiden. Weitere Details dazu sind der vollständigen Version der Diplomarbeit zu entnehmen.

2.9. Reaktionsfrist

[Rz 48] § 26 Abs. 4 DSG 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. Die vollständige Version der Diplomarbeit beinhaltet hierzu nähere Informationen.

---

116 Vgl. VwGH 19. Dezember 2006, 2005/06/0111 = VwSlg 17090 A/2006.

117 DSK 21. Januar 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. Mai 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.

118 ErlRV 472, BlGNR XXIV. GP, 11.

119 DSK 21. Juni 2005, K120.839/0005-DSK/2005.

120 DSK 2. August 2005, K121.038/0006-DSK/2005.

121 DSK 7. Juni 2005, K120.976/0003-DSK/2005.

122 Siehe Begriff Kostenersatz, 29.

2.10. Schema zur Auskunftserteilung

[Rz 49] 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 personenbezogene Daten des Betroffenen darzustellen. Sowohl das Formular zum Auskunftsbegehren der DSB als auch das von Knyrim empfohlene Musterschreiben zur Beantwortung des Auskunftsbegehrens 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[123]. 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.[124] Dies lässt sich schematisch darstellen (Rechtslage vor DS-GVO):

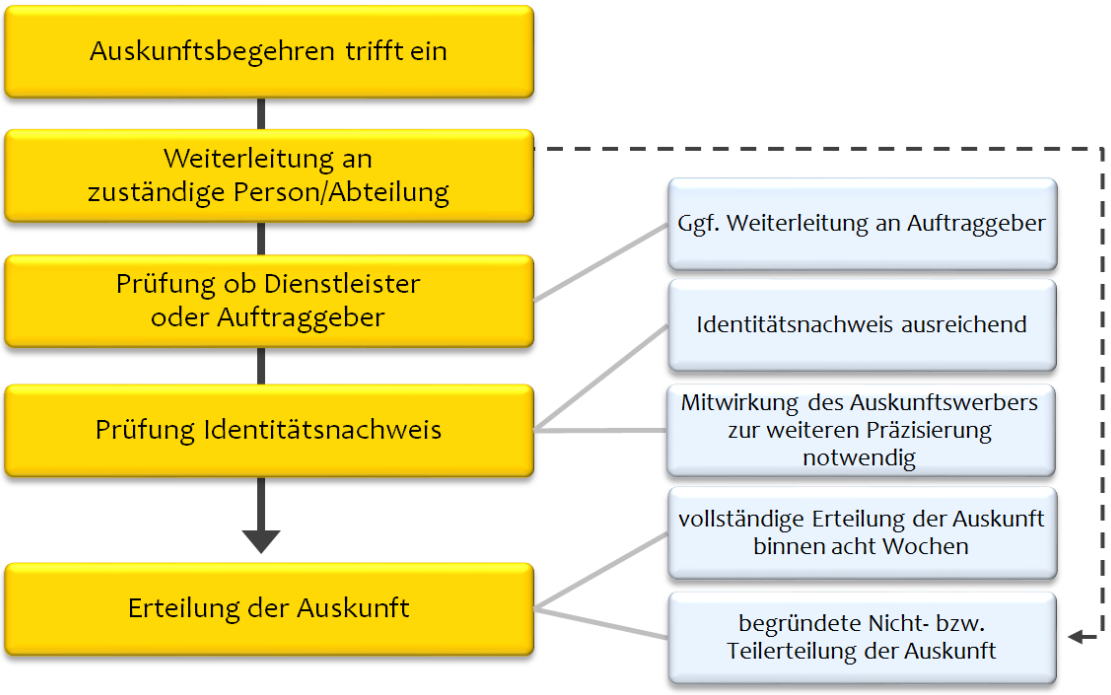

Abbildung 1: Schema zur Auskunftserteilung (erstellt von Joachim Galileo Fasching)

[Rz 50] In weiterer Folge wurde in der Diplomarbeit beschrieben, wie das Löschungsverbot auszulegen ist und welche weiteren Einsichtsrechte bestehen. Die besonderen Auskunftsrechte (automatisierte Einzelentscheidungen, Informationsverbundsysteme sowie Videoüberwachung) wurden näher beleuchtet. Das Auskunftsrecht in Deutschland und Schweiz hat zahlreiche Vor- bzw.

123 Knyrim (Fn. 93), 326.

124 Viktoria Haidinger, Die Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch (Art. 15–21 DSGVO), in: Rainer Knyrim (Hrsg.), Datenschutz-Grundverordnung – Das neue Datenschutzrecht in Österreich und der EU, Manz'sche Verlags- und Universitätsbuchhandlung GmbH, Wien 2016, 125 und 135.

Nachteile, welche überblicksmäßig analysiert wurden. Ergänzend wurde auf Rechtsschutz und Verwaltungsstrafrecht eingegangen. Die Diplomarbeit wurde mit einem Ausblick auf die Änderungen, die sich durch die DS-GVO ergeben, sowie nützlichen Vorlagen und Literaturempfehlungen abgerundet.

3. Ausblick auf die Datenschutz-Grundverordnung und DSG 2018

[Rz 51] Die DS-GVO trat am 25. Mai 2016 in Kraft, gilt ab 25. Mai 2018 und löst die bislang geltende DSRL ab. In weiterer Folge werden die wesentlichen Änderungen, die sich durch die Geltung der DS-GVO ab 2018 ergeben, skizziert. In Art. 12 ff. DS-GVO werden die Modalitäten für die Ausübung der Betroffenenrechte (insbesondere das Auskunftsrecht) geregelt, eng damit ist die Datenportabilität nach Art. 20 DS-GVO verknüpft. Art. 25 DS-GVO legt die Rahmenbedingung für Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen fest, Art. 55 DS-GVO enthält Strafbefugnisse, das One-Stop-Shop-Prinzip ist eine grundlegende Neuregelung, zudem wird mit Art. 68 DS-GVO ein «Europäischer Datenschutzausschuss» geschaffen und in Art. 83 Abs. 5 DS-GVO 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.

[Rz 52] ErwGr. 39 DS-GVO formuliert die Leitgedanken, die bei der Verarbeitung personenbezogener Daten zu berücksichtigen sind. Der Betroffene (vgl. Art. 4 Z 1 DS-GVO: 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 DS-GVO, andererseits sind damit auch Informationen über die Identität des Verantwortlichen (dabei ist m.E. das Impressum ausreichend[125]) 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.[126]

[Rz 53] 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

125 A.A. Ursula Illibauer, Informationsrecht und Modalitäten für die Ausübung der Betroffenenrechte, in: Knyrim (Fn. 124), 116.

126 Näheres dazu in Bundesbeauftragter für Datenschutz und Informationsfreiheit (BfDI), Datenschutz-Grundverordnung, Appel & Klinger Druck und Medien GmbH, Bonn 2016, 22 f.

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 DS-GVO hat der Verantwortliche ausdrücklich Kopien (E-Mails, Datenbankauszüge) der personenbezogenen Daten zur Verfügung zur stellen,[127] zudem sind gemäß Art. 15 Abs. 1 lit. d DS-GVO 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).[128] *Haidinger* Im Unterschied zum DSG kann der Betroffene künftig gemäß Art. 12 Abs. 1 DS-GVO 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 DS-GVO, Verwendung visueller Elemente wie Symbole, Icons u.dgl.) der Informationen entsprechend angepasst wird.

[Rz 54] Die Unentgeltlichkeit der Auskunftserteilung wird in Art. 12 Abs. 5 DS-GVO normiert. Demnach sind Informationen gemäß den Art. 13 und 14 DS-GVO sowie alle Mitteilungen und Maßnahmen gemäß den Art. 15 bis 22 und Art. 34 DS-GVO 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.[129] 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.

[Rz 55] Art. 11 DS-GVO 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 DS-GVO) oder einzuholen (ErwGr. 57 DS-GVO). Sofern der Verantwortliche nachweisen kann, dass er den Betroffenen nicht identifizieren kann, so entfällt dessen Auskunftsanspruch. Denkbar sind hierbei u.a. folgende Datenverarbeitungen: Dienstenutzung via Wertkarte (Telefonie, Internet), Gutscheine für Online-Angebote (z.B. Glücksspiel, Nutzung von Musik- und Videostreamingplattformen), Smart-Anwendungen (Smart Home/Meter, Cars, Watch, TV u.v.m. – 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

127 Bisher lehnte die DSB dies ausdrücklich ab: DSK 22. Mai 2013, K121.925/0007-DSK/2013.

128 Haidinger (Fn. 124), 127 f.

129 Haidinger (Fn. 124), 126.

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.[130] 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 DS-GVO).

[Rz 56] Als Frist für die Auskunftserteilung ist in Art. 12 Abs. 3 DS-GVO 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 DS-GVO) 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.

[Rz 57] Art. 20 DS-GVO normiert neben dem Auskunftsanspruch über die verarbeiteten personenbezogenen Daten die Möglichkeit der Datenübertragbarkeit von einem Verantwortlichen zu einem anderen 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.[131]

[Rz 58] 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 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 öster-

130 Illibauer (Fn. 125), 118.

131 Haidinger (Fn. 124), 134.

reichischem Verfassungsrecht, da der VfGH in ständiger Rsp. 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.[132] 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 DS-GVO), 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 DS-GVO).[133]

[Rz 59] 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 das sogenannte One-Stop-Shop-Prinzip 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.[134] 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.[135]

[Rz 60] Art. 68 DS-GVO (siehe auch ErwGr. 139 DS-GVO) 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.

[Rz 61] 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. DS-GVO beinhaltet, und zwar durch die Umsetzungsverpflichtung in Art. 51 Abs. 4 DS-GVO. Weiters können die Mitgliedsstaaten gemäß Art. 83 Abs. 7 DS-GVO Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.

[Rz 62] Auch in Deutschland gibt es schon konkrete Pläne zur grundlegenden Reform des Bundesdatenschutzgesetzes (BDSG 2018), im inoffiziellen Referentenentwurf des Bundesministeri-

132 Vgl. insb VfSlg 12.151/1989 und Theo Öhlinger/Harald Eberhard, Verfassungsrecht, facultas Universitätsverlag, 11. Auflage, Wien 2016, Rz. 627 m.w.N. Der VfGH hat seine Auffassung auch nach Einführung der Verwaltungsgerichtsbarkeit erster Instanz nicht in Frage gestellt (vgl. etwa VfGH 10. März 2015, G 203/2014 u.a.).

133 Illibauer (Fn. 125), 337 und 342 f.

134 Näheres dazu in BfDI (Fn. 126), 19 f.

135 Alexander Flendrovsky, Die Aufsichtsbehörden, in: Knyrim (Fn. 124), 290.

ums des Innern (der Entwurf wurde mittlerweile zurückgezogen und neu erstellt) finden sich u.a. Bestimmungen zu Betroffenenrechten, Ausgestaltung der unabhängigen Datenschutzaufsichtsbehörden, Rechtsschutzmöglichkeiten und Verhängung von Geldbußen.[136]

[Rz 63] 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 DS-GVO), 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.

[Rz 64] 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.[137]

[Rz 65] Zusammenfassend lässt sich festhalten, dass der Rechtsschutz bei Auskunftsbegehren m.E. 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 weiterentwickelt. 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 DS-GVO), um dem Betroffenen die Informationen präzise, leicht zugäng-

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

137 Stephan Gärtner, Harte Negativmerkmale auf dem Prüfstand des Datenschutzrechts (Dissertation), Dr. Kova, Hamburg 2011.

lich 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.

Mag. Joachim Galileo Fasching, LL.M. hat Rechtswissenschaften an der Universität Salzburg (Diplomarbeit zum Auskunftsbegehren im Datenschutzrecht) und anschließend Informations- und Medienrecht an der Universität Wien (Masterthesis zu Anwendungsbereichen der Blockchain-Technologie und ausgewählten Rechtsfragen) studiert. Er ist nun in Wien als Geschäftsführer einer Beratungsfirma mit den Schwerpunkten Datenschutz, E-Commerce und Trendforschung tätig.
Die vollständige Diplomarbeit steht **hier** zum Download bereit.