www.jusletter-it.eu

Martin C. Walther

Die Löschung von Daten nach dem DSG 2000

Eine Analyse

The article deals with the practical implementation of the right of erasure following the Austrian data protection act 2000 (DSG 2000) in public and private sectors. Using specific examples and legal fields, the article summarizes what is to be done when the processing of personal data is not or no longer permitted. Therefor, an insight into the two central processing sectors of the DSG 2000 is provided, the question of whether and how the enforcement of the right of erasure is possible is constituted and, finally, a short conclusion is given. (ah)

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

Citation: Martin C. Walther, Die Löschung von Daten nach dem DSG 2000, in: Jusletter IT 21 September 2017

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

Inhaltsübersicht

I. Einleitung

[Rz 1] Für den vorliegenden Beitrag wird vorausgesetzt, dass Zulässigkeitsgründe für eine konkrete Datenverwendung nicht vorliegen und sohin die Grundvoraussetzungfür ein Recht auf Löschung der verarbeiteten personenbezogenen Daten gegeben ist.[1]

[Rz 2] Zu Beginn wird die Löschung der Daten, die (unzulässig) durch die öffentliche Hand verarbeitet wurden, anhand ausgewählter Fälle bearbeitet. Es stellt sich dabei die Frage, ob man einen Papierakt, der sich bspw. bei einem Polizeiposten im Aktenschrank befindet und nicht digitalisiert ist, mit Hilfe des Rechts auf Löschung löschen oder vernichten lassen kann. Daran anschließend wird die Frage beantwortet, wie man personenbezogene Daten, die durch ermittlungsdienstliche und erkennungsdienstliche Maßnahmen ermittelt wurden, insb. auch Fingerabdrücke, aus den Datenbanken der Exekutive und Justiz löschen lassen kann bzw. inwieweit dies auch von Amts wegen geschehen muss.

[Rz 3] Im nächsten Schritt wird die Löschung der Daten im privaten Bereich bearbeitet. Da dies jedoch am Beispiel einer Vielzahl von Privatunternehmen möglich wäre, beschränkt sich dieser Beitrag nur auf zwei Beispiele aus dem Internet, nämlich Facebook und Google. Dabei geht es primär darum, ob und wie man seine personenbezogenen Daten von Facebook löschen lassen kann, wie es mit der praktischen Durchsetzbarkeit seines Rechts auf Löschung gegen Facebook aussieht und ob die Geschäftspraxis von Facebook diesem Anspruch auch tatsächlich entspricht. Danach wird auf die Bedeutung des EuGH-Urteils «Google und Google Spain» vom 13. Mai 2014 eingegangen und überlegt, ob eine Betitelung dieses Urteils als «Recht auf Vergessenwerden» durch die Medien als zutreffend zu bezeichnen ist.

---

[1] Vgl. zu diesem Beitrag näher Martin C. Walther, Die Zulässigkeit der Datenverwendung als Voraussetzung des Rechts auf Löschung, in: Magister, Editions Weblaw, Bern 2017.

[Rz 4] Abschließend wird darauf eingegangen, wie die Löschung in der Praxis abzulaufen hat und das Recht auf Löschung gegen Auftraggeber des öffentlichen und des privaten Bereichs vor der Datenschutzbehörde und vor den ordentlichen Gerichten durchzusetzen ist.

II. Löschung im öffentlichen Bereich

[Rz 5] Im öffentlichen Bereich hängt die Verarbeitung von Daten primär davon ab, ob eine gesetzliche Zuständigkeit für Auftraggeber des öffentlichen Bereichs zur Verarbeitung der Daten besteht. Daher muss sich die gesetzliche Zuständigkeit i.S.d. § 7 Abs. 1 des Datenschutzgesetz 2000 (DSG 2000) zunächst aus den Materiengesetzen des Bundes oder der Länder ableiten lassen, die einen gesetzlichen Auftrag zur Führung einer Datenanwendung geben müssen.[2] Doch lassen sich auch bei solch einer relativ klaren Bestimmung über die Zulässigkeit und dem damit verbundenen positiven oder negativen Ausgang des Löschungsbegehrens Problemfelder finden, die einer Klärung bedürfen, wie es z.B. bei der Frage über die generelle Anwendbarkeit des DSG im Hinblick auf das Vorliegen einer manuellen Datei oder über die Rechtfertigung der weiteren Verarbeitung in der EKIS der Fall ist.

1. Manuelle Datei/Papierakt

[Rz 6] Der Begriff der «Datei» wird in § 4 Z. 6 DSG 2000 definiert als eine «strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind». Eine «manuelle» Datei liegt nach § 58 DSG 2000 dann vor, wenn Daten ohne Automationsunterstützung geführt werden, wobei sich in der Zusammenschau mit der Definition der «Datenanwendung» in § 4 Z. 7 DSG 2000 ergibt, dass darunter eine nicht maschinell und nicht programmgesteuerte Verarbeitung zu verstehen ist. Als Beispiel einer manuellen Datei lässt sich eine Handkartei, die nach aufsteigenden Nummern oder Namen geordnet ist oder ein Karteikasten mit sortierten Karteikarten nennen. Abgrenzungsprobleme schafft diese Definition in den beiden Kriterien «strukturierte Sammlung» und «Zugänglichkeit nach einem Suchkriterium», insbesondere bei Papierakten. Um einen solchen «löschen» zu lassen, wäre nämlich notwendig, dass dieser als manuelle Datei einzuordnen ist. Auch ob Akten und Aktensammlungen sowie ihre Deckblätter in den Anwendungsbereich der DSRL und des DSG fallen, wird durch den ErwGr. 27 der Richtlinie 95/46/EG (sog. Datenschutz-Richtlinie [DSRL])[3] unnötig strittig, da in diesem Akten, Aktensammlungen sowie ihre Deckblätter unter keinen Umständen in den Anwendungsbereich der RL fallen sollen, soweit diese nicht nach bestimmten Kriterien strukturiert sind. Zunächst wird also die Zuordnung von Akten zum Dateibegriff generell abgelehnt, nur um im zweiten Satzteil die Möglichkeit offen zu lassen, dass «nach bestimmten Kriterien strukturierte» Akten dennoch eine Datei darstellen könnten.[4]

---

2 Dietmar Jahnel, Handbuch Datenschutzrecht, Jan Sramek Verlag, Wien 2010, Rz. 4/11.

3 Richtlinie 95/46/EG, ErwGr. 27.

4 Natalie Fercher, Manuelle Dateien im Datenschutzgesetz 2000, in: Dietmar Jahnel/Stefan Siegwart/Natalie Fercher (Hrsg.), Aktuelle Fragen des Datenschutzrechts, Facultas, Wien 2007, 33 (45 f.); Jahnel, Datenschutzrecht (Fn. 2), Rz. 3/100.

[Rz 7] Die erste Entscheidung über einen Papierakt hatte der OGH[5] zu treffen, indem er beurteilen musste, ob ein in einem Zivilprozess erstattetes Sachverständigengutachten eine manuelle Datei darstelle. In seinem Ergebnis stellte der OGH fest, dass für das Vorliegen einer Datei sowohl die Notwendigkeit der Strukturiertheit als auch die Zugänglichkeit nach einem Suchkriterium verlangt werden, woraus der OGH schloss, dass ein Gutachten an sich mangels eines Suchkriteriums keine Datei im Sinne des DSG 2000 darstellt. In dieser ersten Entscheidung wird zu Recht von der h.L. kritisiert, dass der OGH unter anderem pauschal feststellt, dass unter manuellen Dateien nur Karteien und Listen, nicht aber Akten und Aktenkonvolute zu verstehen sind, obwohl ErwGr. 27 der DSRL auf die Strukturiertheit abstellt und keineswegs Akten und Aktenkonvolute generell ausschließt. Dammann/Simitis[6] sagen, dass auch einzelne Akten und Aktensammlungen und die dazugehörigen Deckblätter als Datei einzustufen sind, wenn ihr Inhalt nach Art einer Datei strukturiert ist, wie Kommission und Rat als Ergebnis intensiver Beratungen festgestellt haben. Weiters wird in der Aussage des OGH kritisiert, dass ohne Erfordernis der Zugänglichkeit über ein Suchkriterium auch Akten aus einem behördlichen Verfahren als Datei qualifiziert werden müssten, was der gesetzlichen Definition und den angeführten Erwägungen zur Datenschutzrichtlinie widerspricht und eine uferlose Ausweitung des Datenschutzes bedeuten würde. Sie ist zu allgemein und übersieht, dass die in ErwGr. 27 der DSRL formulierte Technologieunabhängigkeit gerade verhindern soll, dass der Datenschutz durch die Wahl der Verarbeitungstechnik umgangen wird.[7]

[Rz 8] Kurz darauf setzte sich auch die Datenschutzkommission (DSK)[8] mit der Frage über die Qualifizierung des Papierakts als Datei auseinander. Aber auch sie stellte in ihrem ersten Bescheid zu dieser Frage zu allgemein fest, dass «Verwaltungsakte keine manuelle Datei darstellen, da diese zwar in der Regel nach einem Suchbegriff (z.B. Geschäftszahl) aufbewahrt werden, der einzelne Akt jedoch keinen geordneten Inhalt aufweist.» Auf diese zu allgemeine und undifferenzierte Aussage, war jedoch eine zunehmende Differenzierung in der nachfolgenden Bescheidpraxis der DSK festzustellen. Diese zunehmende Differenzierung gestaltete die DSK über die Jahre dahingehend aus, dass sie nun in ständiger Spruchpraxis davon ausgeht, dass Verwaltungsakten ohne das Hinzutreten besonderer Strukturierungsmerkmale[9] bzw. ohne besondere Gestaltung (Strukturierung)[10] nicht die Qualität einer Datei gem. § 4 Z. 6 DSG 2000 haben. Dennoch lässt diese Spruchpraxis auch Fälle zu, in denen Papiersammlungen eine Datei darstellen können, wie eine Entscheidung der DSK[11] zeigt, in der Anamneseblätter, die lediglich in Papierform aufbewahrt werden, aber nach Kurs und innerhalb diesem nach Namen sortiert waren, als Datei i.S.d. § 4 Z. 6 DSG 2000 qualifiziert wurden.

[Rz 9] Bestätigt wird die Bescheidpraxis der DSK seit geraumer Zeit auch von den Höchstgerichten. Der VfGH[12] und der VwGH[13] stellten fest, dass ein Papierakt keine manuelle Datei ist und

5 OGH 28. Juni 2000, 6 Ob 148/00h = SZ 73/105.

6 Ulrich Dammann/Spiros Simitis, EG-Datenschutzrichtlinie – Kommentar, Nomos Verlag, Baden-Baden 1997, Art. 2 Anm. 8.

7 Jahnel, Datenschutzrecht (Fn. 2), Rz. 3/101.

8 DSK 10. November 2000, 120/707/7-DSK/00.

9 DSK 11. März 2005, K120.969/0002-DSK/2005.

10 DSK 11. Oktober 2005, K121.043/0008-DSK/2005.

11 DSK 20. Juni 2008, K210.583/0009-DSK/2008.

12 VfGH 15. Dezember 2005, B 1590/03 = VfSlg 17745/2005.

13 VwGH 21. Oktober 2004, 2004/06/0086 = VwSlg 16477 A/2004.

somit nicht unter den Anwendungsbereich des DSG fällt. Auf diese Urteile stützt sich wiederum die DSK[14] in ihren Bescheiden, sodass sowohl die DSK als auch die Höchstgerichte (OGH, VfGH, VwGH) in einhelliger Meinung mit nahezu identischer Begründung davon ausgehen, dass es sich bei einem Papierakt nicht um eine manuelle Datei im Sinne des DSG handelt.

[Rz 10] Die Literatur kritisiert jedoch auch diese generelle Ansicht, da DSG und DSRL klar vorgeben, dass Akten und Aktenkonvolute weder prinzipiell unter diesen Begriff fallen, noch dass dies nicht der Fall ist. So fordert der Dateibegriff des DSG nach seinem Wortlaut Strukturiertheit und Zugänglichkeit nach mindestens einem Kriterium, wobei die Strukturiertheit aufgrund der Entscheidungen des OGH und VwGH mit einer «äußeren Ordnung» gegeben ist, der ein bloßer Fließtext gegenüber gestellt ist. So sollte es für die Strukturiertheit schon ausreichen, dass der Papierakt ein Inhaltsverzeichnis hat, um eine äußere Ordnung herzustellen, da ein Akt in den meisten Fällen chronologisch geordnet sein und auch ein Deckblatt aufweisen wird, welches eine leichtere Auffindbarkeit sicherstellt.[15]

[Rz 11] Ob ein Papierakt als eine manuelle Datei zu werten ist oder nicht, hängt somit im Einzelfall primär davon ab, ob Daten nach einem Suchkriterium zugänglich sind. Der Zweck des Dateibegriffs ist, dass eine Auskunft über personenbezogene Daten nur dann gegeben werden muss, wenn der Zugang zu diesen Daten unter vertretbarem Aufwand möglich ist.[16] Eine Wort-für-Wort-Suche innerhalb eines Akts soll dadurch verhindert werden. Auch der ErwGr. 15 der DSRL[17] kann für diese Auslegung herangezogen werden, da laut diesem nur Daten von der RL erfasst sind, die entweder automatisiert verarbeitet werden oder in Dateien enthalten sind, «die nach bestimmten personenbezogenen Kriterien strukturiert sind, um einen leichten Zugriff auf die Daten zu ermöglichen.»[18] Die Strukturiertheit ist also nicht eine von der Zugänglichkeit unabhängige Notwendigkeit, sondern das Mittel zur Erreichung der Zugänglichkeit. Wenn ein leichter Zugriff durch ein personenbezogenes Kriterium ermöglicht wird, ist der Dateibegriff somit verwirklicht.[19]

[Rz 12] Der positive Ausgang eines Löschungsbegehrens eines Papierakts erfordert somit, dass der Papierakt neben einer nach Durchführung der Zulässigkeitsprüfung unzulässigen Verarbeitung auch als manuelle Datei i.S.d. § 58 DSG 2000 einzuordnen ist. Dies kann er nur sein, wenn er einen solchen äußeren Ordnungsgrad hat und so strukturiert ist, dass eine gezielte Suche nach bestimmten personenbezogenen Daten möglich ist. Wenn die Suche z.B. nach der Anschrift oder nach dem Namen durchgeführt werden kann, so fällt der Papierakt unter den Begriff der manuellen Datei und dem Löschungsbegehren ist von der Datenschutzbehörde (DSB) stattzugeben. Dabei kann die «Löschung» des Papierakts aber so erfolgen, dass nicht der komplette Papierakt vernichtet werden muss, sondern lediglich der Personenbezug durch Schwärzung der personenbezogenen Daten oder durch Vernichtung einzelner Seiten des Papierakts entfernt wird. Sollte

14 DSK 6. September 2013, K121.979/0014-DSK/2013; DSK 6. September 2013, K121.978/0010-DSK/2013; DSK 20. Januar 2010, K121.553/0003-DSK/2010.

15 Jahnel, Datenschutzrecht (Fn. 2), Rz. 3/102 f; Walter Dohr/Hans J. Pollierer/Ernst M. Weiss/Rainer Knyrim, DSG Datenschutzrecht – Kommentar, 2. Auflage, Band I, Manz Verlag, Wien 2002, § 4 Anm. 7 (17. ErgLfg 2014); Viktor Mayer-Schönberger/Hans Kristoferitsch, Datenschutz und Papierakten, ecolex 2006, 615 (618).

16 Vgl. Mayer-Schönberger/Kristoferitsch, ecolex (Fn. 15), 615 (618 f).

17 Richtlinie 95/46/EG, ErwGr. 15.

18 Vgl. Mayer-Schönberger/Kristoferitsch, ecolex (Fn. 15), 615 (619); Fercher, in: Jahnel/Siegwart/Fercher (Fn. 4), 33 (50 ff.).

19 Jahnel, Datenschutzrecht (Fn. 2), Rz. 3/104.

dies jedoch nicht ausreichen, um den Personenbezug des Papierakts zu lösen, so muss der komplette Papierakt tatsächlich vernichtet werden.

2. EKIS

[Rz 13] Das DSG enthält in § 27 Abs. 9 DSG 2000 Ausnahmen vom Recht auf Richtigstellung und Löschung für das Strafregister und für öffentliche Bücher und Register, die von Auftraggebern des öffentlichen Bereichs geführt werden. Die § 27 Abs. 1–8 DSG 2000 sind daher nicht anzuwenden, wenn durch das entsprechende Bundesgesetz hinsichtlich der Verpflichtung zur Richtigstellung und Löschung von Amts wegen oder für das Verfahren der Durchsetzung und die Zuständigkeit zur Entscheidung über Berichtigungs- und Löschungsanträge anderes bestimmt ist.

[Rz 14] Unter diese öffentlichen Register fällt u.a. die Zentrale Informationssammlung des Bundesministeriums für Inneres, das sogenannte EKIS, was bereits seit 1968 geführt wird. In diesem werden neben sicherheitspolizeilichen Datenanwendungen, auch verwaltungspolizeiliche und kriminalpolizeiliche abgespeichert. So kann man über das EKIS auf das Strafregister (Rechtsgrundlage: Strafregistergesetz [StrRegG] / Tilgungsgesetz [TilgG]), die Kfz-Fahndungs-/ Informationsdatei, die Personenfahndungsdatei, die Personeninformationsdatei, die Sachenfahndungsdatei, die Kulturgutfahndungsdatei, den Kriminalpolizeilichen Aktenindex (KPA) (Rechtsgrundlage: § 57 des Sicherheitspolizeigesetzes [SPG]) und die Zentrale Erkennungsdienstliche Evidenz samt AFIS und DNA-Datenbank (Rechtsgrundlage: § 75 SPG) zugreifen.[20]

[Rz 15] Der Auftraggeber der Datenverarbeitung i.S.d. DSG 2000 ist für das EKIS bzw. für die darin zusammengefassten Datenbanken die jeweilige Sicherheitsbehörde in deren Verantwortung die Daten in diesem System verarbeitet werden, auch wenn das Bundesministerium für Inneres (BMI) allenfalls durch generelle oder Weisungen im Einzelfall Anordnungen zur Verarbeitung der Daten in diesem System trifft.[21]

2.1. Ermittlungsdienstlich personenbezogene Daten

[Rz 16] Gem. § 57 SPG können in den Datenbanken der EKIS Name, Geschlecht, frühere Namen, Staatsangehörigkeit, Geburtsdatum, Geburtsort und Wohnanschrift, Namen der Eltern und Aliasdaten, ein Lichtbild eines Menschen sowie eine allenfalls vorhandene Beschreibung des Aussehens eines Menschen oder seiner Kleidung ermittelt und im Rahmen der Zentralen Informationssammlung samt dem für die Speicherung maßgeblichen Grund verarbeitet werden. Die Zulässigkeit der Ermittlung der personenbezogenen Daten muss sich zwingend aus einer Ziffer der § 53 Abs. 1 Z. 1 bis 7 SPG (u.a. Gefahrenforschung in Z. 2a; Abwehr gefährlicher Angriffe in Z. 3 und 4; Zwecke der Fahndung in Z. 5) ergeben und der Grund, der für die Speicherung maßgeblich ist, muss einer sein, der in den in § 57 Z. 1 bis 12 SPG genannten Umständen (u.a. richterlicher Befehl gegen den Betroffenen zur Festnahme; Ermittlungen gegen den Betroffenen; Betroffener ist Opfer einer Gewalttat oder Identitätsdiebstahl) seine Entsprechung findet. Diese geben damit Auskunft über die gesetzliche Grundlage der Maßnahmen gem. § 53 SPG und insb. § 57

20 Bundesministerium für Inneres, Information zum EKIS (bmi.gv.at/cms/BMI_Datenschutz/ekis/start.aspx/ [alle Websites zuletzt abgerufen am 9. August 2017]); Walter Grosinger, in: Theodor Thanner/Matthias Vogl (Hrsg.), SPG Sicherheitspolizeigesetz, 2. Auflage, NWV Verlag, Wien 2013, § 57 Anm. 2.

21 Grosinger, in: Thanner/Vogl (Fn. 20), § 57 Anm. 1; Klaus Wallnöfer, in: Thanner/Vogl (Fn. 20), § 75 Anm. 5.

SPG. Demnach wird man bspw. nur dann die Personenbeschreibung nach § 57 SPG in der EKIS verarbeiten dürfen, wenn diese gem. § 53 SPG, etwa aufgrund des Zwecks der Fahndung (§ 53 Abs. 1 Z. 5 SPG), zulässigerweise ermittelt wurde und gem. § 57 Abs. 1 Z. 6 SPG Ermittlungen im Dienste der Strafrechtspflege gegen die Person eingeleitet wurden.[22]

2.2. Erkennungsdienstlich personenbezogene Daten

[Rz 17] In § 57 SPG findet sich auch ein Hinweis auf die Ermittlung erkennungsdienstlicher Daten, deren Rechtsgrundlage sich für die Zulässigkeit der Ermittlung in §§ 64 ff. SPG und für die Verarbeitung in der Zentralen Erkennungsdienstlichen Evidenz in § 75 Abs. 1 SPG findet. Erkennungsdienstliche Daten werden durch erkennungsdienstliche Maßnahmen, wie die Abnahme von Papillarlinienabdrücken oder die Vornahme von Mundhöhlenabstrichen, erhoben. Daten, welche die Zuordnung erkennungsdienstlicher Daten zu einer bestimmten Person erlauben, werden in dem Fall erkennungsdienstliche Identitätsdaten genannt.[23] Unter diese fallen gem. § 65 Abs. 6 SPG Namen, Geschlecht, frühere Namen, Geburtsdatum, Geburtsort, Namen der Eltern und Aliasdaten.

[Rz 18] Nach § 75 SPG sind die Sicherheitsbehörden ermächtigt, die von ihnen gemäß den §§ 65 Abs. 1, 65a, 66 Abs. 1, 67 Abs. 1 erster Satz und Abs. 1a SPG sowie § 68 Abs. 1 SPG ermittelten erkennungsdienstlichen Daten, die allenfalls vorhandenen erkennungsdienstlichen Identitätsdaten (§ 65 Abs. 6 SPG) und den für die Ermittlung maßgeblichen Grund im Rahmen einer Zentralen Erkennungsdienstlichen Evidenz zu verarbeiten. Die personenbezogenen Daten, die Sicherheitsbehörden nach anderen Bestimmungen rechtmäßig ermittelt haben, dürfen in der Zentralen Erkennungsdienstlichen Evidenz weiterverarbeitet werden, wenn deren Ermittlung und Verarbeitung für sicherheitspolizeiliche Zwecke zu dem Zeitpunkt zulässig wäre, in dem die Daten verwendet werden sollen.

[Rz 19] Demnach ist die Verarbeitung gem. § 75 SPG auf die den erkennungsdienstlichen Maßnahmen zugrundeliegenden Tatbestände eingeschränkt. Es dürfen ausschließlich Daten zentral und bundesweit verarbeitet werden, die aufgrund des Verdachts einer mit Strafe bedrohten Handlung [...] und zur Vorbeugung weiterer gefährlicher Angriffe (§ 65 Abs. 1 SPG), der begründeten Befürchtung eines Selbstmords, einer Gewalttat sowie eines Unfalls (§ 65a SPG), der unbekannten Identität eines Toten (§ 66 Abs. 1 SPG) oder des Verdachts eines gefährlichen Angriffs (§ 67 Abs. 1 SPG) erhoben wurden.[24] Diese entsprechen im Grunde den § 57 Abs. 1 Z. 1–12 SPG für die Speicherung ermittlungsdienstlicher Daten in der EKIS.

[Rz 20] Das bedeutet konkret, dass erkennungsdienstliche Daten, die nicht aufgrund der in § 75 Abs. 1 Satz 1 SPG angeführten Gesetzesbestimmungen erhoben wurden, wie etwa die Daten von Gelegenheitspersonen, deren erkennungsdienstliche Daten nach § 65 Abs. 2 SPG nur erfasst wurden, um einen gefährlichen Angriff aufzuklären, ohne dass diese tatverdächtig sind, sie aber Gelegenheit hatten, am Tatort Spuren (insb. Fingerabdrücke oder DNA-Spuren) zu hinterlassen,[25] auch nicht in der Zentralen Erkennungsdienstlichen Evidenz, und somit nicht in der EKIS verarbeitet werden dürfen. Diese müssen gem. § 70 SPG in den regionalen erkennungsdienstlichen

22 Grosinger, in: Thanner/Vogl (Fn. 20), § 57 Anm. 4 f.

23 Ewald Wiederin, Einführung in das Sicherheitspolizeirecht, Verlag Österreich, Wien 1998, Rz. 645.

24 Wallnöfer, in: Thanner/Vogl (Fn. 20), § 75 Anm. 3.

25 Martina Schlögl, in: Thanner/Vogl (Fn. 20), § 65 Anm. 8.

Evidenzen der einzelnen Sicherheitsbehörden, die die Daten im Rahmen einer erkennungsdienstlichen Behandlung ermittelt haben, verarbeitet werden, was einen bundesweiten Zugriff auf diese Daten verhindern soll. Es entspricht außerdem dem Verhältnismäßigkeitsgebot des § 51 SPG, den bundesweiten Zugriff auf Daten von Gelegenheitspersonen sowie Opfern und Zeugen zu vermeiden. Im Falle der Ausnahme des § 75 Abs. 1 Satz 2 SPG können jedoch auch diese Daten in der Zentralen Erkennungsdienstlichen Evidenz verarbeitet werden, wenn die Erhebung und Verarbeitung zum Zwecke der Sicherheitspolizei nach anderen Gesetzen zulässig ist.[26]

[Rz 21] Wird also ein Mensch gem. § 65 Abs. 1 SPG einer mit Strafe bedrohten Handlung verdächtigt und scheint es notwendig, eine erkennungsdienstliche Behandlung durchzuführen, um weiteren gefährlichen Angriffen vorzubeugen, so dürfen diese Daten in der Zentralen Erkennungsdienstlichen Evidenz verarbeitet werden.

[Rz 22] Sollten jedoch erkennungsdienstliche Daten, die nicht aufgrund der angeführten Gesetzesbestimmungen erhoben wurden, in der Zentralen Erkennungsdienstlichen Evidenz verarbeitet werden, dann nur wenn ihre Erhebung und Verarbeitung zum Zwecke der Sicherheitspolizei nach anderen Gesetzen zulässig ist. Ansonsten ist ihre Verarbeitung nur in den regionalen erkennungsdienstlichen Evidenzen gem. § 70 SPG zulässig.

[Rz 23] Die §§ 65 bis 67 SPG stellen zusammengefasst die gesetzliche Grundlage für die Zulässigkeit der Ermittlung erkennungsdienstlicher Daten und §§ 70 und 75 SPG für die Zulässigkeit der Speicherung in den regionalen und der Zentralen Erkennungsdienstlichen Evidenz dar.

2.3. Ermittlungsdienstlich und erkennungsdienstlich personenbezogene Daten der Ermittlungsmaßnahmen der StPO

[Rz 24] Bei der Reform des strafprozessualen Vorverfahrens 2004[27] verankerte der Gesetzgeber auch einige neue Ermittlungsmaßnahmen in der Strafprozessordnung (StPO), u.a. die Identitätsfeststellung (§ 118 StPO), die körperliche (§ 123 StPO) und die molekulargenetische Untersuchung (§ 124 StPO). Diese bilden die gesetzliche Grundlage für die Ermittlung der personenbezogenen Daten und deren weiteren strafprozessualen Verarbeitung. So bestimmt § 118 Abs. 2 StPO, dass die Kriminalpolizei ermächtigt wird, zur Identitätsfeststellung die Namen einer Person, ihr Geschlecht, ihr Geburtsdatum, ihren Geburtsort, ihren Beruf und ihre Wohnanschrift zu ermitteln. Ist es zur Identitätsfeststellung notwendig, darf sie einer Person Fingerabdrücke abnehmen, ihre Größe feststellen, sie fotografieren und ihre Stimme aufnehmen. Sollten gegen den Betroffenen Ermittlungen wegen des Verdachts einer Straftat geführt werden, ergibt sich laut der RV[28] zu § 118 StPO aus den §§ 53 Abs. 2 und 57 Abs. 1 Z. 6 SPG außerdem die Ermächtigung der Kriminalpolizei, nach Abs. 2 ermittelte Daten für Zwecke des Strafverfahrens und zur Abwehr gefährlicher Angriffe zu verwenden und zu diesem Zwecke in der EKIS zu verarbeiten. Es können somit nach § 118 StPO nicht nur bloß ermittlungsdienstliche personenbezogene Daten, wie Namen, Adresse und Geburtsdatum, sondern auch erkennungsdienstliche personenbezogene Daten, ermittelt und im KPA, also in der EKIS, verarbeitet werden.

---

26 Wallnöfer, in: Thanner/Vogl (Fn. 20), § 75 Anm. 6.

27 Bundesgesetz, mit dem die Strafprozessordnung 1975 neu gestaltet wird (Strafprozessreformgesetz), BGBl. I Nr. 19/2004.

28 RV 25 BlgNR XXII. GP 164.

[Rz 25] Dies steht jedoch im Widerspruch mit den Vorschriften des SPG. Eine Übermittlung und Speicherung von personenbezogenen Daten in der EKIS ist nur zulässig, wenn ihre Ermittlung und Speicherung auch nach den Vorschriften in §§ 53 und 57 SPG sowie §§ 65–67 und 75 SPG zulässig wäre. Eine Speicherung erkennungsdienstlicher personenbezogener Daten in der EKIS nach § 118 Abs. 2 StPO ist nach der Systematik des SPG jedenfalls nur in der Zentralen Erkennungsdienstlichen Evidenz zulässig. Auch die ErläutRV[29] zu § 57 Abs. 1 SPG unterstreicht dies, indem sie die Ermittlung und Verarbeitung von Fingerabdrücken im EKIS, der zentralen Informationssammlung nach § 57 SPG, nicht vorsieht. Lediglich ein Hinweis auf allenfalls bereits vorhandene erkennungsdienstliche nach § 75 SPG in der Zentralen Erkennungsdienstlichen Evidenz gespeicherte Daten soll möglich sein.

[Rz 26] Aufgrund des § 57 SPG als *lex specialis* bzw. als *lex posterior* und der Systematik des SPG muss wohl davon ausgegangen werden, dass in der RV[30] zu § 118 StPO die Verarbeitung von Fingerabdrücken und anderen erkennungsdienstlichen Daten in der EKIS nicht gesondert durchdacht wurde. Daher können nur ermittlungsdienstliche Daten, wie Namen, Geschlecht, Geburtsdatum, Geburtsort, Beruf und Wohnanschrift in dem KPA gem. § 57 SPG verarbeitet werden. Jedoch dürfen alle darüber hinausgehenden erkennungsdienstlichen Daten, wie Fingerabdrücke, Größe etc. nach den Vorschriften §§ 65 bis 67 und 75 SPG nur in der Zentralen Erkennungsdienstlichen Evidenz verarbeitet werden.

[Rz 27] Bei den erkennungsdienstlich personenbezogenen Daten, die auf Grundlage der §§ 123 und 124 StPO ermittelt werden (u.a. Blutproben und DNA), besteht gem. § 124 Abs. 5 StPO auch die Möglichkeit der Übermittlung an die Sicherheitsbehörden auf deren Verlangen, soweit die Ermittlung und Verarbeitung dieser Daten nach sicherheitspolizeilichen Vorschriften (§§ 65 bis 67 und 75 SPG) zulässig wäre und diese dann nach diesen Vorschriften in der Zentralen Erkennungsdienstlichen Evidenz gespeichert werden.

[Rz 28] Durch Ermittlungsmaßnahmen im Rahmen der StPO können somit Daten in den Evidenzen und Datenbanken der Justiz wie auch im EKIS gem. § 57 und 75 SPG verarbeitet werden.

2.4. Strafregister

[Rz 29] Wie oben schon erwähnt, ist über das EKIS auch ein Zugriff auf das Strafregister möglich. Dieses wird zum Zwecke der Evidenthaltung strafgerichtlicher Verurteilungen von der Landespolizeidirektion Wien für das gesamte Bundesgebiet geführt und nach der Organisation der Landespolizeidirektion Wien von dieser Behörde vom Strafregisteramt besorgt.[31] Gem. § 2 StRegG sind in das Strafregister alle rechtskräftigen Verurteilungen durch inländische Strafgerichte, rechtskräftige Entscheidungen ausländischer Gerichte, rechtskräftige Verurteilungen durch ausländische Strafgerichte nach § 2 Abs. 1 Z. 2 StRegG und Mitteilungen an das Strafregisteramt aufzunehmen. Darüber hinaus sind auch aus solchen Verurteilungen bezogene Entschließungen, Entscheidungen, Verfügungen und Mitteilungen nach § 2 Abs. 1 Z. 4 bis 6 StRegG darin aufzunehmen.

---

29 ErläutRV 1520 XXIV. GP 9.

30 RV 25 BlgNR XXII. GP 164.

31 § 1 StRegG; Maria Eder-Rieder, Strafregister- und Tilgungsgesetz, NWV Verlag, Wien 2008, Teil 1: II, § 1 Anm. zu § 1.

[Rz 30] Die Ermittlung der Daten obliegt im Falle des Strafregisters somit den ordentlichen Gerichten, die den Betroffenen verurteilt haben. Die Übermittlung der Daten muss gem. § 3 StRegG nach Eintritt der Rechtskraft durch die Übersendung von Strafkarten an die Landespolizeidirektion Wien erfolgen. In diesen Strafkarten sind u.a. die Angaben über die Bezeichnung und das Aktenzeichen des Strafgerichtes erster Instanz, Namen, Geburtstagsdatum und -ort, das Geschlecht, die Staatsangehörigkeit, Vornamen der Eltern des Verurteilten, Tag des Erkenntnisses erster Instanz und des Eintritts der Rechtskraft und alle vom Strafgericht ausgesprochenen Strafen enthalten. All diese personenbezogenen Daten sind dann von dem Strafregisteramt auf der rechtlichen Grundlage des StRegG zu verarbeiten.

3. Löschung aus dem EKIS

[Rz 31] Die Löschungsbestimmungen für das EKIS finden sich in § 58 SPG. Diese beziehen sich nur auf in der zentralen Datenanwendung des § 57 SPG gespeicherte Daten und sind auf die sonst nach § 53 ff. SPG ermittelten Daten nicht anzuwenden.[32] Nach § 58 SPG ist der Zugriff der Sicherheitsbehörden als Auftraggeber auf personenbezogene Daten, die gem. § 57 Abs. 1 SPG evident gehalten werden, zu sperren, wenn die Fristen der Z. 1 bis 11 abgelaufen sind. Nach Ablauf von weiteren zwei Jahren sind die Daten dann auch physisch zu löschen.

[Rz 32] Die Sperre des Zugriffs besteht dabei in einer technischen Maßnahme, die die Daten zwar im System behält, aber bei Abfragen durch die Sicherheitsbehörden nicht mehr beauskunftet. Sinn dieser Sperre für Zugriffe ist es, inhaltsgleichen Neuspeicherungen, die auf Übermittlungsfehler einer Fahndungsbehörde zurückzuführen sind, vorzubeugen. Daher bedarf es in diesem Zeitraum von zwei Jahren einer speziellen Kontrolleinrichtung, wobei bei inhaltsgleicher Neuspeicherung die Sperre automationsunterstützt aufgehoben und der Sicherheitsbehörde im Hinblick auf die beabsichtigte Neuspeicherung eine Überprüfung aufgetragen wird.[33]

[Rz 33] In Z. 6 wird die Löschungsverpflichtung für Daten in dem KPA normiert, die aufgrund von §§ 53 Abs. 2 und 57 Abs. 1 Z. 6 SPG verarbeitet wurden. Die Verpflichtung zur Sperre für Zugriffe tritt ein, wenn der Betroffene nicht mehr im Verdacht steht, eine strafbare Handlung begangen zu haben. Diese Löschungsregelung sieht eine Speicherdauer von fünf Jahren (nach der letzten Speicherung) vor, es sei denn die Sicherheitsbehörde hat sie zu löschen, weil sie keine Anzeige an die Staatsanwaltschaft erstattet. Der VfGH[34] interpretierte die Bestimmung im Hinblick auf das Verhältnismäßigkeitsprinzip des § 51 SPG und die allgemeine Löschungsregel des § 63 SPG derart, dass bereits eine frühere Löschung geboten sei, wenn die Daten vor Ablauf dieser Frist nicht mehr benötigt werden. Dies könnte etwa der Fall sein, wenn im Strafverfahren festgestellt wird, dass der Betroffene die Tat nicht begangen hat. Legt die Staatsanwaltschaft eine Anzeige z.B. nach Durchführung einer diversionellen Maßnahme zurück oder wird der Betroffene mangels Zurechnungsfähigkeit im Tatzeitpunkt freigesprochen, wird der Verdacht der Begehung einer strafbaren Handlung nicht entkräftet. Daher sollen den Sicherheitsbehörden die Informationen aus dem KPA weiter für die Erfüllung sicherheits- oder kriminalpolizeilicher Aufgaben zur Verfügung stehen. Es soll ihnen ermöglicht werden, die Daten sowohl bei später auftauchen-

32 Grosinger, in: Thanner/Vogl (Fn. 20), § 58 Anm. 1.

33 EBRV 148 XVIII. GP 45.

34 VfGH 16.03.2001, G 94/00 = VfSlg 16150/2001.

den Anhaltspunkten, für weitere Ermittlungen in derselben Sache oder auch im Hinblick auf Verbindungen zu anderen Straftaten des Betroffenen oder anderen Tatverdächtigen als auch für die sicherheitspolizeiliche Beurteilung, ob jemand in Zukunft einen gefährlichen Angriff begehen oder ausführen werde, zu verwenden.[35]

[Rz 34] Wie die DSK[36] ebenfalls entschied, muss für die Löschung einer KPA-Eintragung, entweder die Eintragung unrichtig oder die fünfjährige Löschungsfrist abgelaufen sein. Durch die Bestätigung der Eintragung in einem Hauptverfahren und dem Vermerk im Strafregister wird jedenfalls keine Löschungspflicht ausgelöst, ganz im Gegenteil. Eine Löschung vor Ablauf der Frist, wäre nur möglich, wenn Gründe vorgebracht werden, die einen Wegfall der Notwendigkeit der Aufbewahrung nach § 63 SPG begründen.

[Rz 35] In § 63 SPG wird weiters die allgemeine Löschungsregel normiert. § 63 Abs. 1 SPG besagt, dass unrichtige oder entgegen den Bestimmungen des SPG ermittelte und aufbewahrte Daten unverzüglich richtigzustellen oder zu löschen sind. Personenbezogene Daten sind zu löschen, sobald sie für die Erfüllung der Aufgabe, für die sie verwendet worden sind, nicht mehr benötigt werden, es sei denn, für ihre Löschung wäre eine besondere Regelung getroffen worden. Dies entspricht dem Zweckbindungsgrundsatz des § 6 Abs. 1 Z. 2 DSG 2000. In § 63 Abs. 2 SPG wird des Weiteren noch eine Höchstaufbewahrungsdauer für Daten festgelegt, die sechs Jahre unverändert geblieben sind. Es ist zu überprüfen, ob diese nicht gem. Abs. 1 richtig zu stellen oder zu löschen sind.

[Rz 36] Aus den ErläutRV[37] ergibt sich, dass die Regelung des § 63 SPG sowohl für automationsunterstützt verarbeitete Daten wie auch für konventionell verarbeitete Daten gilt, wobei das Gesetz hierbei auf alle Daten Bezug nimmt, die aufbewahrt werden.[38] Nach dem VwGH[39] sind von dieser Löschungsverpflichtung auch Eintragungen in Protokollbüchern und Steckzettel umfasst.

[Rz 37] Der VwGH[40] sieht in § 63 SPG jedoch nur eine Pflicht der Behörde zur Richtigstellung oder Löschung von Daten. Für den Betroffenen selbst ergibt sich daraus kein Recht, sich mit einer Beschwerde an die Datenschutzbehörde zu wenden und die Löschung seiner personenbezogenen Daten zu verlangen. Dies muss er mit dem Löschungsrecht des DSG über § 27 Abs. 1 und 4 i.V.m. § 31 Abs. 2 DSG 2000 durchsetzen.

3.1. Löschung der Daten aus der Zentralen Erkennungsdienstlichen Evidenz

[Rz 38] Die allgemeinen Vorschriften der EKIS der §§ 53 bis 63 SPG und insb. die Löschungsvorschriften des §§ 58 und 63 SPG sind laut der ErläutRV[41] nicht auf die Ermittlung und Verarbeitung von erkennungsdienstlichen Daten wie Fingerabdrücken im EKIS anzuwenden. Lediglich der Hinweis auf eine bereits vorhandene Verarbeitung von erkennungsdienstlichen Daten in der Zentralen Erkennungsdienstlichen Evidenz ist in den übrigen Datenbanken der EKIS zulässig.

35 EBRV 1138 XXI. GP 32.

36 DSK 14.12.2012, K121.885/0011-DSK/2012.

37 EBRV 148 XVIII. GP 47.

38 Grosinger, in: Thanner/Vogl (Fn. 20), § 63 Anm. 1.

39 VwGH 25. November 2008, 2005/06/0301; VwGH 21. Oktober 2004, 2004/06/0086 = VwSlg 16477 A/2004.

40 VwGH 21. Oktober 2004, 2004/06/0086 = VwSlg 16477 A/2004.

41 ErläutRV 1520 XXIV. GP 9.

Daher sind auf erkennungsdienstliche Daten, die im Rahmen der zentralen Informationssammlung (§ 75 SPG) und auch im Rahmen der regionalen Evidenthaltung (§ 70 SPG) gespeichert wurden, die Löschungsvorschriften der §§ 73 und 74 SPG anzuwenden. Die §§ 73 und 74 SPG sind als *lex specialis* zu § 27 DSG 2000 zu verstehen, der dadurch auf die geregelten Tatbestände keine Anwendung findet.[42]

[Rz 39] Grundsätzlich sind erkennungsdienstliche Daten zu löschen und eine Übermittlung oder Verarbeitung darf lediglich in den gesetzlich geregelten Fällen erfolgen. Bei der Löschung von erkennungsdienstlichen Daten ist ein wesentlicher Anknüpfungspunkt der Verlauf der Zeit. So sind erkennungsdienstliche Daten fünf Jahre nach dem Tod der betroffenen Person (§ 73 Abs. 1 Z. 3 SPG), fünf Jahre nach der letzten erkennungsdienstlichen Behandlung der betroffenen über 80 Jahre alten Person (§ 73 Abs. 1 Z. 1 SPG), drei Jahre nach der letzten erkennungsdienstlichen Behandlung der betroffenen zum Tatzeitpunkt strafunmündigen Person (§ 73 Abs. 1 Z. 2 SPG) oder fünf Jahre nach der erkennungsdienstlichen Behandlung einer Leiche aufgrund von § 68 SPG (§ 73 Abs. 5 SPG) zu löschen. Diese Löschfristen markieren dabei einerseits die Höchstgrenzen der Aufbewahrung und andererseits abstrakte Anknüpfungspunkte für eine entsprechende generelle Programmierung in den erkennungsdienstlichen Evidenzen.[43]

[Rz 40] Für erkennungsdienstliche Daten, die zu Identifikationszwecken ermittelt wurden, gilt, dass sie zu löschen sind, wenn sie ihre Funktion für den Anlassfall erfüllt haben.[44] Davon umfasst werden die Daten von Gelegenheitspersonen nach § 65 Abs. 2 SPG, wenn sie Spuren am Tatort hinterlassen haben und diese ausgesondert wurden (§ 73 Abs. 1 Z. 5 SPG), von Hilflosen nach § 65 Abs. 3 SPG, wenn die der erkennungsdienstlichen Behandlung zugrundeliegende Hilfeleistung abgeschlossen wurde (§ 73 Abs. 1 Z. 6 SPG), von Kriminalbeamten nach § 70 Abs. 4 SPG, die nicht mehr regelmäßig in der Tatortausw.ertung eingesetzt werden (§ 73 Abs. 1 Z. 5 SPG), von Abgängigen, von denen gem. § 65a SPG erkennungsdienstliche Daten erhoben wurden, nach deren Auffindung (§ 73 Abs. 4 SPG) und von Leichen, die gem. § 66 SPG erkennungsdienstlich behandelt wurden, nach erfolgreicher Identifizierung (§ 73 Abs. 5 SPG).

[Rz 41] Einen der zentralen Anknüpfungspunkte für die erkennungsdienstliche Behandlung stellt der Verdacht der Begehung eines gefährlichen Angriffs (§ 16 Abs. 2 SPG) oder der Tätigkeit im Rahmen einer kriminellen Verbindung dar. Sollte dieser Verdacht nach erfolgter erkennungsdienstlicher Behandlung nicht bestätigt werden, so sind die Daten von Amts wegen sofort zu löschen (§ 73 Abs. 1 Z. 4 SPG). Dabei erfolgt die Bestätigung des Verdachts im Regelfall durch eine nachfolgende gerichtliche Verurteilung. Bei einem Freispruch oder der Einstellung des gerichtlichen Strafverfahrens besteht grundsätzlich keine Bestätigung des Verdachts.[45] Trotz der Entkräftung des Verdachts ist jedoch von der Löschung der Daten abzusehen, wenn konkrete Hinweise künftige gefährliche Angriffe durch den Betroffenen befürchten lassen. Dem liegt auch die Überlegung zugrunde, dass die Verurteilung einer Person nicht das einzige, wenn auch sehr gewichtige, Indiz dafür ist, dass sie in Zukunft einen gefährlichen Angriff begehen werde.[46]

[Rz 42] Um erkennungsdienstlichen Daten auch ohne bestätigten Verdacht aufgrund der Gefährlichkeit des Betroffenen evident zu halten, muss von den Sicherheitsbehörden eine Interessen-

42 Grosinger, in: Thanner/Vogl (Fn. 20), § 57 Anm. 6; Wallnöfer, in: Thanner/Vogl (Fn. 20), § 73 Anm. 1.

43 Wallnöfer, in: Thanner/Vogl (Fn. 20), § 73 Anm. 4.

44 EBRV 148 XVII. GP 50.

45 VwGH 2. Oktober 2001, 2000/01/0233 = VwSlg 15692 A/2001.

46 EBRV 148 XVII. GP 50.

abwägung (Prognoseentscheidung) durchgeführt werden, in der das grundrechtliche Löschungsbedürfnis des Betroffenen mit dem Sicherheitsbedürfnis der Bevölkerung hinsichtlich der mehr oder weniger wahrscheinlichen künftigen gefährlichen Angriffe abzuwägen ist.[47] Dabei bedarf es der konkreten Befürchtung der Verwirklichung aller Tatbestandsmerkmale eines gefährlichen Angriffs in der Zukunft,[48] wobei insb. das Verhalten des Betroffenen (wie bekannte einschlägige Handlungen im Ausland, auch wenn diese dort nicht strafbar sind),[49] und die Dauer seines Wohlverhaltens[50] berücksichtigt werden müssen. Jedenfalls sind die konkreten Umstände im Einzelfall zu prüfen,[51] da allgemeine Umstände oder Prognosen wie eine statistische Rückfallsvermutung für eine weitere Verarbeitung nicht genügen.[52] Auch die spezialpräventive Wirkung des Wissens des Betroffenen über die Speicherung seiner Daten ist kein rechtfertigender Grund von der Löschung der Daten abzusehen.[53]

[Rz 43] § 74 Abs. 1 SPG sah[54] hierbei in ähnlicher Weise vor, dass auf Antrag des Betroffenen derartige Daten, die gem. § 65 Abs. 1 SPG ermittelt wurden, sofern nicht die Voraussetzungen des § 73 SPG vorliegen, zu löschen sind, wenn der Verdacht, der für ihre Verarbeitung maßgeblich ist, schließlich nicht bestätigt werden konnte oder wenn die Tat nicht rechtswidrig war. Dem Antrag war nicht stattzugeben, wenn weiteres Verarbeiten deshalb erforderlich ist, weil aufgrund konkreter Umstände zu befürchten ist, der Betroffene werde gefährliche Angriffe begehen.

[Rz 44] Den VfGH[55] beschäftigte die Reichweite und die Verhältnismäßigkeit des Begriffs des gefährlichen Angriffs im Hinblick auf § 73 Abs. 1 Z. 4 SPG und § 74 SPG und auch die Verhältnismäßigkeit der Ermittlung und Speicherung von DNA-Daten gem. § 67 Abs. 1 erster Satz SPG. So sah § 67 SPG die gesetzliche Ermächtigung zum Ermitteln der DNA eines Menschen schon vor, wenn der Betroffene in Verdacht stand, einen gefährlichen Angriff begangen zu haben. Durch die Anknüpfung an die in § 16 SPG vorgenommene Begriffsbestimmung des gefährlichen Angriffs wurden jedoch selbst Vorsatztaten der leichtesten Vermögenskriminalität erfasst. Der Gesetzgeber verabsäumte es hinsichtlich der verschiedenen Deliktstypen zu differenzieren oder manche überhaupt auszunehmen. Hinzu kommt, dass § 67 Abs. 1 erster Satz SPG keine hinreichenden Kriterien enthielt, welche die im Einzelfall vorzunehmende Prognoseentscheidung entsprechend determinieren würden. Wegen der unzureichenden Determiniertheit erklärte der VfGH § 67 Abs. 1 SPG daher als verfassungswidrig und der Gesetzgeber erließ[56] daraufhin einen neu formulierten § 67 Abs. 1 SPG, der die Reichweite auf eine mit mindestens einjähriger Freiheitsstrafe bedrohte, vorsätzliche, gerichtlich strafbare Handlung einschränkt.

[Rz 45] Im Fall des § 73 Abs. 1 Z. 4 SPG nahm der VfGH in verfassungskonformer Interpretation an, dass er dahin gehend ausgelegt werden kann, dass zu den im SPG vorgesehenen Löschungstatbeständen die allgemeinen Grundsätze über die Verwendung von Daten inkl. dem Verhältnis-

47 Wallnöfer, in: Thanner/Vogl (Fn. 20), § 73 Anm. 6.

48 VwGH 28. Juni 2005, 2002/01/0235.

49 VwGH 24. Juni 1998, 97/01/0261.

50 VwGH 2. Oktober 2001, 2000/01/0229; VwGH 28. Juni 2005, 2002/01/0082.

51 VwGH 28. Februar 2008, 2007/21/0508 = VwSlg 17389 A/2008.

52 Gerhard Pürstl/Manfred Zirnsack, SPG Sicherheitspolizeigesetz, 2. Auflage, Manz Verlag, Wien 2011, § 73 Anm. 12.

53 VwGH 30. Januar 2001, 2000/01/0061; VwGH 2. Oktober 2001, 2000/01/0229.

54 VfGH 12. März 2013, G 76/12 = jusIT 2013/50, 105 (Jahnel).

55 VfGH 12. März 2013, G 76/12 = jusIT 2013/50, 105 (Jahnel).

56 Bundesgesetz, mit dem das Sicherheitspolizeigesetz geändert wird (SPG-Novelle 2014), BGBl. I 43/2014.

mäßigkeitsgrundsatz nach dem DSG hinzutreten. Daher erlaubt § 73 Abs. 1 SPG im Einzelfall eine angemessene Abwägung und Gewichtung des Interesses des Betroffenen an der Geheimhaltung bzw. Löschung seiner personenbezogenen Daten. Damit wurde der § 73 Abs. 1 Z. 4 SPG als nicht verfassungswidrig angesehen.

[Rz 46] Im Fall des § 74 Abs. 1 und 2 SPG sah es der VfGH jedoch anders und hob diese Bestimmungen auf, da sie nach seiner Ansicht unzweifelhaft eine abschließende Regelung darstellten.

[Rz 47] Daher ist zur Löschung von erkennungsdienstlich verarbeiteten Daten in der regionalen erkennungsdienstlichen Evidenz gem. § 70 SPG, sowie in der Zentralen erkennungsdienstlichen Evidenz gem. § 75 SPG, der § 73 SPG und nach Wegfall des *lex specialis* § 74 Abs. 1 und 2 SPG der § 27 DSG 2000 maßgeblich.

3.2. Löschung der Daten der Ermittlungsmaßnahmen der StPO

[Rz 48] Für das Löschen von Daten, die im Rahmen der StPO verarbeitet wurden, sind §§ 74 und 75 StPO anzuwenden. § 74 StPO erklärt als Grundsatzbestimmung das DSG auch im Rahmen des Strafverfahrens für anwendbar, sofern in der StPO nicht im Einzelnen anderes bestimmt wird, wobei § 75 StPO i.d.S. materienspezifische Regelungen zum Berichtigen, Löschen und Sperren von Daten enthält. § 75 Abs. 4 StPO widmet sich den personenbezogenen Daten, die ausschließlich aufgrund einer Identitätsfeststellung (§ 118 StPO), einer körperlichen Untersuchung (§ 123 StPO) oder einer molekulargenetischen Analyse (§ 124 StPO) gewonnen werden. Demnach dürfen diese personenbezogenen Daten nur so lange verwendet werden, als wegen der Art der Ausführung der Tat, der Persönlichkeit der betroffenen Person oder aufgrund anderer Umstände zu befürchten ist, dass diese Person eine strafbare Handlung mit nicht bloß leichten Folgen begehen werde. Die Daten sind zu löschen, wenn der Angeklagte rechtskräftig freigesprochen oder das Ermittlungsverfahren ohne Vorbehalt späterer Verfolgung eingestellt wird. § 75 Abs. 4 StPO trägt damit dem im DSG verankerten Zweckbindungsgrundsatz Rechnung.

[Rz 49] Es scheint jedoch so, als ob § 75 Abs. 4 StPO nur den Verdächtigen im Auge hätte. Die angeführten Ermittlungsmaßnahmen sind jedoch auch gegenüber anderen Personen zulässig. So darf z.B. die Identitätsfeststellung nach § 118 StPO auch an Personen durchgeführt werden, die über die Umstände der Tatbegehung Auskunft geben können, also an potentiellen Zeugen und an Personen, die Spuren hinterlassen haben, die der Aufklärung dienen können (§ 118 Abs. 1 StPO). Wenn man davon ausgehen würde, den § 75 StPO als abschließende Spezialnorm gegenüber dem DSG zu sehen, hätte nur der Verdächtige eine Chance auf Löschung der Daten vor Ablauf der maximalen Speicherfristen des § 75 StPO. Daher muss man bedenken, dass § 74 StPO die Geltung des DSG anordnet, sofern die StPO im Einzelnen nichts anderes bestimmt. Nur in Bezug auf die fraglichen Erhebungen für den Verdächtigen ist tatsächlich auch etwas anderes bestimmt, wonach auch nur für ihn § 75 Abs. 4 StPO als abschließende Spezialnorm zu gelten hat. Für alle anderen von Ermittlungsmaßnahmen Betroffenen treten daher die allgemeinen Verwendungsgrundsätze des DSG neben § 75 StPO. Danach sind die Daten zu löschen, sobald sie nicht mehr benötigt werden und ihre Zweckbindung entfällt, also mitunter schon vor Ablauf der weiteren Fristen des § 75 StPO.[57]

[57] Susanne Reindl-Krauskopf, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit – Bemerkungen zum vorliegenden Gutachten aus strafrechtlicher Sicht, in 18. ÖJT Band I/2 (2013) 146 (150 f).

[Rz 50] Diese Höchstfristen gem. § 75 Abs. 2 und 3 StPO besagen nämlich, dass der Zugriff auf Namensverzeichnisse nach Ablauf von zehn Jahren ab den im Gesetz festgelegten Zeitpunkten zu unterbinden ist und nach 60 Jahren ab den genannten Zeitpunkten alle Daten im direkten Zugriff zu löschen sind. Diese Zeitpunkte sind im Fall der Verurteilung jener Zeitpunkt, ab dem die Strafe vollzogen wurde, die Verurteilung, falls eine Strafe nicht ausgesprochen oder bedingt nachgesehen wurde und die Entscheidung, mit der ein Freispruch, eine Einstellung des Verfahrens oder ein (endgültiger) Rücktritt erfolgte. Durch das Sperren des Zugriffs auf Namensverzeichnisse erreicht § 75 Abs. 2 StPO, dass ab diesen Zeitpunkten die Daten unbescholtener Personen nicht mehr über Namensabfrage im ADV (automationsunterstützte Datenverarbeitung-System der Justiz verfügbar sind und garantiert damit das Recht auf Geheimhaltung i.S.d. § 1 DSG 2000.[58]

[Rz 51] Hierbei stellt sich jedoch die Frage, ob eine 60-jährige Speicherdauer jedenfalls und für alle Strafverfahren – unabhängig von der Schwere des Tatvorwurfs und der Art ihrer Beendigung (Freispruch, Schuldspruch, Einstellung, usw.) – im öffentlichen Interesse liegt, das das Individualinteresse des Betroffenen an der Löschung der Daten überwiegt. Da § 75 StPO das Regime des DSG hinsichtlich der Löschung von Daten nicht abschließend ersetzt, lässt es nach Reindl-Krauskopf[59] jedoch die Interpretation zu, dass sich aus § 74 StPO i.V.m. § 27 DSG 2000 ergibt, dass die Daten zu löschen sind, sofern sie nicht mehr für die Aufgabenerfüllung benötigt werden, es sei denn, dass ihre Archivierung rechtlich zulässig ist und dass der Zugang zu diesen Daten besonders geschützt ist. Auch wenn § 75 Abs. 3 StPO eine solche Archivierungsregel ist, so kann man bei Heranziehen des Grundrechts des § 1 DSG 2000 den § 75 Abs. 3 StPO i.V.m. dem Verhältnismäßigkeitsgrundsatz des § 5 StPO dahingehend auslegen, dass dieser nur auf jene personenbezogenen Daten anzuwenden ist, die im Dienste der Strafrechtspflege ermittelt und verwendet wurden und deren weitere Speicherung für diese Zwecke auch im jeweiligen Einzelfall noch erforderlich ist. Sollte somit jemand vor Ablauf der Frist des § 75 Abs. 3 StPO einen Antrag auf Löschung stellen, müsste geprüft werden, ob die weitere Speicherung noch notwendig ist und dabei eine Abwägung zwischen dem Individualinteresse des Betroffenen an der Datenlöschung und dem Interesse der Allgemeinheit an der weiteren Verwendung der Daten für strafrechtliche Zwecke vorgenommen werden. Gegebenenfalls wären somit die Daten auch schon vor Ablauf der Höchstfrist von 60 Jahren des § 75 Abs. 3 StPO zu löschen.[60]

3.3. Löschung aus dem Strafregister

[Rz 52] Nach der Verurteilung und der Übermittlung der Strafkarten an die Landespolizeidirektion Wien hängt es maßgeblich von den Tilgungsfristen ab, wann der Eintrag im Strafregister gelöscht werden muss. § 12 StRegG bestimmt, dass die Löschung von den die getilgte Verurteilung und den Verurteilten betreffenden Daten nach Ablauf von zwei Jahren nach Eintritt der Tilgung zu erfolgen hat.

[Rz 53] Wann die Tilgung eintritt, wird im TilgG geregelt. In § 2 TilgG ist geregelt, dass die Tilgungsfrist beginnt, sobald alle Freiheits- oder Geldstrafen und die mit Freiheitsentzug verbundenen vorbeugenden Maßnahmen vollzogen sind, als vollzogen gelten, nachgesehen worden sind oder nicht mehr vollzogen werden dürfen. Ist keine Freiheits- oder Geldstrafe verhängt wor-

58 Reindl-Krauskopf, ÖJT (Fn. 57), 146 (151).

59 Reindl-Krauskopf, ÖJT (Fn. 57), 146 (153)

60 VfGH 29. Juni 2012, G 7/12 = VfSlg 19659/2012 = jusIT 2012/87, 187 (Jahnel).

den oder sind die verhängten Freiheits- oder Geldstrafen durch Anrechnung einer Vorhaft zur Gänze verbüßt und ist auch keine mit Freiheitsentziehung verbundene vorbeugende Maßnahme angeordnet worden, so beginnt die Frist schon mit Rechtskraft der Verurteilung.

[Rz 54] Dabei wird im TilgG zwischen den Tilgungsfristen bei einer einzelnen Verurteilung und mehreren Verurteilungen unterschieden. Gem. § 3 TilgG tritt die Tilgung nach dem Ablauf bestimmter Grundfristen (§ 3 TilgG) ein, die sich im Fall von mehreren Verurteilungen verlängern (§ 4 TilgG), es sei denn die anderen Verurteilungen sind erst nach Ablauf der Tilgungsfrist erfolgt (§ 4 Abs. 1 TilgG). Die Tilgungsfristen bestimmen sich je nach Art und Höhe der Verurteilung und reichen von drei bis fünfzehn Jahren, jedoch ist es für das Ausmaß der Tilgungsfrist ohne Bedeutung, ob die Strafe bedingt nachgesehen worden ist oder nicht, da dies nur Einfluss auf den Beginn der Tilgungsfrist hat.[61]

[Rz 55] Nach § 3 Abs. 1 Z. 1 TilgG beträgt die Tilgungsfrist *drei* Jahre, wenn der Täter nur wegen Jugendstraftaten zu einem Schuldspruch ohne Strafe nach § 12 des Jugendgerichtsgesetzes (JGG) oder einem Schuldspruch unter Vorbehalt der Strafe nach § 13 JGG verurteilt wurde. Bei jeder anderen Verurteilung nur wegen Jugendstraftaten beträgt die Tilgungsfrist *fünf* Jahre, unabhängig vom Ausmaß der verhängten Strafe. *Fünf* Jahre beträgt die Tilgungsfrist auch gem. § 3 Abs. 1 Z. 2 TilgG bei Verurteilungen zu einer höchstens einjährigen Freiheitsstrafe, nur zu einer Geldstrafe oder zu weder einer Freiheitsstrafe noch zu einer Geldstrafe, wobei eine Verurteilung zu «weder einer Freiheits- noch zu einer Geldstrafe» nach geltendem Strafgesetzbuch (StGB) nicht mehr vorgesehen ist.[62]

[Rz 56] Nach § 3 Abs. 1 Z. 3 und 4 TilgG beträgt die Tilgungsfrist *zehn* Jahre bei einer Verurteilung auf eine Freiheitsstrafe von mehr als einem Jahr und höchstens auf drei Jahre. Sie beträgt *fünfzehn* Jahre bei einer Verurteilung zu einer Freiheitsstrafe von mehr als drei Jahren oder bei der Anordnung der Unterbringung eines zurechnungsunfähigen Rechtsbrechers in einer Anstalt für geistig abnorme Rechtsbrecher nach § 21 Abs. 1 StGB.

[Rz 57] Bei Verurteilungen wegen Sexualstraftaten verlängert sich die Tilgungsfrist gem. § 4a TilgG um das Einfache. Gem. § 5 TilgG sind jedoch Verurteilungen zu lebenslanger Freiheitsstrafe nicht tilgbar und schließen darüber hinaus auch die Tilgung aller anderen Verurteilungen aus.

[Rz 58] Ist die Tilgung der Verurteilung nach Ablauf der Tilgungsfristen des TilgG eingetreten, so sind die betreffenden Daten aus dem Strafregister nach Ablauf von zwei Jahren zu löschen. Diese Löschung ist von der Tilgung, also der rechtlichen Löschung, zu unterscheiden, die bereits jede Verwertung ausschließt und ermöglicht noch für zwei Jahre die Auswertung der Daten über die eingetretene Tilgung hinaus zu nicht personenbezogenen wissenschaftlichen Untersuchungen gem. § 13a StRegG.[63]

[Rz 59] Der Betroffene selbst, dessen Daten hinsichtlich der Verurteilung, Verfügung, Entschließungen und dgl. in das Strafregister aufgenommen wurden, hat über § 8 StRegG die Möglichkeit eine Feststellung zu beantragen, ob die Aufnahme in das Strafregister unrichtig oder unzulässig war, die Aufnahme hätte erfolgen müssen oder die Verurteilung getilgt ist. Der Feststellungsantrag ist beim BMI einzubringen, der darüber entscheidet, ob dem Antrag Folge gegeben wird oder nicht. Gem. § 13c StRegG ist gegen diesen Feststellungsbescheid die Beschwerde an das

61 Eder-Rieder (Fn. 31), § 3 A 1.

62 Eder-Rieder (Fn. 31), § 3 B 1 b.

63 Eder-Rieder (Fn. 31), § 12 Anm. zu § 12.

Landesverwaltungsgericht möglich und in weiterer Folge die Revision an den VwGH gegen die Erkenntnisse des Landesverwaltungsgerichts (Art. 133 Abs. 1 Z. 1 B-VG).

[Rz 60] Das in § 8 StRegG geregelte Rechtsschutzverfahren ermöglicht jedoch nur die Überprüfung der Zulässigkeit, Richtigkeit und Vollständigkeit einer Registereintragung durch das Bundesministerium für Inneres zum Zeitpunkt der Antragstellung. Die Beurteilung der Unbedenklichkeit des Datenbestandes ist jedoch beschränkt auf die Frage des Vorliegens eines allfälligen, (primär) im Bereich der Strafregisterbehörde unterlaufenen Fehlers der Eintragung. Das Gesetz bietet hierbei keine Möglichkeit, im Rahmen eines solchen Feststellungsverfahrens vor dem Bundesministerium für Inneres die Überprüfung der materiellen Richtigkeit des Strafurteils oder einer darauf bezogenen Gerichtsentscheidung herbeizuführen und die allfällige Löschung der Speicherung einer (nicht getilgten) Verurteilung ohne gerichtliche Anordnung zu erwirken.[64]

4. Zwischenergebnis

[Rz 61] Im öffentlichen Bereich führen die Bindung an die gesetzliche Zuständigkeit als Voraussetzung für die Datenverarbeitung und die Vielzahl an Entscheidungen der DSK und der Höchstgerichte zu einem in den meisten Fällen klaren und doch flexiblen Regelungswerk. Ein konventioneller Papierakt fällt dabei generell nicht unter das Recht auf Löschung, jedoch werden auch Fälle zugelassen, bei denen ein Papierakt mit einer gewissen Ordnung und Strukturiertheit doch auf Antrag des Betroffenen gelöscht werden muss. Auch die in den Vorschriften der EKIS und der StPO explizit erwähnte Subsidiarität des § 27 DSG 2000 trägt hierbei soweit zur Rechtssicherheit bei, dass die Durchsetzung des Rechts auf Löschung auf Grundlage der *lex specialis* und des § 27 DSG 2000 gegen Auftraggeber des öffentlichen Bereichs gewährleistet ist. So wird in den Vorschriften des SPG und der StPO stets dem Zweckbindungsgrundsatz des § 6 Abs. 1 Z. 2 DSG 2000 sowie dem Wesentlichkeitsgrundsatz des § 6 Abs. 1 Z. 3 DSG 2000 Rechnung getragen, um einer Ausuferung der Datenverarbeitung durch die öffentliche Hand entgegen zu wirken.

III. Löschung im privaten Bereich

[Rz 62] Im privaten Bereich stellen sich wie auch im öffentlichen Bereich einige Problemfelder in Hinblick auf die Zulässigkeit der Verarbeitung von Nutzerdaten. Insbesondere im Internetzeitalter machen dabei neben europäischen Unternehmen besonders amerikanische Online-Unternehmen wie Facebook Inc. und Google Inc. von sich reden, da sie ihren Verträgen meist sehr vage, undurchsichtige und fragwürdige Datenverwendungsrichtlinien und Nutzerbestimmungen zugrunde legen. Meist hängt die Zulässigkeit der Datenverarbeitungen von der Zustimmung ab, jedoch stellt sich die Frage, wie weit die Reichweite des zugestimmten Zwecks ist und was passiert, wenn die Zustimmung widerrufen und dadurch die Verarbeitung unzulässig wird oder eine Interessenabwägung durchgeführt werden muss.

64 VfGH 4. Oktober 2006, B 742/06 = VfSlg 17948/2006; VwGH 19. April 2012, 2011/01/0186; VwGH 21. März 2007, 2006/05/0076.

1. Facebook

[Rz 63] Der Begriff des sozialen Netzwerkdienstes wird in der Stellungnahme zur «Nutzung sozialer Online-Netzwerke» der *Artikel-29-Datenschutzgruppe* passend als Kommunikationsplattformen im Online-Bereich definiert, die es dem Einzelnen ermöglichen, sich Netzwerken von gleich gesinnten Nutzern anzuschließen bzw. solche zu schaffen. Im rechtlichen Sinn handelt es sich bei den sozialen Netzwerken um Dienstleistungen der Informationsgesellschaft i.S.d. Art. 1 Nr. 2 der Richtlinie 98/34/EG in der durch die Richtlinie 98/48/EG geänderten Fassung. Bei allen sozialen Netzwerkdiensten sind dabei bestimmte Merkmale ähnlich. So werden die Nutzer aufgefordert, personenbezogene Daten zur Erstellung einer Beschreibung von sich selbst bzw. eines selbst generierten persönlichen «Profils» anzugeben. Die sozialen Netzwerkdienste bieten daneben auch Funktionen an, mit denen die Nutzer ihr eigenes Material (selbst generierte Inhalte wie z.B. Bilder oder Tagebucheinträge, Musik- und Videoclips oder Links zu anderen Webseiten) dort veröffentlichen können. Die Nutzung der sozialen Netzwerke erfolgt dabei über die jedem Nutzer bereitgestellten Funktionen samt Kontaktliste bzw. Adressbuch, mittels derer die Verweise auf die anderen Mitglieder der Netzgemeinschaft verwaltet und zu Interaktionen mit diesen genutzt werden können.[65]

[Rz 64] Nach einer Studie von BITKOM sind vier von fünf (78%) der deutschen Internetnutzer in einem sozialen Netzwerk aktiv, bei Facebook in Deutschland allein über 20 Millionen,[66] in Österreich 3,4 Millionen.[67] Dabei werden die Einnahmen von sozialen Netzwerken wie Facebook zum Großteil aus Werbung erzielt, die auf den Webseiten eingeblendet wird und von den Nutzern angeklickt werden kann. Die Werbung wird dabei gezielt auf die Interessen der Nutzer zugeschnitten («behavioral advertising»), wobei die Grundlage dafür den selbst eingestellten Profildaten, aber auch der Erfassung des Nutzerverhaltens («behavioral tracking») entstammt. Darüber hinaus werden Nutzungsprofile im Internet durch auf mobiler Dienstnutzung basierenden «location based services» ergänzt, die das geografische Auffinden von Personen ermöglichen («friend finder»). Das Sammeln von Daten über Lebensläufe von Einzelnen, dessen Vorlieben, Eigenschaften, Krankheiten und das Wissen über Gruppen hat sich zu einem lukrativen Geschäft entwickelt, sodass Daten seit geraumer Zeit als die Währung des Internets gelten.[68]

[Rz 65] Dieses Geschäftsmodell, das als «Web 2.0» bezeichnet wird und die Verschiebung der Produktion von Inhalten vom Betreiber einer Internetseite zum Nutzer («nutzergenerierte Inhalte») beschreibt, betreibt auch Facebook. Die Nutzung des Dienstes ist für den Nutzer «kostenlos» und Facebook entfallen die Produktions und Redaktionskosten von Inhalten, sodass der Nutzer heute nicht mehr nur passiver Informationsnutzer, sondern gleichzeitig aktiver Informationsanbieter ist und nicht nur Informationen über sich selbst, sondern auch intime Informationen über Dritte, Familie, Freunde etc einstellt.[69]

---

65 Art. 29-Datenschutzgruppe, Stellungnahme 5/2009 zur Nutzung sozialer Online Netzwerke, WP 163, 01189/09/DE, 5 (ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_de.pdf).

66 BITKOM, Soziale Netzwerke – dritte, erweiterte Studie, 29. August 2011 (bitkom.org/de/publikationen/38338_77778.aspx [abgerufen am 8. Oktober 2014]).

67 socialmediaradar.at/facebook (abgerufen am 8. Oktober 2014).

68 Andreas Wiebe, Datenschutz in Zeit von Web 2.0 und BIG DATA – dem Untergang geweiht oder auf dem Weg zum Immaterialgüterrecht?, ZIR 2014, 35 (35 f).

69 Vgl. Maximilian Schrems, Klageschrift gegen Facebook Ireland Limited (31. Juli 2014), Rz. 10 ff. und 18 ff. (europe-v-facebook.org/sk/sk.pdf); Wiebe, ZIR (Fn. 68), 35 (36).

[Rz 66] Bei der Registrierung auf *facebook.com* geht der Nutzer, wie bei anderen sozialen Netzwerken und Diensten auch, einen Vertrag ein, der vom Betreiber verfassten Nutzungsbedingungen und Datenschutzrichtlinien unterliegt. Der Vertragspartner ist hierbei Facebook Ireland Limited[70] mit Niederlassung und Sitz im irischen Dublin und unterliegt dem irischen Datenschutzgesetz (Data Protection (Amendment) Act 2003 [DPA]). Facebooks Datenschutzrichtlinien[71] müssen laut der Art. 29-Datenschutzgruppe den Vorgaben der DSRL entsprechen, auch wenn die Niederlassung der Muttergesellschaft Facebook Inc. in den USA liegt,[72] die Nutzungsbedingungen als alleinigen Gerichtsstand das im nördlichen Bezirk von Kalifornien zuständige US-Bezirksgericht nennen und die Gesetze des Bundesstaats Kalifornien für anwendbar erklären.[73] Nur für Nutzer mit Wohnsitz in Deutschland sind von Facebook jedoch interessanterweise eigene Sonderbedingungen[74] vorgesehen, welche unter anderem an Stelle von kalifornischem Recht deutsches Recht für anwendbar erklären. Im Grunde ist aber auch ohne Sonderbedingungen für österreichische Nutzer das österreichische Datenschutzgesetz bzw. die DSRL anzuwenden.

[Rz 67] Dabei muss man zuerst natürlich bedenken, dass das Grundrecht auf Geheimhaltung nur für Daten besteht, die einen Personenbezug aufweisen und nicht öffentlich zugänglich sind bzw. nicht rechtmäßig veröffentlicht wurden. Ohne Zweifel besteht der Personenbezug bei Daten, wie Name, Geburtsdatum, Beziehungsstatus sowie Fotos und Videos, auf denen der Betroffene selbst abgebildet ist. Aber auch Beiträge und Kommentare enthalten den Nutzernamen und die Verknüpfung mit dem Nutzerprofil sowie meist Informationen über die Beziehung des Nutzers zu anderen Menschen oder über sein Freizeitverhalten. Diese Angaben sind ebenfalls wie Bilder und Videos, auf denen der Nutzer selbst nicht abgebildet ist, sich aber auf ein bestimmtes Verhalten des Nutzers schließen lässt, als personenbezogene Daten zu qualifizieren.[75]

[Rz 68] Wenn die Daten des Nutzers zwar personenbezogen, jedoch allgemein verfügbar und öffentlich zugänglich sind, so verliert der Nutzer ebenfalls den Schutz auf Geheimhaltung. Allgemein verfügbar sind die Daten dann, wenn sie «zulässigerweise veröffentlicht» wurden,[76] also für jedermann auffindbar sind und diese Kenntnisnahmemöglichkeit jedenfalls im Zeitpunkt der Datenverwendung noch besteht.[77] Darüber hinaus muss der Akt der Veröffentlichung rechtmäßig erfolgen, was bei der Veröffentlichung durch den Nutzer selbst in jedem Fall anzunehmen ist.[78] Stammdaten, wie das Profilbild oder der Name des Profils, für welche es keine Einschränkungsmöglichkeit gibt, gelten als solche allgemein verfügbaren Daten. Werden die Daten jedoch nur einer bestimmten Gruppe zugänglich gemacht (nur Freunden), bleibt der Geheimhaltungs-

70 Facebook Ireland Limited, Nutzungsbedingungen von Facebook in der Fassung 15. November 2013 (Erklärung der Rechte und Pflichten), 19.1. (facebook.com/terms.php?locale=DE [abgerufen am 8. Oktober 2014]) für die Nutzer außerhalb der USA und Kanada, ansonsten ist der Vertragspartner Facebook Inc.

71 Facebook Ireland Limited, Datenverwendungsrichtlinien von Facebook in der Fassung 15. November 2013 (facebook.com/full_data_use_policy [abgerufen am 8. Oktober 2014]) außerhalb der USA und Kanada.

72 Art. 29-Datenschutzgruppe, Arbeitspapier über die Frage der internationalen Anwendbarkeit des EUDatenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU, WP 56, 5035/01/DE/endg. (ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_de.pdf).

73 Facebook Ireland Limited, Nutzungsbedingungen (Fn. 70), 16.1.

74 Facebook Ireland Limited, Für Nutzer mit Wohnsitz in Deutschland: (facebook.com/terms/provisions/german/index.php [abgerufen am 10. Dezember 2014]).

75 Arzu Sedef, The Social Network – (k)ein Recht auf Datenlöschung?, Zak 2011/351, 183; Jahnel, Datenschutzrecht (Fn. 2), Rz. 3/71 f.

76 Jahnel, Datenschutzrecht (Fn. 2), Rz. 2/18.

77 DSK 25. Februar 2009, K121.419/0007-DSK/2009.

78 Jahnel, Datenschutzrecht (Fn. 2), Rz. 2/18; § 9 Z. 1 DSG 2000.

schutz aufrecht, weil nicht von einer allgemeinen Verfügbarkeit gesprochen werden kann und daher benötigt Facebook für die Verarbeitung dieser Daten einen Rechtfertigungsgrund i.S.d. § 8 und 9 DSG 2000.[79] Auch wenn die Daten einer Vielzahl an Freunden zugänglich ist, so ändert dies nichts an der Tatsache, dass deren Kreis vom betroffenen Nutzer begrenzt worden ist und er es in der Hand hat zu bestimmen, wer zugriffsberechtigt sein soll.[80]

[Rz 69] Im Hinblick auf die Daten, die der Nutzer selbst auf Facebook hochlädt und beim Anwenden der DSG-Grundsätze stellt man weiters fest, dass der Nutzer, der sein eigenes Profil bei Facebook anlegt, selbst als Auftraggeber «seiner eigenen Daten» fungiert und zudem aber naturgemäß auch Betroffener ist («Doppelnatur»). Per se wäre diese Konstellation auch nicht bedenklich, da die Zulässigkeit hierbei nicht in Frage gezogen werden muss. Solange der Nutzer die «Herrschaft» über seine eigenen Daten nicht verliert, gibt es keinen datenschutzrechtlichen Regelungsbedarf, da als Auftraggeber nur derjenige gelten kann, der Daten eines anderen verarbeitet.[81]

[Rz 70] Problematisch wird es erst, wenn der Nutzer personenbezogene Inhalte Dritter einstellt, etwa durch das Hochladen von Daten oder Bildern von Freunden und Bekannten auf seinen Account, da der Nutzer durch den Gestaltungsspielraum, «ob» und «wie» er die Daten verarbeitet, als Auftraggeber für die Datenverarbeitung anzusehen ist, wobei Facebook nur als Dienstleister tätig wird. In den meisten Fällen wird diese Verarbeitung jedoch von der Ausnahme der Verantwortlichkeit des § 45 DSG 2000, wenn eine Datenverarbeitung ausschließlich zur Ausübung persönlicher oder familiärer Tätigkeit vorgenommen wird, gedeckt sein, auch wenn die Reichweite dieser Ausnahme unklar ist. Eine Nutzung der Plattform zur Förderung kommerzieller, politischer oder karitativer Zwecke wird die Grenzen der Ausnahmeklausel jedenfalls überschreiten.[82] Als Indiz für eine entsprechende Nutzung nennt die Art. 29-Datenschutzgruppe[83] eine hohe Zahl von Drittkontakten. Dies ist bei sozialen Netzwerken jedenfalls anzunehmen, wenn der Zugriff auf die hochgeladenen Daten über die vom Nutzer ausgewählten Kontakte hinausgeht und allen Mitgliedern des Netzwerks Zugang gewährt wird oder die Daten von externen Suchmaschinen indexiert werden können. Auch die Nutzung von Profilen zu beruflichen oder geschäftlichen Zwecken wird die Anwendung der Ausnahme ausschließen. Hierbei bräuchte der Nutzer somit zur Verarbeitung der Daten von Dritten die Einwilligung der betroffenen Person.

[Rz 71] Wenn der Nutzer die «Herrschaft» über seine eigenen Daten und die Daten Dritter durch eine von Facebook vorgenommenen Datenanwendung verliert, dann kann der Nutzer jedoch nach dem DSG nicht mehr als Auftraggeber qualifiziert werden, da Facebook allein darüber entscheidet, «ob» und «wie» die Daten verarbeitet werden. Facebook versucht in seinen Nutzungsbedingungen[84] zwar, den Nutzer als Auftraggeber bzw. als verantwortliche Stelle der Verarbeitung zu benennen, jedoch ist diese Ansicht in Hinblick auf die Frage, inwieweit der Nutzer für alles, was Facebook auch in Zukunft mit den Daten machen darf, ohne, dass der Nutzer eine Möglichkeit der Einflussnahme darauf hat, datenschutzrechtlich nicht wirklich tragbar.[85] Daher muss Facebook dabei als Auftraggeber i.S.d. DSG und der Nutzer als Betroffener angesehen werden.

---

79 Peter Burgstaller, Soziale Netzwerke. Eine rechtliche Einführung, lex:itec 2012 H 2-3, 16 (17).

80 Günther Leissler, Social Networks – Datenschutz in der vernetzten Welt, ecolex 2010, 834.

81 Burgstaller, lex:itec (Fn. 79), 16 (17); § 4 Z. 1, 3 und 4 DSG 2000.

82 Wiebe, ZIR (Fn. 68), 35 (43).

83 Art. 29-Datenschutzgruppe, WP 163 (Fn. 65), 6.

84 Facebook Ireland Limited, Nutzungsbedingungen (Fn. 70), 2.

85 Wiebe, ZIR (Fn. 68), 35 (44).

[Rz 72] Es ergibt sich daraus also eine Zweiteilung der Rollenverteilung, je nachdem wer die Verarbeitung der Daten vornimmt. Für die Verarbeitung seitens Facebook wird jedenfalls sogar eine ausdrückliche Zustimmung des Betroffenen notwendig sein, wenn sensible Daten verarbeitet werden, was durch die Verknüpfung von nicht-sensiblen mit sensiblen Daten in der Mehrheit der Fälle zutreffen wird.[86] Die Zustimmung, ob konkludent oder ausdrücklich, kann laut OGH «in Kenntnis der Sachlage» gem. § 4 Z. 14 DSG 2000 jedenfalls nur erfolgen, wenn die konkreten Daten, der konkrete Zweck und gegebenenfalls die konkreten Empfänger von Übermittlungen abschließend und transparent genannt werden. Eine demonstrative Aufzählung der Daten durch das Wort «etwa» und «z.B.» sowie «zum Zweck der Bereitstellung von Diensten» ist dabei keine Einschränkung, zu intransparent und als Zweck zu weit gefasst. Im Rahmen der Übermittlung von Daten an Dritte fehlt der Wendung «soweit notwendig» jedenfalls jede Bestimmtheit.[87]

[Rz 73] Die Datenverwendungsrichtlinien[88] von Facebook sollten für eine rechtmäßige Zustimmung also die konkreten Daten, den konkreten Zweck und die konkreten Empfänger der Daten der Verarbeitung enthalten. Tatsächlich verwendet Facebook aber zahlreiche Generalklauseln, welche nur mit vagen, demonstrativen und verharmlosenden Beispielen erläutert werden. So findet sich gleich am Anfang unter der Überschrift «Informationen, die wir über dich erhalten» eine Generalklausel («Wir erhalten eine Vielzahl an verschiedenen Informationen über dich, einschließlich:») und eine demonstrative Aufzählung welche Daten des Betroffenen gesammelt werden. So sammelt Facebook «beispielsweise» Daten, wenn der Nutzer eine/n FreundIn hinzufügt, angibt, dass ihm eine Seite gefällt oder dass er sich in einer Beziehung befindet oder «zum Beispiel» in sonstiger Weise über Facebook kommuniziert. Facebook räumt sich in diesen Bestimmungen, die die Art der gesammelten Daten und die Quellen dieser Daten in keiner Weise einschränken, durch die generelle Zustimmung des Nutzers das Recht ein, jede Art von Daten des Nutzers von jeder beliebigen Quelle zu sammeln und sogar selbst neue personenbezogene Daten über den Nutzer zu schaffen.[89]

[Rz 74] Zum Zweck sagen die Datenverwendungsrichtlinien[90] unter der Überschrift «Wie wir die uns bereitgestellten Informationen verwenden», nach einer Generalermächtigung klingend, dass sie die ihnen bereitgestellten Informationen über den Nutzer im Zusammenhang mit den Dienstleistungen und Funktionen, die sie dem Nutzer und anderen Nutzern (wie zum Beispiel Freunden, ihren Partnern, den Werbetreibenden, die Werbeanzeigen auf Facebook buchen, sowie den Entwicklern genutzter Spiele, Apps und Webseiten) anbieten, verwenden. Daher ist jede erdenkliche Datenverwendung und alles, was mit den Dienstleistungen auch nur in Zusammenhang steht, offenbar von der Zustimmung des Nutzers umfasst. Des Weiteren räumt sich Facebook das Recht ein, nicht nur Facebook in seiner heutigen Form zur Verfügung zu stellen, sondern auch zukünftig innovative Funktionen und Dienstleistungen anzubieten, die sie unter neuartigem Einsatz der Informationen, die sie über den Nutzer erhalten, entwickeln. Dies schafft Facebook die Möglichkeit nicht nur die Daten für jeglichen denkbaren Zweck zu verwenden, sondern sogar

86 Burgstaller, lex:itec (Fn. 79), 16 (17).

87 OGH 14. November 2012, 7 Ob 84/12x = SZ 2012/115 = jusIT 2013/13, 26 (Thiele) = jusIT 2013/42, 87 (Thiele); OGH 22. Juni 2011, 2 Ob 198/10x = jusIT 2011/87, 181 (Thiele) = ZVR 2012/92, 166 (Kathrein).

88 Facebook Ireland Limited, Datenverwendungsrichtlinien (Fn. 61), Wir erhalten eine Vielzahl an verschiedenen Informationen über dich.

89 Schrems, Klageschrift (Fn. 69), Rz. 67 ff.

90 Facebook Ireland Limited, Datenverwendungsrichtlinien (Fn. 61), Wie wir die uns bereitgestellten Informationen verwenden.

für noch gar nicht vorstellbare Zwecke. Daher lassen die Datenverwendungsrichtlinien auch zum konkreten Zweck jedwede Einschränkung vermissen. Vielmehr wird die Zustimmung des Nutzers zu jeder Art der Datenverwendung für jeden Zweck, der derzeit oder zukünftig verfolgt wird, eingeräumt.[91]

[Rz 75] Faktisch lässt sich somit feststellen, dass die Nutzungsbedingungen und Datenverwendungsrichtlinien von Facebook in dieser Form den zwingenden gesetzlichen Vorgaben des DSG, der DSRL und der Rechtsprechung des OGH nicht gerecht werden.

[Rz 76] Man kann davon ausgehen, dass Facebook durch die sehr vagen, generalisierten und pauschalisierten Nutzungsbedingungen und Datenverwendungsrichtlinien vom Nutzer nie eine nach der österreichischen Rechtsprechung und der DSRL gültige Zustimmung erhalten hat und jedwede von Facebook durchgeführte Datenanwendung daher unzulässig ist. Da bei einer Interessenabwägung andere Gründe sehr wenig Aussicht auf Erfolg versprechen, wären gem. § 8 Abs. 1 Z. 4 i.V.m. Abs. 3 Z. 4 DSG jedenfalls nur Datenverarbeitungen von nichtsensiblen Daten rechtfertigbar, die zur Vertragserfüllung notwendig wären, was sich schon in der Datenverarbeitung zur Erbringung der Dienstleistung erschöpft. Jedwede darüber hinausgehende Auswertung der Daten z.B. für Werbung, Zusatzdienste, nicht unbedingt notwendige Auslagerungen der Datenverarbeitung, Kooperation mit Dritten und die Weitergabe der Daten an Dritte sind jedenfalls auch dadurch nicht gerechtfertigt.[92] Alle weiteren Verarbeitungen, insb. die Verarbeitung von sensiblen Daten, wären weiterhin nur mit der (ausdrücklichen) Zustimmung des Betroffenen zulässig.

[Rz 77] Die Datenverwendungsrichtlinien widersprechen darüber hinaus auch dem allgemeinen Grundsatz der Zweckbindung gem. § 6 Abs. 1 Z. 2 DSG 2000 mangels eines festgelegten, eindeutigen und rechtmäßigen Zwecks. Außerdem fehlt es auch an der Verknüpfung von Datenverarbeitungen mit den spezifischen Zwecken, die Daten werden über das erhebliche Maß i.S.d. § 6 Abs. 1 Z. 3 DSG 2000 (Wesentlichkeitsgrundsatz) und länger als für die Zweckerfüllung gem. § 6 Abs. 1 Z. 5 DSG 2000 notwendig verarbeitet,[93] sodass die Daten von Facebook ohnehin zu löschen wären. Im Grunde kann man sogar die Verwendung von Daten «nach Treu und Glauben» i.S.d. § 6 Abs. 1 Z. 1 DSG 2000 durch Facebooks Praktiken[94] und die Formulierungen der Nutzungsbedingungen und Datenverwendungsrichtlinien in Zweifel ziehen, da sie den Betroffenen über seine Rechte und über die Verwendung seiner Daten weitestgehend irreführen und im Unklaren lassen.

[Rz 78] Die Verarbeitung der Daten Dritter durch den Nutzer wird in vielen Fällen durch den Ausnahmetatbestand des § 45 DSG 2000 auch ohne Zustimmung des Betroffenen zulässig sein. Jedoch widerspricht wohl jede Verarbeitung der Daten, die durch Facebook durchgeführt wird, den Zulässigkeitsvoraussetzungen des DSG und die Datenverarbeitungen sind in Zukunft zu unterlassen bzw. alle gesammelten Daten sind zu löschen, wenn sie nicht direkt und klar von der Zustimmung des Nutzers bzw. des Betroffenen erfasst sind.

[Rz 79] Wie oben schon festgestellt, dürfte der Großteil der Daten, die von Facebook gesammelt werden, in Konformität mit den europäischen Datenschutzbestimmungen ohne gültige Zustim-

91 Schrems, Klageschrift (Fn. 69), Rz. 72 ff.

92 Schrems, Klageschrift (Fn. 69), Rz. 84.

93 Schrems, Klageschrift (Fn. 69), Rz. 85.

94 europe-v-facebook.org, Facebooks Datenbestand (www.europe-v-facebook.org/DE/Datenbestand/datenbestand.html).

mung erst gar nicht existieren und wäre dadurch auch ohne Antrag des Nutzers von Facebook zu löschen. Nur solche Daten, die vom Nutzer selbst veröffentlicht wurden und selbst in seinem Profil gespeichert werden, sind für die Verarbeitung auf den Servern von Facebook bis auf Widerruf erlaubt. Doch selbst bei diesen unterscheidet sich die Praxis vom in den Datenverwendungsrichtlinien Vereinbarten und dem gesetzlich Erlaubten erheblich. So räumt sich Facebook schon von vornherein das Recht ein, dass die Löschung mancher Daten bis zu 90 Tage dauern kann, da diese in Sicherungskopien und Protokolldateien weiterhin vorhanden bleiben, wobei eine Löschung des Kontos normalerweise einen Monat beanspruchen soll.[95] § 27 Abs. 4 DSG 2000 normiert für die Löschung aber eine gesetzliche Höchstfrist von acht Wochen. Demnach ist nach Stellen des Löschungsbegehrens in Form der Kontolöschung der Auftraggeber dazu verpflichtet, entweder dem Antrag auf Löschung innerhalb von acht Wochen nach Einlangen des Antrags zu entsprechen und dem Betroffenen davon Mitteilung zu machen oder der Auftraggeber hat schriftlich zu begründen, warum die verlangte Löschung nicht vorgenommen wird.[96]

[Rz 80] In den Datenverwendungsrichtlinien[97] von Facebook findet sich auch ein Punkt über die Löschung der Daten, die von Facebook erfasst wurden. Neben der Unklarheit, welche und wie viele Daten von Facebook tatsächlich erfasst wurden sowie welche Daten von der Zustimmung des Nutzers erfasst sein sollen, gestaltet sich aber selbst die dem Nutzer von Facebook zugestandene Löschung seiner Daten denkbar schwierig, da Facebook nur die Kontolöschung erwähnt, eine Löschung sämtlicher von Facebook erfassten Daten zwar durch den Wortlaut impliziert, jedoch nicht *expressis verbis* anspricht.

[Rz 81] Neben der 90-tägigen Löschungsfrist weist Facebook in den Datenverwendungsrichtlinien auch darauf hin, dass bestimmte Informationen darüber hinaus erforderlich sind, um dem Nutzer Dienste anbieten zu können, und diese Informationen daher erst nach der Kontolöschung gelöscht werden können und dass einige Dinge, die der Nutzer auf Facebook hochlädt, außerhalb des Kontos gespeichert werden und somit nicht bei der Kontolöschung gelöscht werden, sondern weiterhin erhalten bleiben. Dies wird wiederum verharmlost durch die beispielhafte Aufzählung «von in einer Gruppe geposteten Beiträgen» und «dem Senden einer Nachricht an einen Freund.»[98] De facto scheinen durch die Kontolöschung wohl nur Daten gelöscht zu werden, die auch in dem Konto gespeichert sind und Daten, die außerhalb des Kontos gespeichert werden, bleiben erhalten.

[Rz 82] Nicht nur die Speicherung der Daten bis zu 90 Tage nach der Löschung widerspricht der achtwöchigen Höchstfrist des § 27 Abs. 4 DSG 2000, sondern dem Nutzer ist auch völlig unklar, welche Daten in den Sicherungskopien und Protokolldateien länger bestehen können und welche Daten tatsächlich außerhalb des Kontos des Nutzers gespeichert werden und dadurch nicht der in den Datenverwendungsrichtlinien vereinbarten Löschungspflicht unterliegen.

[Rz 83] Europe versus facebook richtete mehrere Auskunftsersuchen an Facebook und erstellte aufgrund dieser eine Liste von Datengruppen, die nachweislich von Facebook gespeichert werden. Unter diesen Gruppen finden sich z.B. Namen, Passwörter, Telefonnummern, Freunde, Geburtsdaten, Beziehungsstatus, Status-Mitteilungen und politische oder religiöse Einstellungen.

---

95 Facebook Ireland Limited, Datenverwendungsrichtlinien (Fn. 61), Löschung und Deaktivierung deines Kontos.

96 Jahnel, Datenschutzrecht (Fn. 2), Rz. 7/72.

97 Facebook Ireland Limited, Datenverwendungsrichtlinien (Fn. 61), Löschung und Deaktivierung deines Kontos.

98 Facebook Ireland Limited, Datenverwendungsrichtlinien (Fn. 61), Löschung und Deaktivierung deines Kontos.

Der Datenbestand ist vermeintlich noch viel höher als Facebook zugibt und sich den Auskunftsersuchen entnehmen lässt. Auch das von Facebook angebotene «Download Tool», was der Durchsetzung des dem Nutzer zustehenden Auskunftsrechts gerecht werden soll, liefert nur unvollständige Datensätze. Mit diesem erhält der Nutzer nämlich nur Auskunft über einen Bruchteil der Daten (z.B. frühere Namen, Nachrichten, selbst hochgeladene Fotos), die von Facebook verarbeitet wurden, da man, wenn überhaupt, nur eine Kopie seines Kontos erhält. Facebook speichert aber darüber hinaus auch Daten, die für die Gesichtserkennung notwendig sind, Daten aus der «Gefällt mir»-Funktion, Trackingdaten von Webseiten, sowie Indikatoren, welche die Intensität von Beziehungen anzeigen.[99] Nur ein Bruchteil der Daten wird vermutlich auch von der vereinbarten Löschung des Kontos betroffen sein, wobei selbst entfernte und geänderte Daten, wie geänderte Namen und E-Mail-Adressen, gelöschte Chat-Nachrichten und Statusnachrichten, nachweislich auch nach der Löschung von Facebook auf ihren Servern verarbeitet werden.[100] So sammelt Facebook beispielsweise explizit das Datum und die Uhrzeit, wann und wo man einen Freund aus seiner Freundesliste löscht, obwohl Facebook die Daten über die Freundschaft löschen sollte. Facebook schafft daher sogar neue Daten, anstatt schon vorhandene Daten aus ihren Datensätzen zu löschen.

[Rz 84] Die Löschung vorhandener Daten auf Facebook scheint also praktisch nicht durchsetzbar. Facebook hält sich sehr bedeckt mit Informationen über auf ihren Servern gespeicherte Daten und kommt durch seine Praktiken weder der in den Datenverwendungsbestimmungen vereinbarten Löschung der Daten nach, da durch diese ein bloßes «unsichtbar machen» geschieht, noch irgendeiner anderen Vernichtung von Daten. Die Daten der Nutzer sind schließlich das Kapital von Facebook. Vielmehr geschieht das Gegenteil, da Facebook die Daten noch zu größeren Datensätzen weiterverarbeitet («Big Data»). Nicht umsonst wird Facebook von den Medien gerne als die «Datenkrake Facebook»[101] bezeichnet. Die Löschung der Daten auf Facebook ist de facto nur auf dem Papier möglich, was den Vorschriften und Grundsätzen des DSG sowie der DSRL widerspricht. Die gesammelten Daten bleiben, denn das Internet vergisst nicht, und niemand weiß, welche technischen Möglichkeiten es in fünf, zehn oder fünfzehn Jahren gibt.[102]

2. Google

[Rz 85] Mit den Worten «Recht auf Vergessenwerden» wurde die Entscheidung des EuGH[103] in den Medien betitelt, in der der EuGH zahlreiche Grundsatzfragen des europäischen Datenschutzrechts zu beurteilen hatte. *Mario Costeja González* hatte bei der spanischen Datenschutzagentur AEPD (Agencia Española de Protección de Datos) dagegen geklagt, dass bei Eingabe seines Namens in der Suchmaschine des Google-Konzerns den Internetnutzern Links zu zwei Seiten aus dem Onlinearchiv der Tageszeitung *La Vanguardia* aus 1998 angezeigt wurden, in denen über

99 EUROPE-V-FACEBOOK.ORG, Facebooks Datenbestand (Fn. 94); EUROPE-V-FACEBOOK.ORG, data categories Facebook likely gathers, 3. April 2012 (europevfacebook.org/fb_cat1.pdf).

100 EUROPE-V-FACEBOOK.ORG, «Entfernte» Daten (europe-v-facebook.org/removed_content.pdf).

101 GEOFFREY A. FOWLER, Wie Sie der Facebook-Datenkrake entwischen, The Wall Street Journal, 6. August 2014 (wsj.de/nachrichten/SB10001424052702303800604580075814104496460); MARTIN GRABMAIR, Datenkrake Facebook: Die Nutzer sind Ware – ihre Daten bares Geld, Tech.de, 25. April 2014 (tech.de/news/datenkrake-facebook-nutzer-sind-ware-ihre-daten-bares-geld-10031040.html).

102 WIEBE, ZIR (Fn. 68), 35 (36).

103 EuGH 13. Mai 2014, C-131/12 (Google Spain und Google).

die Zwangsversteigerung seines Hauses berichtet wurde. Herr *Costeja González* beantragte, die Tageszeitung anzuweisen, die Seiten zu löschen oder zu anonymisieren und Google Spain oder Google Inc. anzuweisen, ihn betreffende personenbezogene Daten zu löschen oder zu verbergen. Die AEPD wies die Beschwerde gegen *La Vanguardia* zurück, da die Veröffentlichung gerechtfertigt war, und gab der Beschwerde gegenüber Google Spain und Google Inc. statt. Google Spain und Google Inc. erhoben bei der Audiencia Nacional zwei gesonderte Klagen gegen diese Entscheidung, was dazu führte, dass dem EuGH zahlreiche Fragen zur Vorabentscheidung vorgelegt wurden.[104]

[Rz 86] Als erstes stellte sich die Frage, ob die Tätigkeit einer Suchmaschine als «Verarbeitung von Daten» i.S.d. Art. 2 lit. b DSRL anzusehen ist. Dies bejahte der EuGH, da sich unter den von der Suchmaschine gefundenen, indexierten, gespeicherten und den Nutzern zur Verfügung gestellten Informationen auch Informationen über bestimmte oder bestimmbare natürliche Personen, also «personenbezogene Daten» i.S.d. Art. 2 lit. a DSRL befinden. Auch ist die Tätigkeit eines Suchmaschinenbetreibers als «Verarbeitung» i.S.d. DSRL anzusehen, da dabei das Internet automatisch, kontinuierlich und systematisch auf die dort veröffentlichten Informationen durchforstet wird.[105]

[Rz 87] Danach war zu beantworten, ob ein Suchmaschinenbetreiber als «für die Verarbeitung Verantwortlicher» (Auftraggeber) i.S.d. Art. 2 lit. d DSRL anzusehen ist. Dies bejahte der EuGH ebenfalls, mit der Begründung, dass der Suchmaschinenbetreiber über die Zwecke und Mittel der von ihm selbst ausgeführten Verarbeitung personenbezogener Daten entscheidet, sodass er für diese Verarbeitung als «Verantwortlicher» anzusehen ist. Dem steht nicht entgegen, dass die auf den Internetseiten Dritter veröffentlichten personenbezogenen Daten nicht seiner Kontrolle unterliegen, weil durch einen weiten Begriff des «Verantwortlichen» ein wirksamer und umfassender Schutz der betroffenen Personen erreicht werden soll.[106]

[Rz 88] Mit dem positiven Ausgang dieser beiden «Fragen» stellte sich in weiterer Folge die Frage, ob auf die Tätigkeit des Suchmaschinenbetreibers Google die spanischen Datenschutzvorschriften anzuwenden sind. Dazu muss gem. Art. 4 Abs. 1 lit. a DSRL die Voraussetzung vorliegen, dass die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaates besitzt. Auch dies sah der EuGH als gegeben, da Google Inc. über Google Spain in Spanien effektiv und tatsächlich eine Tätigkeit mittels einer festen Einrichtung ausübt und zudem Google Spain über eine eigene Rechtspersönlichkeit verfügt, sodass sie eine Tochtergesellschaft von Google Inc. in Spanien und somit eine «Niederlassung» i.S.d. Art. 4 Abs. 1 lit. a DSRL ist. Daher sind nationale Normen anzuwenden.[107]

[Rz 89] Der EuGH stellte somit fest, dass Google für die Verarbeitung in der Suchergebnisliste verantwortlich ist und darüber hinaus auch das nationale Recht, hierbei Spanien, zur Anwendung kommt.

[Rz 90] Auch die Frage über die Reichweite der Rechte auf Löschung und Widerspruch hatte der EuGH zu beantworten. Dazu musste festgestellt werden, ob der Suchmaschinenbetreiber zur

104 Dietmar Jahnel, Löschungspflicht von Suchmaschinenbetreibern – Die «Google Spain und Google»-Entscheidung des EuGH, jusIT 2014/72, 149 (149).

105 Jahnel, jusIT (Fn. 104), 149 (150).

106 Jahnel, jusIT (Fn. 104), 149 (150).

107 Jahnel, jusIT (Fn. 104), 149 (150).

Wahrung der in der DSRL vorgesehenen Rechte verpflichtet ist, von der Ergebnisliste, die im Anschluss an eine anhand des Namens einer Person durchgeführte Suche angezeigt wird, Links von Dritten veröffentlichten Internetseiten mit Informationen zu dieser Person zu entfernen, auch wenn der Name oder die Informationen auf diesen Internetseiten nicht vorher oder gleichzeitig gelöscht werden und gegebenenfalls auch dann, wenn ihre Veröffentlichung auf den Internetseiten als solche rechtmäßig ist. Indem der EuGH annahm, dass sensible Daten von dem Suchmaschinenbetreiber nicht verarbeitet werden, was ziemlich unwahrscheinlich ist, vermied der EuGH – gewollt oder ungewollt – das Problem, vor dem man bei einer datenschutzrechtlichen Beurteilung der Zulässigkeit der Verarbeitung von auch sensiblen Daten steht. Nämlich, dass mangels der Möglichkeit eine Interessenabwägung vorzunehmen, gar keiner der Zulässigkeitsgründe des Art. 8 Abs. 2 DSRL (§ 9 DSG 2000) zur Anwendung kommen kann. Demnach ist nach der Erkenntnis vom EuGH die Verarbeitung personenbezogener Daten zulässig, wenn sie zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, erforderlich ist, sofern nicht das Interesse oder die Grundrechte des Betroffenen überwiegen.[108]

[Rz 91] Aufgrund der potenziellen Schwere des Grundrechtseingriffs durch InternetSuchmaschinen kann ein solcher Eingriff nicht allein mit dem wirtschaftlichen Interesse des Suchmaschinenbetreibers an der Verarbeitung der Daten gerechtfertigt werden. Jedoch steht auf dieser Seite auch das berechtigte Interesse von potenziell am Zugang zu der Information interessierten Internetnutzern, sodass ein angemessener Ausgleich zwischen diesem Interesse und den Grundrechten des Betroffenen gefunden werden muss. Somit kann das nationale Gericht nach der Beurteilung dieser Anwendungsvoraussetzung den Suchmaschinenbetreiber anweisen, aus der Liste mit den Ergebnissen, einer anhand des Namens einer Person durchgeführten Suche, Links zu von Dritten veröffentlichten Seiten mit Informationen über diese Person zu entfernen, ohne dass eine solche Anordnung voraussetzt, dass der Name und die Informationen vorher oder gleichzeitig vom Herausgeber der Internetseite, auf der sie veröffentlicht worden sind, freiwillig oder auf Anordnung der Kontrollstelle oder des Gerichts von dieser Seite entfernt werden. Dazu stellt der EuGH weiter fest, dass auf solchen Webseiten veröffentlichte Informationen nicht immer dem Unionsrecht bzw. der DSRL unterliegen müssen, aufgrund der Ausnahme der Art. 9 DSRL «allein zu journalistischen Zwecken» erfolgen und die Interessenabwägung zwischen dem Suchmaschinenbetreiber oder dem Herausgeber der Internetseite verschieden ausfallen kann.[109]

[Rz 92] Schließlich hatte der EuGH noch zu beurteilen, ob die Rechte auf Löschung und Widerspruch dahingehend auszulegen sind, dass die betroffene Person Links löschen lassen kann, weil diese Informationen ihr schaden können oder weil sie möchte, dass sie nach einer gewissen Zeit «vergessen» werden. Dahingehend stellte der EuGH fest, dass bei einem Antrag auf Löschung zu prüfen ist, ob die Einbeziehung von Links zu von Dritten rechtmäßig veröffentlichten Internetseiten, die wahrheitsgemäße Informationen zu einer Person enthalten, in die Ergebnisliste, die im Anschluss an eine Namenssuche angezeigt wird, zum gegenwärtigen Zeitpunkt mit Art. 6 Abs. 1 DSRL vereinbar ist. Sollte sich dabei herausstellen, dass die Informationen in Anbetracht aller Umstände des Einzelfalls den Zwecken der Verarbeitung durch den Suchmaschinenbetrei-

108 Jahnel, jusIT (Fn. 104), 149 (151).

109 Jahnel, jusIT (Fn. 104), 149 (152).

ber nicht entsprechen, dafür nicht oder nicht mehr erheblich sind oder darüber hinausgehen, müssen die betreffenden Informationen und Links von der Ergebnisliste gelöscht werden.[110]

[Rz 93] Zusammengefasst lässt sich festhalten, dass die Löschung von Links aus der Suchergebnisliste von Google maßgeblich davon abhängt, ob noch ein berechtigtes Interesse des Suchmaschinenbetreibers oder vielmehr der Internetnutzer besteht, die die Interessen des Betroffenen überwiegen. Liegt also eine im Internet befindliche Information eine lange Zeit zurück, so ist von einem Überwiegen des Betroffenen auszugehen; ist sie noch aktuell, so ist ein Löschungsantrag abzuweisen. Von einem automatischen «Recht auf Vergessenwerden» kann jedenfalls nicht gesprochen werden, da zur Löschung von Links eine Interessenabwägung im Einzelfall durchzuführen ist und diese Löschung der Verlinkung auch nur für den Suchmaschinenbetreiber gilt, bei dem die Löschung beantragt wurde. Für die Webseite auf der die Information veröffentlicht wurde sowie weitere Suchmaschinenbetreiber muss ein eigener Löschungsantrag eingebracht werden, sodass eine faktische Löschung einer Information aus dem Internet nahezu unmöglich wird.

3. Zwischenergebnis

[Rz 94] Die Durchsetzung des Rechts auf Löschung gestaltet sich im privaten Bereich mitunter viel schwieriger als das im öffentlichen Bereich der Fall ist. Durch das primäre Zugrundelegen der Interessenabwägung als Zulässigkeitsvoraussetzung entsteht eine größere Möglichkeit, mit Argumenten die Zulässigkeit der Datenanwendung zu erreichen. Besonders private Unternehmen haben durchaus ein sehr großes Interesse einmal akquirierte Daten und Datensätze möglichst nie mehr löschen zu müssen, da ein großer Vorrat an Daten mit großem Gewinn gleichgesetzt werden kann und wird. An Facebook erkennt man eindeutig, dass besonders amerikanische Unternehmen hemmungslos mit den Daten von Nutzern umgehen, sie gar als Allgemeingut behandeln und den europäischen Datenschutzstandard de facto ignorieren. Eine Löschung der Daten ist hierbei kaum durchsetzbar.

IV. Löschungsart

[Rz 95] Wie man Daten zu löschen hat, entschied der OGH.[111] Um das datenschutzrechtliche Löschungsgebot zu erfüllen, genügt es demnach nicht die Datenorganisation so zu verändern, dass bloß ein gezielter Zugriff auf die betreffenden Daten ausgeschlossen wäre. Es bedarf einer physischen Beseitigung. Damit klärte der OGH die nicht nur in der Lehre z.T. umstrittene Anforderung an die «Datenlöschung», sondern klärte auch eine in der Praxis häufig gestellte Herausforderung zumindest aus juristischer Sicht ab. Das DSG unterscheidet in § 4 Z. 9 DSG 2000 selbst praxisnah zwischen dem «Löschen und Vernichten von Daten» einerseits und dem «Sperren von Daten» andererseits. In der modernen elektronischgestützten Datenverarbeitung kann es nämlich durchaus den Anwenderwunsch geben, gelöschte Daten so lange wie möglich zu erhalten, da sie (möglicherweise) irrtümlich gelöscht sein können und dies erst nach einiger Zeit auffällt. Hierbei

110 Jahnel, jusIT (Fn. 104), 149 (152).

111 OGH 15. April 2010, 6 Ob 41/10p = SZ 2010/36 = jusIT 2010/69, 146 (Kastelitz).

spricht die Praxis von aufwandslos rekonstruierbaren Daten und einem sogenannten logischen Löschen.[112]

[Rz 96] Jahnel[113] versteht unter dem «Löschen» eine Maßnahme mit der Wirkung, dass der Auftraggeber nicht mehr über die Daten verfügt. Dieser Meinung schließt sich der OGH ausdrücklich an, wonach zur Erfüllung des Löschungsgebotes es nicht genügt, die Datenorganisation bloß so zu verändern, dass ein «gezielter Zugriff» auf die Daten ausgeschlossen ist. So bedarf es eines physischen Löschens im Sinne einer unumkehrbaren Beseitigung.[114]

V. Durchsetzung des Rechts auf Löschung

[Rz 97] Gem. § 27 Abs. 1 Z. 2 DSG 2000 hat jeder Auftraggeber auf begründeten Antrag des Betroffenen unrichtige oder entgegen den Bestimmungen des DSG verarbeitete Daten richtigzustellen oder zu löschen. Dieser Antrag hat den in Abs. 1 angeführten Gründen (z.B. dass die Daten für den Zweck der Datenanwendung nicht mehr benötigt werden) zu entsprechen.[115] Der Betroffene muss dabei lediglich die Rechtswidrigkeit der Verarbeitung behaupten, da dem Auftraggeber die Beweispflicht der Rechtmäßigkeit obliegt.[116]

[Rz 98] Gem. § 27 Abs. 4 DSG 2000 hat der Auftraggeber innerhalb von acht Wochen nach dem Einlangen des Antrags auf Löschung dem Antrag zu entsprechen und dem Betroffenen davon Mitteilung zu machen oder schriftlich zu begründen, warum die verlangte Löschung nicht vorgenommen wird. Es trifft den Auftraggeber somit auch eine Mitteilungspflicht,[117] sowohl wenn er dem Antrag entspricht wie auch wenn er den Antrag abweist, da er ansonsten, wie auch bei nicht fristgerechter Löschung, mit einer Verwaltungsstrafe von bis zu EUR 500,00 rechnen muss (§ 52 Abs. 2a DSG 2000).

[Rz 99] Die DSB ist hierbei zur Entscheidung über Beschwerden wegen behaupteter Verletzungen der in §§ 26 bis 28, 49 und 50 DSG 2000 geregelten Betroffenenrechte berufen (§ 31 DSG 2000). Im Gegensatz zu Verletzungen des Auskunftsrechts, bei denen die DSB für Entscheidungen über Beschwerden sowohl gegen öffentliche als auch gegen private Auftraggeber zuständig ist, entscheidet die DSB bei Verletzungen des Rechts auf Geheimhaltung, Richtigstellung oder Löschung oder des Widerspruchsrechts aber nur über Beschwerden wegen Gesetzesverstößen durch einen Auftraggeber des öffentlichen Bereichs.[118] Im privaten Bereich sind hier die ordentlichen Gerichte anzurufen. Nicht zuständig ist die DSB jedoch für Beschwerden über die Verletzung von Betroffenenrechten durch Akte der Gesetzgebung oder Gerichtsbarkeit.[119] Bei diesen sind gem. §§ 83 bis 85 GOG die Gerichte für die Wahrung des Datenschutzes zuständig, wobei die Entschei-

112 Clemens Thiele, Löschen heißt Vernichten, lex:itec 2010 H 4, 20 (20 f).

113 Jahnel, Datenschutzrecht (Fn. 2), Rz. 3/112.

114 Thiele, lex:itec (Fn. 112), 20 (21).

115 Dohr/Pollierer/Weiss/Knyrim, DSG (Fn. 15), § 27 Anm. 6.

116 Dohr/Pollierer/Weiss/Knyrim, DSG (Fn. 15), § 27 Anm. 13.

117 DSK 25. Juni 2004, K120.877/0017-DSK/2004.

118 Viktor Mayer-Schönberger/Ernst Brandl/Hans Kristoferitsch, Datenschutzgesetz, 3. Auflage, Linde Verlag, Wien 2014, 44.

119 VfGH 23. Juni 2010, B 1048/09 = VfSlg 19112/2010 = jusIT 2010/68, 144 (Jahnel).

dung in Verfahren bürgerlicher Rechtssachen im Außerstreitverfahren und in Strafsachen nach den Bestimmungen der StPO ergeht.[120]

[Rz 100] Die Beschwerde hat gem. § 31 Abs. 3 DSG 2000 u.a. die Bezeichnung des als verletzt erachteten Rechts, die Bezeichnung des Rechtsträgers oder Organs, dem die behauptete Rechtsverletzung zugerechnet wird, den Sachverhalt und die Gründe, auf die sich die Behauptung der Rechtswidrigkeit stützt, zu enthalten.

[Rz 101] Die Bescheide der DSB im öffentlichen Bereich können innerhalb einer Frist von vier Wochen durch eine bei der DSB einzubringende Beschwerde an das Bundesverwaltungsgericht angefochten werden. Dessen Erkenntnisse sind wiederum mittels Revision beim Verwaltungsgerichtshof (bzw. Beschwerde beim Verfassungsgerichtshof) bekämpfbar. Die Beschwerde an das BVwG kann hierbei nicht nur vom Betroffenen, sondern auch vom betroffenen Auftraggeber des öffentlichen Bereichs erhoben werden, wodurch die Verfahren vor dem BVwG in vielen Fällen kontradiktorischen Charakter haben.[121]

[Rz 102] Gegen Auftraggeber des privaten Bereichs sind Ansprüche wegen Verletzung der Rechte auf Richtigstellung oder Löschung gem. § 32 Abs. 1 DSG 2000 auf dem Zivilrechtsweg geltend zu machen. Hierbei hat der Betroffene nach § 32 Abs. 2 DSG 2000 Anspruch auf Unterlassung und Beseitigung eines dem DSG widersprechenden Zustands. Zur Sicherung dieser Ansprüche auf Unterlassung nach dem DSG können nach § 32 Abs. 3 DSG 2000 einstweilige Verfügungen erlassen werden, auch wenn die in § 381 EO bezeichneten Voraussetzungen nicht zutreffen.

[Rz 103] Nach § 32 Abs. 4 DSG 2000 ist für Klagen und Anträge auf Erlassung einer einstweiligen Verfügung nach dem DSG in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht zuständig, in dessen Sprengel der Betroffene seinen gewöhnlichen Aufenthalt oder Sitz hat. Klagen können aber auch bei dem Landesgericht erhoben werden, in dessen Sprengel der Auftraggeber seinen gewöhnlichen Aufenthalt, Sitz oder Niederlassung hat.

[Rz 104] In Fällen, in denen der begründete Verdacht einer schwerwiegenden Datenschutzverletzung durch einen Auftraggeber des privaten Bereichs besteht, hat die DSB gem. § 32 Abs. 5 DSG 2000 gegen diesen eine Feststellungsklage (§ 228 ZPO) beim zuständigen Gericht zu erheben. Diese Möglichkeit ist auf vermutete schwerwiegende Datenschutzverletzungen beschränkt und soll dabei nach der ErläutRV[122] für solche Fälle, an deren Klärung auch ein öffentliches Interesse besteht, das Prozessrisiko des Betroffenen vermeiden. Der Betroffene kann dann auf der Grundlage des gerichtlichen Feststellungsurteils entscheiden, ob er seine Unterlassungs- und Schadenersatzansprüche selbst weiterverfolgen will.[123]

[Rz 105] Weiters sieht § 32 Abs. 6 DSG 2000 vor, dass die DSB einem Rechtsstreit auf Seiten des Betroffenen als Nebenintervenient (§§ 17 ff. ZPO) beizutreten hat, wenn dieser es verlangt und es zur Wahrung der nach dem DSG geschützten Interessen einer größeren Zahl von Betroffenen geboten ist.

---

120 OGH 25. April 2007, 3 Ob 37/07y; OGH 25. April 2007, 3 Ob 31/07s; OGH 16. Juli 2013, 5 Ob 40/13p = jusIT 2013/107, 225 (Thiele) = wobl 2014/32, 88 (Kodek); DSK 16. Mai 2012, K121.785/0003-DSK/2012.

121 Mayer-Schönberger/Brandl/Kristoferitschm, DSG (Fn. 118), 45.

122 ErläutRV 1613 BlgNR XX. GP 49.

123 Jahnel, Datenschutzrecht (Fn. 2), Rz. 9/59.

[Rz 106] Ist dem Betroffenen durch die schuldhafte entgegen den Bestimmungen des DSG durchgeführte Verwendung seiner Daten durch einen Auftraggeber im privaten Bereich ein Schaden entstanden, hat der Auftraggeber diesen gem. § 33 Abs. 1 DSG 2000 nach den allgemeinen Bestimmungen des bürgerlichen Rechts zu ersetzen. Nach der h.L. und Rechtsprechung ist immaterieller Schaden grundsätzlich nicht Gegenstand des Ersatzes, sondern nur dort wo das Gesetz dies ausdrücklich vorsieht, wie etwa in § 1325 des Allgemeinen Bürgerlichen Gesetzbuches (ABGB) (Schmerzensgeld) oder § 33 Abs. 1 zweiter Satz DSG 2000. Ideeller Schadenersatz gebührt nunmehr, wenn durch die öffentlich zugängliche Verwendung von sensiblen oder strafrechtlich relevanten Daten oder solche zur Kreditwürdigkeit, die schutzwürdigen Geheimhaltungsinteressen des Betroffenen in einer Weise verletzt werden, die einer Bloßstellung i.S.d. § 7 Abs. 1 des Mediengesetzes (MedienG) gleichkommt, und zwar auch ohne Veröffentlichung in einem Medium. Für eine solch erlittene Kränkung ist vom Auftraggeber der Datenanwendung eine Entschädigung bis EUR 20000 zu leisten.[124]

[Rz 107] Der Auftraggeber, der gem. § 33 Abs. 2 DSG 2000 auch für das Verschulden seiner Leute haftet, soweit deren Tätigkeit für den Schaden ursächlich war, könnte sich nach § 33 Abs. 3 DSG 2000 nur dadurch von seiner Haftung befreien, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, ihm und seinen Leuten nicht zur Last gelegt werden kann.

[Rz 108] Im privaten Bereich sind dabei also verschiedene Schadenersatzklagen möglich. Bei einem Verstoß gegen das Grundrecht auf Geheimhaltung des § 1 DSG 2000 i.V.m. § 1311 ABGB gibt es die Möglichkeit auch bei nicht automationsunterstützt verarbeiteten Daten Schadenersatz zu fordern, da das Recht auf Datenschutz ein Persönlichkeitsrecht ist und als absolutes Recht Schutz gegen Eingriffe Dritter genießt. Bei automationsunterstützter Datenverwendung kann der Betroffene weiters auf den Ersatz des materiellen wie auch des ideellen Schadens auf Grundlage des § 33 Abs. 1 DSG 2000 oder des § 1328a ABGB (Recht auf Wahrung der Privatsphäre) klagen.[125]

VI. Conclusio

[Rz 109] Der Erfolg der Durchsetzung des Rechts auf Löschung ist im öffentlichen Bereich unter normalen Umständen jedenfalls gegeben. So hat sich durch langjährige einhellige Rechtsprechung der DSK und der Höchstgerichte gezeigt, dass zwar ein konventioneller Papierakt generell nicht unter das Recht auf Löschung fällt, jedoch auch Fälle zugelassen werden, bei denen ein Papierakt mit einer gewissen Ordnung und Strukturiertheit doch auf Antrag des Betroffenen gelöscht werden muss. In Hinblick auf die verarbeiteten Daten im EKIS sind zwar meist andere Löschungsvorschriften als § 27 DSG 2000 anzuwenden, jedoch folgen auch diese den Grundsätzen des DSG und entsprechen somit im Großen und Ganzen dem verfassungsmäßig gewährleisteten Grundrecht auf Datenschutz, sodass das Interesse des Betroffenen auf Geheimhaltung und Datenschutz auf jeden Fall gewahrt werden kann. Meist sind solch verarbeitete Daten schon von Amts wegen zu löschen und sollten im Normalfall nur weiter verarbeitet werden, wenn es gewichtige Gründe für die weitere Aufbewahrung gibt.

---

124 Dohr/Pollierer/Weiss/Knyrim, DSG (Fn. 15), § 33 Anm. 2 ff.

125 Dohr/Pollierer/Weiss/Knyrim, DSG (Fn. 15), § 33 Anm. 9.

[Rz 110] Ein anderes Bild zeigt sich im privaten Bereich, wo sich die Durchsetzung des Rechts auf Löschung, zumindest gegen ausländische bzw. amerikanische Online-Unternehmen, denkbar schwierig gestaltet. So scheitert eine effektive Durchsetzung an einer Vielzahl von Faktoren, da im Fall von Facebook das gesamte Geschäftsmodell darauf aufbaut, dem DSG zu widersprechen, indem Daten hemmungslos gesammelt werden, um sie so uneingeschränkt wie möglich weiter zu verarbeiten, zu übermitteln und zu versilbern. Die Löschung der Daten auf Facebook ist dabei praktisch nicht durchsetzbar.

[Rz 111] Im Fall «Google und Google Spain» lässt sich weiters zusammenfassend festhalten, dass auch hier der Begriff «Recht auf Vergessenwerden» von den Medien übertrieben dargestellt wurde. Das Löschen der Verlinkung auf der Ergebnisliste bedeutet keinesfalls, dass die Informationen aus dem Internet gelöscht werden. Über unzählige andere Wege bleibt die Information im Internet erhalten und eine Löschung ist daher wohl mit dem benötigten Zeitaufwand unrentabel, wenn nicht sogar unmöglich.

[Rz 112] Es scheint ratsam, dass jede Person darauf achtet, welche personenbezogenen Daten an welches (im Internet agierendes) Unternehmen übermittelt werden, da eine Löschung dieser Daten mitunter faktisch nicht durchsetzbar ist.

Mag. Martin C. Walther, Rechtsanwaltsanwärter in Salzburg.
Dieser Beitrag stellt eine Kurzfassung der Magisterarbeit des Autors vor. Diese wurde 2017 in Editions Weblaw publiziert: Martin C. Walther, Die Zulässigkeit der Datenverwendung als Voraussetzung des Rechts auf Löschung, in: Magister, Editions Weblaw, Bern 2017.