

LÖSCHPFLICHTEN UND DAS RECHT AUF VERGESSENWERDEN IM UNTERNEHMEN

Maurits Haas

Dissertant, Rechtswissenschaftliche Fakultät, Universität Wien, Arbeitsgruppe Rechtsinformatik, und juristischer Mitarbeiter,
Rechtsanwaltskanzlei Lichtenberger & Partner Rechtsanwälte GbR
Lange Gasse 48/33, 1080 Wien, AT
maurits.haas@gmx.de

Schlagworte: *Recht auf Löschung, Recht auf Vergessenwerden, Datenschutz-Grundverordnung, IT Compliance*

Abstract: *Unternehmen häufen größer werdende Datenberge an; dies kann aus strategischen Gründen geschehen oder auch schlicht aus Unwissenheit. Der vorliegende Beitrag soll einen Überblick darüber geben, welche Löschpflichten nach der geltenden und künftigen Rechtslage für Unternehmen zu beachten sind und in welchem Verhältnis diese zu Aufbewahrungspflichten stehen. Gesondert wird auf das Recht auf Vergessenwerden sowie die Umsetzung von Löschpflichten bei der Verwendung von Cloud-Diensten eingegangen.*

1. Ausgangslage

Zahlreiche Unternehmen häufen kontinuierlich größer werdende Datenberge an.¹ Die dahinterstehende Motivation kann dabei sehr unterschiedlich sein. Es gibt Unternehmen, die gezielt Daten sammeln, um sie in Big Data Analysen verwerten zu können. Andere speichern «für alle Fälle» vorsichtshalber und trennen sich nicht mehr von einmal angelegten Datenbeständen. Viele Unternehmen horten Daten aber auch schlicht aus Unwissenheit bzw. weil sie ihren Umgang mit Datenbeständen nicht ausreichend reflektieren.

In nahezu jedem Unternehmen fallen personenbezogene Daten an, wie Kunden- oder Beschäftigendaten. Häufig sind Datenbestände mit der Zeit ohne übergreifende Datenmanagementstruktur gewachsen. Als Folge ist in zahlreichen Unternehmen nicht vollumfänglich bekannt, welche Daten überhaupt gespeichert sind und wo diese Daten genau zu finden sind (Dark Data).² Die gewachsenen Strukturen sind zum Teil darin begründet, dass es oft zunächst günstiger ist die Speicherkapazität zu erhöhen, als Zeit in die Löschung nicht mehr benötigter Daten zu investieren. Zudem waren insbesondere viele ältere Datenverarbeitungsprogramme nicht für Löschungen konzipiert.³ Die Lage verkompliziert sich zusätzlich dann, wenn in Unternehmen Softwarelösungen verschiedener Anbieter eingesetzt werden. Mangels einheitlicher technischer Standards ist eine systemübergreifende Löschung unter Umständen äußerst aufwendig.

Unternehmen sollten die nahende Geltung der Datenschutz-Grundverordnung⁴ als Anlass nehmen, ihre bisherige Praxis zur Sammlung von personenbezogenen Daten zu überdenken und Konzepte entwickeln, die den Anforderungen des Datenschutzrechts gerecht werden. Denn viele Unternehmen sind sich der bevorstehenden Änderungen nicht ausreichend bewusst.⁵ Der vorliegende Beitrag soll die derzeit geltende und die künftige

¹ Vgl. VERITAS TECHNOLOGIES LLC., The Data Berg Report, http://images.info.veritas.com/Web/Veritas/%7B364a7ca5-e05c-4fce-971b-88e18c62eafb%7D_45145_EMEA_Veritas_Strike_Report_Gulf.pdf (alle Internetadressen zuletzt aufgerufen am 9. Januar 2017), 2015.

² Ebenda.

³ SCHILD, Datenlöschen in SAP – Wo liegt das Problem? DANA 1/2013, S. 13.

⁴ Die VO (EU) 2016/679 (im Folgenden: DS-GVO) gilt ab dem 25. Mai 2018 (Art. 99 Abs. 2 DS-GVO).

⁵ Vgl. COMPUWARE REPORT, Unprepared for GDPR? http://resources.compuware.com/hubfs/Collateral/White_Papers/31465_Test_Data_Privacy_wp_6_002.pdf, 2016.

Rechtslage zu Löschpflichten und dem Recht auf Vergessenwerden im unternehmensbezogenen Kontext sowie diesbezügliche Vorschriften bei der Verwendung von Cloud-Diensten beleuchten.

2. Das Recht auf Löschung und Vergessenwerden

Die Pflicht zur Löschung personenbezogener Daten, die unzulässigerweise verarbeitet werden, ist ein Grundpfeiler des Datenschutzrechts⁶, der in Verbindung mit dem Zweckbindungsgrundsatz auch eine anlasslose Speicherung personenbezogener Daten auf Vorrat⁷ verhindern soll. Daten dürfen demnach nur solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben.⁸ Hinzu trat in den letzten Jahren die Überlegung, Betroffenen müsse ein Recht auf Vergessenwerden zukommen, da der Anspruch auf Löschung insbesondere im Internet unzureichend sein könnte.⁹

2.1. Die Rechtslage gemäß DSGVO 2000

Das Grundrecht auf Datenschutz gewährt das Recht auf Löschung unzulässigerweise verarbeiteter Daten.¹⁰ Einfachgesetzlich ist das Recht auf Löschung in § 27 DSGVO festgeschrieben, der die Vorgaben der EU-Datenschutzrichtlinie 1995 umsetzt.¹¹ Demnach hat jeder Auftraggeber entgegen den Bestimmungen der DSGVO verarbeitete Daten nach Kenntnis von sich aus oder auf begründeten Antrag des Betroffenen zu löschen.

2.1.1. Löschen auf Antrag und Widerspruchsrecht

Unternehmen haben unzulässig verarbeitete Daten auf Antrag zu löschen. Datenverarbeitungen sind grundsätzlich dann unzulässig, wenn sie von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen¹² des jeweiligen Auftraggebers nicht gedeckt sind oder schutzwürdige Geheimhaltungsinteressen von Betroffenen¹³ verletzen. Stellt ein Betroffener einen Antrag auf Löschung, hat der Auftraggeber die Daten binnen 8 Wochen zu löschen und dem Betroffenen darüber Mitteilung zu machen oder schriftlich zu begründen, warum die verlangte Löschung nicht vorgenommen wird.¹⁴

Darüber hinaus gibt es das Widerspruchsrecht gemäß § 28 DSGVO¹⁵, das eine besondere Form des Lösungsbegehrens darstellt. Der Betroffene hat das Recht, gegen die Verwendung seiner Daten wegen Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen, die sich aus seiner besonderen Situation ergeben, beim Auftraggeber Widerspruch zu erheben, sofern die Verwendung der Daten nicht gesetzlich vorgesehen ist. Auch in diesem Fall sind die Daten – sofern der Widerspruch berechtigt ist – binnen 8 Wochen zu löschen. Das Recht auf Löschung und das Widerspruchsrecht können nicht geltend gemacht werden, soweit nur indirekt personenbezogene Daten verwendet werden.¹⁶

⁶ Vgl. bereits § 1 Abs. 4 und § 12 DSGVO 1978; Art. 5 lit. e und Art. 8 lit. c Europäische Datenschutzkonvention 1981.

⁷ Vgl. EuGH 21. Dezember 2016, C-203/15 und C-698/15. EuGH 8. April 2014, C-293/12 und C-594/12; VfGH 27. Juni 2014, G 47/2012.

⁸ § 6 Abs. 1 Z 5 DSGVO.

⁹ Siehe Kapitel 2.2.2.

¹⁰ § 1 Abs. 3 Z 2 DSGVO. Dem Grundrecht auf Datenschutz kommt unmittelbare Drittwirkung zu, es gilt somit auch gegenüber Privaten.

¹¹ Vgl. Art. 6 lit. d und e, Art. 12 lit. b und c RL 1995/46/EG.

¹² Bspw. eine Gewerbeberechtigung oder Konzession, die zur Verarbeitung personenbezogener Daten im Rahmen der Tätigkeit ermächtigen. Vgl. KNYRIM, Handbuch Datenschutzrecht² (2012), S. 86 f.

¹³ Vgl. §§ 8 und 9 DSGVO. Ob Daten auf rechtmäßige Weise verwendet werden, richtet sich aber nicht ausschließlich nach den Bestimmungen der DSGVO (vgl. VwGH 28. Januar 2013, 2012/12/0050).

¹⁴ § 27 Abs. 4 DSGVO. Vgl. auch VwGH 28. Mai 2013, 2009/17/0011.

¹⁵ Zur Aufhebung des § 28 Abs. 2 DSGVO wegen eines Verstoßes gegen Art. 10 EMRK, siehe VfGH 8. Oktober 2015, G 264/2015.

¹⁶ § 29 DSGVO. Zum Begriff «indirekt personenbezogene Daten» § 4 Z 1 DSGVO.

2.1.2. Löschen aus eigenem Antrieb

Unabhängig von Löschbegehren und Widerspruchsrecht eines Betroffenen, ist ein Unternehmen auch dazu verpflichtet, aus eigenem Antrieb zu prüfen, ob Daten zu löschen sind.¹⁷ § 27 Abs. 1 DSGVO konkretisiert diesbezüglich: *«Sobald Daten für den Zweck der Datenanwendung nicht mehr benötigt werden, gelten sie als unzulässig verarbeitete Daten und sind zu löschen, es sei denn, daß ihre Archivierung rechtlich zulässig ist und daß der Zugang zu diesen Daten besonders geschützt ist.»* Diese Lösungsverpflichtung betrifft den häufigen Fall, dass Daten zunächst rechtmäßig verarbeitet werden, die Verarbeitung aber durch Zeitablauf unzulässig wird.¹⁸

Die Frage, wann verpflichtend zu löschen ist und in welchem Fall eine Archivierung zulässig bzw. vorgeschrieben ist, kann nicht allein aus dem DSGVO beantwortet werden. Das DSGVO gibt keine expliziten Löschfristen vor. Schutzwürdige Geheimhaltungsinteressen werden bei der Verwendung nicht-sensibler Daten¹⁹ u.a. dann nicht verletzt, wenn eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht²⁰ oder die Verwendung zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenen erforderlich ist.²¹ Bei Bestehen gesetzlicher Aufbewahrungspflichten darf somit jedenfalls nicht gelöscht werden. Diese Aufbewahrungspflichten können sich in der gesamten Rechtsordnung finden.²² Aber auch aus vertraglichen Vereinbarungen kann sich das Recht oder die Pflicht zur Aufbewahrung von personenbezogenen Daten ergeben.

2.1.3. Löschfristen und Aufbewahrungspflichten

Zu den Aufbewahrungspflichten zählen die Vorschriften des § 212 UGB und § 132 BAO, nach denen Unternehmer ihre Bücher und Aufzeichnungen sowie Buchungsbelege 7 Jahre aufzubewahren haben. Die Daten sind darüber hinaus noch solange aufzubewahren, als sie für ein anhängiges gerichtliches oder behördliches Verfahren, in dem der Unternehmer Parteistellung hat, von Bedeutung sind. Berufsspezifische Sondervorschriften können weitere Aufbewahrungspflichten vorsehen.²³

Eindeutige Löschfristen finden sich bspw. im TKG, das für die Verarbeitung und Übermittlung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlicher Kommunikationsdienste in öffentlichen Kommunikationsnetzen Sonderdatenschutzvorschriften vorschreibt, die den Bestimmungen des DSGVO vorgehen.²⁴ Demnach sind Stammdaten nach Beendigung der vertraglichen Beziehungen zu löschen, sofern sie nicht noch benötigt werden, um Entgelte zu verrechnen oder einzubringen, Beschwerden zu bearbeiten oder sonstige gesetzliche Verpflichtungen zu erfüllen.²⁵ Verkehrsdaten müssen – wenn sie zu Abrechnungszwecken gespeichert werden dürfen – binnen 3 Monaten gelöscht oder anonymisiert werden, sofern die Abrechnung nicht schriftlich beansprucht wurde.²⁶ Inhaltsdaten dürfen nur gespeichert werden, wenn dies aus technischen Gründen erforderlich ist oder ein Merkmal des Dienstes ist und sind unmittelbar nach Wegfall der technischen Gründe bzw. nach Erbringung des Dienstes zu löschen.²⁷

¹⁷ Eine Löschung muss auch dann vorgenommen werden, wenn der Betroffene dies nicht eigens beantragt. Vgl. Erläuterung zu § 27 Abs. 1 DSGVO.

¹⁸ Vgl. DOHR/POLLIERER/WEISS/KNYRIM, Kommentar Datenschutzrecht², § 27 DSGVO Rz 10.

¹⁹ Für die Verwendung sensibler Daten (§ 4 Z 2 DSGVO) vgl. § 9 Z 3 DSGVO.

²⁰ § 8 Abs. 1 Z 1 DSGVO.

²¹ § 8 Abs. 3 Z 4 DSGVO.

²² Der vorliegende Artikel kann daher nur Hinweise geben, ohne Anspruch auf Vollständigkeit.

²³ Vgl. § 51 Abs. 3 ÄrzteG; § 12 RAO.

²⁴ § 92 Abs. 1 TKG.

²⁵ § 97 Abs. 2 TKG.

²⁶ § 99 Abs. 1 u. 2 TKG.

²⁷ § 101 Abs. 1 u. 2 TKG.

Weitere Löschfristen und Aufbewahrungspflichten ergeben sich auch aus dem DSG selbst und der auf dessen Grundlage erlassenen Standard- und Musterverordnung²⁸. Zu beachten ist etwa, dass, wenn sich die Zulässigkeit der Datenverarbeitung auf eine Einwilligung stützt, ab Widerruf der Einwilligung diese Datenverarbeitung unzulässig wird, sofern nicht andere Erlaubnistatbestände die Verarbeitung rechtfertigen. Macht ein Betroffener sein Recht auf Auskunft geltend, dürfen hingegen Daten über den Auskunftswerber innerhalb eines Zeitraums von vier Monaten und im Falle der Erhebung einer Beschwerde gemäß § 31 an die Datenschutzbehörde bis zum rechtskräftigen Abschluss des Verfahrens nicht gelöscht werden. Diese Frist gilt wiederum dann nicht, wenn einem Löschantrag des Auskunftswerbers nach § 27 Abs. 1 Z 2 oder § 28 DSG zu entsprechen ist.²⁹ In der Standard- und Musterverordnung wird jeweils die Höchstdauer der zulässigen Datenaufbewahrung für eine Datenanwendung vorgeschrieben. Daten gemäß der SA022 Kundenbetreuung und Marketing für eigene Zwecke dürfen demnach z.B. bis zum Ablauf des dritten Jahres nach dem letzten Kontakt mit dem Unternehmen aufbewahrt werden.

Im Verhältnis zu Kunden und Lieferanten kommt eine Anwendung der SA001 Rechnungswesen und Logistik in Frage, nach der Daten bis zur Beendigung der Geschäftsbeziehung oder bis zum Ablauf der für den Auftraggeber geltenden Garantie-, Gewährleistungs-, Verjährungs- und gesetzlichen Aufbewahrungsfristen gespeichert werden dürfen und darüber hinaus bis zur Beendigung von allfälligen Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden. Gewährleistungs- und Verjährungsfristen richten sich i.d.R. nach dem ABGB, Garantiefristen nach vertraglicher Vereinbarung. Das Produkthaftungsgesetz sieht ein Erlöschen von Ersatzansprüchen 10 Jahre nach Inverkehrbringen eines Produktes vor.³⁰

Beschäftigtendaten unterliegen ebenfalls den Löschpflichten. Die SA002 Personalverwaltung für privatrechtliche Dienstverhältnisse gibt vor, dass Beschäftigtendaten bis zur Beendigung der Beziehung mit dem Betroffenen gespeichert werden dürfen und darüber hinaus solange als gesetzliche Aufbewahrungsfristen bestehen oder solange Rechtsansprüche aus dem Arbeitsverhältnis gegenüber dem Arbeitgeber geltend gemacht werden können. Als Aufbewahrungspflichten kommen insbesondere die sozialversicherungsrechtliche Verjährungsfrist von 5 Jahren³¹ und die bereits oben erwähnte abgabenrechtliche Frist gemäß BAO in Frage. Die Verjährungsfrist für Ansprüche aus dem Arbeitsverhältnis ergibt sich aus dem ABGB oder dem anzuwendenden Kollektivvertrag. Ein Personalakt ist deshalb nach den jeweiligen Fristen teilzulöschen, der Name und die Dauer des Arbeitsverhältnisses sind aber weiterhin zu speichern, um der Pflicht zur Ausstellung eines Dienstzeugnisses nachkommen zu können, die erst nach 30 Jahren verjährt.³² Verzichtet ein Arbeitnehmer wirksam auf seine Ansprüche und fordert gleichzeitig die Löschung seiner Daten, ist dieses Begehren zu erfüllen, sofern keine gesetzlichen Aufbewahrungspflichten dem entgegenstehen.³³

2.1.4. Die Durchführung einer Löschung

Das DSG beinhaltet keine Legaldefinition des Begriffs «löschen». Der Rechtsprechung des OGH³⁴ lässt sich entnehmen, dass Löschen im Sinne des Datenschutzgesetzes «physisches Löschen» bedeutet, rein logisches Löschen reicht hingegen nicht aus. Das DSG 1978 verstand unter «physischem Löschen» das Unkenntlichmachen von Daten in der Weise, dass eine Rekonstruktion nicht möglich ist. «Logisches Löschen» bedeutete

²⁸ Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 – StMV 2004) i.d.F. BGBl. II Nr. 278/2015.

²⁹ § 26 Abs. 7 DSG.

³⁰ § 13 PHG.

³¹ § 68 Abs. 1 ASVG. Die Verjährung ist gehemmt, solange ein Verfahren in Verwaltungssachen bzw. vor den Gerichtshöfen des öffentlichen Rechtes über das Bestehen der Pflichtversicherung oder die Feststellung der Verpflichtung zur Zahlung von Beiträgen anhängig ist.

³² BRODIL, Löschung von Arbeitnehmerdaten, ZAS 2014/54, S. 335.

³³ GRÜNANGER, Recht auf Löschung des Personalakts? ecoloex 8/2014, S. 675.

³⁴ OGH 15. April 2010, 6 Ob 4/10p.

hingegen die Verhinderung des Zugriffs von Daten durch programmtechnische Maßnahmen.³⁵ Das Gericht folgte der Meinung JAHNELS³⁶, demzufolge es nicht ausreicht, *«die Datenorganisation so zu verändern, dass ein «gezielter Zugriff» auf die betreffenden Daten ausgeschlossen ist.»*³⁷ Es ist aber wohl nicht das physische Vernichten des Datenträgers gefordert.³⁸ Zudem ist auch eine Anonymisierung zulässig³⁹, da in der Folge keine personenbezogenen Daten mehr vorliegen.

Wenn Daten aus wirtschaftlichen Gründen nur zu bestimmten Zeitpunkten gelöscht werden können, sind sie bis zur Löschung zu sperren.⁴⁰ Hat der Auftraggeber zu löschende Daten vor der Löschung übermittelt, sind die Empfänger davon zu verständigen, sofern dies keinen unverhältnismäßigen Aufwand bedeutet und die Empfänger noch feststellbar sind.⁴¹

2.1.5. Sanktionen

Wer Daten nicht fristgerecht löscht, begeht eine Verwaltungsübertretung, die mit einer Strafe bis EUR 500 bedroht ist.⁴² Werden Daten entgegen einem rechtskräftigen Urteil oder Bescheid nicht gelöscht, sind Strafen bis zu EUR 25'000 möglich.⁴³

2.2. Änderungen durch die Datenschutz-Grundverordnung

Auch nach der DS-GVO gilt der Grundsatz der Speicherbegrenzung, demgemäß personenbezogene Daten nur solange in personenbezogener Form gespeichert werden dürfen, wie es für die Zwecke der Verarbeitung erforderlich ist. Ausnahmen sind zulässig für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke.⁴⁴ Unternehmen haben somit auch weiterhin Löschpflichten zu beachten. Hinzu tritt nun das sogenannte Recht auf Vergessenwerden.

2.2.1. Löschpflichten und Speicherdauer

Das Recht auf Löschung findet sich in Art. 17 DS-GVO. Demnach ist der Verantwortliche (ehemals Auftraggeber) dazu verpflichtet, Daten unverzüglich zu löschen, wenn sie für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind; wenn ein Betroffener seine Zustimmung widerruft und es keine anderweitige Rechtsgrundlage für die Verarbeitung gibt; wenn ein Betroffener berechtigterweise Widerspruch gegen die Verarbeitung erhebt; wenn die Daten unrechtmäßig verarbeitet wurden oder wenn die Löschung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist. Diese Löschpflichten decken sich weitestgehend mit der Rechtslage gemäß DSGVO.⁴⁵ Neu eingefügt wurde eine gesonderte Löscherpflicht für Dienste der Informationsgesellschaft⁴⁶, die personenbezogene Daten Minderjähriger verarbeiten.⁴⁷

Das Widerspruchsrecht bezieht sich weiterhin auf besondere Situationen, in denen eine Verarbeitung der Betroffenenendaten zu unterbleiben hat, wenn nicht zwingende schutzwürdige und überwiegende Gründe für die Verarbeitung auf Seiten des Verantwortlichen vorliegen oder die Verarbeitung der Ausübung von Rechtsan-

³⁵ Art. 2 § 3 Z 11 DSGVO 1978 i.d.F. DSGVO-Novelle 1986.

³⁶ A.A. DOHR/POLLIERER/WEISS/KNYRIM, Kommentar Datenschutzrecht², § 27 DSGVO Rz 18.

³⁷ JAHNEL, Handbuch Datenschutzrecht (2010), S. 159.

³⁸ KASTELIZ/LEITER, OGH: Art der Löschung nach Ausübung des Widerspruchsrechts, jusIT 2010/69, S. 147.

³⁹ Vgl. KNYRIM, Handbuch Datenschutzrecht² (2012), S. 81.

⁴⁰ § 27 Abs. 6 DSGVO.

⁴¹ § 27 Abs. 8 DSGVO.

⁴² § 51 Abs. 2a DSGVO.

⁴³ § 51 Abs. 1 Z 3 DSGVO.

⁴⁴ Art. 5 Abs. 1 lit. e DS-GVO. Vgl. auch Erwägungsgrund 39.

⁴⁵ Vgl. Kapitel 2.1.

⁴⁶ Vgl. § 3 Z 1 ECG.

⁴⁷ Art. 17 Abs. 1 lit. f DS-GVO.

sprüchen dient.⁴⁸ Explizit erwähnt wird nun das jederzeitige Widerspruchsrecht gegen die Verarbeitung personenbezogener Daten zum Zweck der Direktwerbung.⁴⁹

Die Löschpflichten gelten nicht, soweit die Datenverarbeitung erforderlich ist zur Ausübung des Rechts auf freie Meinungsäußerung und Information; zur Erfüllung einer rechtlichen Verpflichtung, zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde; aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit; für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke; oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.⁵⁰

Gesonderte Löschfristen und Aufbewahrungspflichten richten sich somit auch weiterhin nach nationalen Vorschriften der Mitgliedstaaten⁵¹ oder nach dem Recht der Europäischen Union.⁵² Personenbezogene Daten dürfen nicht länger als nötig gespeichert werden. Der Verantwortliche hat deshalb Fristen für die Löschung oder regelmäßige Überprüfungen vorzusehen.⁵³ Neu ist, dass die Speicherdauer bzw. Kriterien für die Speicherdauer dem Betroffenen bereits bei der Erhebung von personenbezogenen Daten mitzuteilen sind.⁵⁴ Auch im Verfahrensverzeichnis sind, anders als bisher bei der Meldung zum Datenverarbeitungsregister, – wenn möglich – die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien anzugeben.⁵⁵

Einer Löschung auf Antrag ist nun innerhalb eines Monats nachzukommen. Bei einer hohen Komplexität oder Anzahl von Anträgen kann sich diese Frist um weitere zwei Monate verlängern.⁵⁶ Auch weiterhin gilt, dass Betroffene über eine Löschung bzw. Gründe für eine Nichtlöschung zu informieren sind, wobei im Falle der Nichtlöschung nun zusätzlich auf eine Beschwerdemöglichkeit bei der Aufsichtsbehörde bzw. auf gerichtliche Rechtsbehelfe hinzuweisen ist.⁵⁷ Hat der Verantwortliche Daten vor der Löschung übermittelt, ist der Empfänger über das Löschungsbegehren zu informieren, sofern dies keinen unverhältnismäßigen Aufwand erfordert. Betroffenen sind die Empfänger auf Anfrage mitzuteilen.⁵⁸ Kann der Verantwortliche einen Betroffenen nicht identifizieren, muss er einem Löschungsbegehren nicht nachkommen.⁵⁹

2.2.2. Das Recht auf Vergessenwerden

Das Recht auf Vergessenwerden fand sich bereits im ersten Entwurf zur DS-GVO⁶⁰ und geht auf eine Idee MAYER-SCHÖNBERGERS zurück, der anregte, Daten mit einem Verfallsdatum zu versehen, um einer dauerhaften Speicherung im Internet entgegenzutreten.⁶¹ Die technische Umsetzung eines «digitalen Radiergummis» im Internet sollte sich allerdings als unmöglich erweisen.

In der Folge erlangte das Recht auf Vergessenwerden Berühmtheit durch die «Google Spain» Entscheidung des Europäischen Gerichtshofs⁶², in der Suchmaschinenbetreiber dazu verpflichtet wurden, Links zu Webseiten

⁴⁸ Art. 21 DS-GVO.

⁴⁹ Zur bisherigen Rechtslage vgl. § 107 TKG.

⁵⁰ Art. 17 Abs. 3 DS-GVO.

⁵¹ Siehe dazu Kapitel 2.1.3.

⁵² Vgl. Art. 17 Abs. 1 lit. e und Abs. 3 lit. b DS-GVO.

⁵³ Vgl. Erwägungsgrund 39 zur DS-GVO.

⁵⁴ Art. 13 Abs. 2 und Art. 14 Abs. 2 DS-GVO.

⁵⁵ Art. 30 Abs. 1 lit. f DS-GVO.

⁵⁶ Art. 12 Abs. 3 DS-GVO. Dem Betroffenen sind die Gründe der Verzögerung binnen eines Monats mitzuteilen.

⁵⁷ Art. 12 Abs. 4 DS-GVO.

⁵⁸ Art. 19 DS-GVO.

⁵⁹ Art. 12 Abs. 2 i.V.m. Art. 11 Abs. 2 DS-GVO.

⁶⁰ Art. 17 Entwurf zur DS-GVO vom 25. Januar 2012, KOM(2012) 11.

⁶¹ MAYER-SCHÖNBERGER, Delete: The Virtue of Forgetting in the Digital Age (2009).

⁶² EuGH, 13. Mai 2014, C-131/12.

zu löschen, wenn sich auf diesen Informationen über Personen befinden, die veraltet sind⁶³ und an denen kein öffentliches Interesse besteht. Um «Vergessen zu werden» wird die Gatekeeper-Funktion von Suchmaschinen dahingehend genutzt, dass nach einer Link-Löschung das Auffinden von beanstandeten Informationen über Betroffene im Internet erheblich erschwert ist. Rechtlich leitete der EuGH seine Entscheidung aus dem Lösungsanspruch und dem Widerspruchsrecht der Datenschutzrichtlinie 1995 sowie der Achtung des Privat- und Familienlebens (Art. 7 GRC) und dem Schutz personenbezogener Daten (Art. 8 GRC) ab.⁶⁴

In der DS-GVO findet sich das Recht auf Vergessenwerden nun als in Klammern beigefügter Zusatz zum Recht auf Löschung. Es soll als Ausweitung des Rechts auf Löschung verstanden werden und sich auf das Internet beziehen.⁶⁵ Art. 17 Abs. 2 DS-GVO schreibt vor, dass Verantwortliche, die personenbezogene Daten öffentlich gemacht haben und zur Löschung verpflichtet sind, angemessene Maßnahmen, auch technischer Art, treffen müssen, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen Daten oder von Kopien oder Replikationen dieser Daten verlangt hat. Diese Bestimmung wird ebenso wie Art. 17 Abs. 1 DS-GVO von Art. 17 Abs. 3 DS-GVO eingeschränkt.

Die Tragweite des Art. 17 Abs. 2 DS-GVO ist bisher nicht geklärt. Die Bezugnahme auf Links, Kopien oder Replikationen der Daten spricht m.E. für eine enge Anlehnung an die Öffentlichmachung der Daten. Werden die Daten durch einen Dritten in einem neuen Kontext verwendet, ist Art. 17 Abs. 2 DS-GVO wohl nicht mehr anwendbar. Die Erstellung von Kopien oder Replikationen durch Dritte im World Wide Web grundsätzlich zu überwachen, kann m.E. nicht als angemessene Maßnahme betrachtet werden.⁶⁶ Vielmehr bezieht sich der Anwendungsbereich des Art. 17 Abs. 2 DS-GVO m.E. nur auf Kopien, Replikationen und Links, die zum Zeitpunkt der Löschverpflichtung selbst öffentlich auffindbar sind.⁶⁷ Es müssten die feststellbaren Webseiten- und Suchmaschinenbetreiber, die diese Daten verarbeiten, nicht mehr vom Betroffenen, sondern nun vom Verantwortlichen über ein Löschbegehren informiert werden, womit sich der Aufwand der Rechtsverfolgung für den Betroffenen verringert. Fraglich ist allerdings, inwieweit Art. 17 Abs. 2 DS-GVO dem Betroffenen einen eigenständig durchsetzbaren Rechtsanspruch gegenüber dem Verantwortlichen gewährt.

2.2.3. Sanktionen

Bei Verstößen gegen das Recht auf Löschung (Recht auf Vergessenwerden) können Geldbußen bis zu EUR 20'000'000 oder 4% des weltweiten Jahresumsatzes eines Unternehmens verhängt werden.⁶⁸

2.3. Die Verwendung von Cloud-Diensten

Es ist für Unternehmen heute üblich, nicht mehr alle Datenverarbeitungen selbst vorzunehmen. Insbesondere die Verwendung von Cloud-Diensten bietet die Möglichkeit kosteneffizient Datenverarbeitungen auszulagern. Der österreichische Gesetzgeber definiert in § 6 Abs. 3 GTelG⁶⁹ Cloud Computing als Datenspeicher, *«die einem Auftraggeber bedarfsorientiert von einem Betreiber bereitgestellt werden»*. Die Cloud-Anbieter

⁶³ Im Fall «Google Spain» 16 Jahre. Vgl. aber ein viel kritisiertes Urteil aus Italien, demzufolge Onlineartikel bereits nach 2 Jahren zu löschen sein sollen. <http://www.golem.de/news/recht-auf-vergessenwerden-online-artikel-bekommen-ablaufdatum-1609-123354.html>.

⁶⁴ EuGH, 13. Mai 2014, C-131/12, Rz 99.

⁶⁵ Vgl. Erwägungsgrund 66 zur DS-GVO.

⁶⁶ Selbst sofern dies technisch möglich ist. Vgl. aber bspw. das Abfotografieren des Bildschirms.

⁶⁷ Bspw. über Suchmaschinen. Damit würde in Anlehnung an EuGH C-131/12 und in Einklang mit Art. 7 und 8 GRC einer Prangerwirkung im Internet entgegen gewirkt.

⁶⁸ Art. 83 Abs. 5 lit. b DS-GVO.

⁶⁹ Bundesgesetz betreffend Datensicherheitsmaßnahmen bei der Verwendung elektronischer Gesundheitsdaten (Gesundheitstelematikgesetz 2012 – GTelG 2012).

verarbeiten Daten in aller Regel im Auftrag des Verantwortlichen⁷⁰ und sind deshalb Auftragsverarbeiter.⁷¹ Wie bereits gemäß DSGVO, bleibt der Verantwortliche dabei auch nach der DS-GVO für die Rechtmäßigkeit der Verarbeitung verantwortlich.⁷² Er darf nur solche Auftragsverarbeiter beauftragen, die den Anforderungen an die DS-GVO gerecht werden und den Schutz der Rechte der Betroffenen gewährleisten.⁷³

Betreffend das Recht auf Löschung (Recht auf Vergessenwerden) ist vertraglich sicherzustellen, dass der Auftragsverarbeiter in der Lage ist, einem entsprechenden Begehren nachzukommen.⁷⁴ Ob die Überwachung und Durchführung von Löschvorschriften insgesamt dem Auftragsverarbeiter übertragen werden kann, ohne dass dieser zum Verantwortlichen für die Verarbeitung wird, ist allerdings fraglich. Meines Erachtens ist dies dann möglich, wenn die Kriterien der Löschung ausreichend bestimmt vorgegeben werden und der Auftragsverarbeiter lediglich die technischen und organisatorischen Maßnahmen zur Erfüllung der Kriterien auswählt.⁷⁵ Unternehmen haben bei der Verwendung von Cloud-Diensten auch darauf zu achten, dass eine wirksame Löschung⁷⁶ oder Rückgabe der Daten nach Beendigung des Auftrags vertraglich geregelt wird.⁷⁷

3. Fazit

Bereits nach der geltenden Rechtslage ist die Speicherung von personenbezogenen Daten nicht ohne Einschränkung zulässig. In der DS-GVO werden die Löschpflichten und Ausnahmen nun konkreter benannt und gegenübergestellt. Der überwiegende Teil dieser Pflichten ist nicht neu, vor dem Hintergrund der nahenden DS-GVO, die eine gravierende Verschärfung der Sanktionen für Verstöße mit sich bringt, sollten Unternehmen allerdings die Praxis ihrer Datenverarbeitung überdenken.

Zunächst müssen die Datenbestände erfasst werden, was insbesondere im Fall der Aufteilung über mehrere Systeme bereits eine langwierige Aufgabe darstellen kann. In der Folge sollte ein Löschkonzept entwickelt und implementiert werden. Löschpflichten und Aufbewahrungspflichten stehen in komplexen Verflechtungen zueinander, die häufig erst in Einzelfallbetrachtungen richtig aufgelöst werden können. Aus diesem Grund ist es von großer Bedeutung, dass die im Unternehmen verwendete Software flexible Lösungen ermöglicht. Dies betrifft insbesondere den Widerruf einer Einwilligung, einen berechtigten Widerspruch, unberechtigt erhobene Daten, einen Antrag auf Löschung oder den Streitfall.

Für den Großteil der Datenverarbeitung müssen allerdings Standardlösungen vorgegeben werden, um Löschpflichten effizient umsetzen zu können. Die Daten sind Datenarten zuzuordnen, die nach bestimmten Löschregeln zu löschen sind.⁷⁸ Werden personenbezogene Daten übermittelt oder öffentlich gemacht, ist dies gesondert zu vermerken, um den geforderten Informationspflichten nachkommen zu können. Bei der Verwendung von Cloud-Diensten ist darauf zu achten, dass das beauftragende Unternehmen für die Einhaltung der Löschpflichten verantwortlich bleibt, weshalb es den Cloud-Anbieter vertraglich dazu verpflichten muss, die genannten Vorschriften zu erfüllen.

⁷⁰ Vgl. WEICHERT, Cloud Computing und Datenschutz, DuD 10/2010, S. 682.

⁷¹ Art. 4 Z 8 DS-GVO. Im DSGVO wird der Begriff «Dienstleister» verwendet (§ 4 Z 5 DSGVO).

⁷² Der Auftragsverarbeiter ist weisungsgebunden (Art. 29 DS-GVO). Verstößt er gegen die DS-GVO und bestimmt die Zwecke der Verarbeitung selbst, gilt er diesbezüglich als Verantwortlicher (Art. 28 Abs. 10 DS-GVO, vgl. auch § 4 Z 4 DSGVO).

⁷³ Art. 28 Abs. 1 DS-GVO. Vgl. auch § 10 Abs. 1 DSGVO.

⁷⁴ Art. 28 Abs. 3 lit. e DS-GVO. Vgl. auch § 11 Abs. 1 Z 4 DSGVO.

⁷⁵ Vgl. Artikel 29 Datenschutzgruppe, WP 196, Stellungnahme 05/2012 zum Cloud Computing, S. 10. S.a. BOGENDORFER, Und was ändert sich für Dienstleister mit der DSGVO noch?, in: Knyrim (Hrsg.), Datenschutz-Grundverordnung (2016), S. 171.

⁷⁶ Zum Problem der wirksamen Löschung bei Cloud-Diensten: Art. 29 Datenschutzgruppe, WP 196, S. 15.

⁷⁷ Art. 28 Abs. 3 lit. g DS-GVO. Vgl. auch § 11 Abs. 1 Z 5 DSGVO.

⁷⁸ HAMMER/SCHULER, Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten (2015), S. 13.