Regulierung der Datenlöschung im europäischen Datenschutzrecht

Dominik Schmelz

I. Einleitung

Der Datenschutz stellt ein fundamentales Recht dar, das in der heutigen digitalen Ära von entscheidender Relevanz ist, da die Menge der erfassten Daten sowie die Rechenleistung kontinuierlich zunehmen und somit eine parallele Verarbeitung ermöglichen. Es lässt sich feststellen, dass der Partei, welche über mehr Informationen bezüglich einer anderen Partei verfügt, im Allgemeinen eine Machtposition innewohnt. Das Machtverhältnis ist in dieser Hinsicht als stark unausgewogen zu bewerten. Um eine gerechte digitale Umgebung zu schaffen, ist eine Korrektur dieses Machtungleichgewichts erforderlich. Es ist daher von essentieller Bedeutung, Personen, deren Daten verarbeitet werden, vor den potenziellen Risiken zu schützen oder sie zumindest transparent zu machen.

Insbesondere die Datenschutz-Grundverordnung (DSGVO), Verordnung (EU) 2016/679, legt großen Wert auf den Schutz personenbezogener Daten durch technische Maßnahmen, um die damit verbundenen Risiken für die Betroffenen zu minimieren. Das Recht auf Löschung personenbezogener Daten ist neben den verschiedenen Auskunftsrechten der Kern der Betroffenenrechte. Kritisch betrachtet fehlen jedoch konkrete Anleitung, Methodik oder Instrumente dazu in der Norm[1] [2].

Diese Konkretisierung der Verpflichtung ist jedoch essenziell, da die durch die DSGVO angestrebte Balance zwischen Datenverarbeitern und Betroffenen nur erreicht werden kann, wenn Verpflichtungen des Datenverarbeiters, welche auf einem Vertrauen auf die korrekte Ausführung basieren, auch einer rechtlichen Verpflichtung entsprechen. Im Gegensatz zu den Auskunftsrechten ist das Löschen von Daten für den Betroffenen

1 *Kühling ea*, Datenschutz-Grundverordnung, BDSG4. Auflage, Art. 17 Rz. 17.

2 *Fritz*, Das Löschungsrecht nach Art 17 DSGVO in der Entscheidungspraxis und Rechtsprechung, S. 93.

schwerer nachvollziehbar und für den Datenverarbeiter schwerer zu beweisen.

Im Zuge der fortschreitenden Digitalisierung und Datenverarbeitung kommt der Untersuchung der rechtlichen und technischen Rahmenbedingungen sowie deren Wirksamkeit zur Gewährleistung des Schutzes personenbezogener Daten eine entscheidende Bedeutung zu. Der Datenschutz durch Technikgestaltung spielt hierbei eine zentrale Rolle und ist Gegenstand intensiver rechtlicher und technischer Debatten.

Die vorliegende Untersuchung verfolgt das zentrale Ziel, die technischen, rechtlichen und nutzerbezogenen Dimensionen verschiedener Löschmechanismen im Kontext des menschenzentrierten Datenschutzes systematisch zu analysieren. Der menschenzentrierte Ansatz erweist sich hierbei als maßgeblich, da nicht die technischen Spezifikationen oder Implementierungsdetails des Systems im Vordergrund stehen, sondern vielmehr die Erwartungen der Nutzerinnen und Nutzer. Im Fokus steht somit die Frage, inwieweit bestehende technisch-juristische Löschmechanismen den Anforderungen und Bedürfnissen der betroffenen Personen entsprechen. Besondere Aufmerksamkeit gilt dabei der Identifikation möglicher Divergenzen zwischen den technischen Umsetzungsmöglichkeiten und den rechtlichen Vorgaben. Die Ergebnisse dieser Analyse sollen nicht nur dazu beitragen, potenzielle Herausforderungen aufzuzeigen, sondern auch praxisorientierte Empfehlungen für die Verbesserung des Datenschutzes zu liefern. Dabei soll insbesondere die folgende Forschungsfrage beantwortet werden:

> *Inwieweit erfüllen verschiedene juristisch-technische Löschmechanismen im menschenzentrierten Datenschutz die technischen Anforderungen, sind rechtlich konform?*

Um eine detaillierte Analyse der juristisch-technischen Löschmechanismen im Rahmen des menschenzentrierten Datenschutzes zu ermöglichen, werden folgende Unterforschungsfragen untersucht:

- Welche Löschmechanismen existieren?
- Inwieweit ist die Konformität der Löschmechanismen zur DSGVO gegeben?

Die erste Unterforschungsfrage zielt darauf ab, die technischen Spezifikationen zu identifizieren, die für die effektive Umsetzung von Löschmechanismen im Datenschutz relevant sind. Hierbei sollen insbesondere aktuelle technische Standards und Normen sowie ihre Anwendbarkeit auf verschiedene Datenkontexte analysiert werden.

Die zweite Unterforschungsfrage befasst sich mit der juristischen Konformität der vorhandenen Löschmechanismen. Es sollen Rechtsnormen, Kommentare und Urteile untersucht werden, um herauszufinden, wie verschiedene Mechanismen den Anforderungen der Datenschutzgesetze, insbesondere der DSGVO, entsprechen und ob mögliche rechtliche Interpretationen konsistent angewendet werden.

Die methodische Vorgehensweise dieser Arbeit basiert auf einem ganzheitlichen Ansatz, der sowohl rechtliche als auch technische Aspekte berücksichtigt. Es wird daher eine Kombination aus qualitativen und quantitativen Methoden der Natur- und Geisteswissenschaften angewendet, um eine umfassende Bewertung der Löschmechanismen vorzunehmen. Dabei werden rechtliche Textanalysen und technische Bewertungen durchgeführt.

Die vorliegende Arbeit ist wie folgt strukturiert: Nach der Einleitung, in der der Hintergrund, die Zielsetzung, die Forschungsfragen, die Methodik und der Aufbau der Arbeit dargelegt werden, folgt der theoretische Hintergrund. In diesem Abschnitt werden die relevanten rechtlichen Konzepte, technischen Standards und die bisherige Literatur dargestellt. Die Diskussion der Ergebnisse im Kontext der Forschungsfragen und des theoretischen Hintergrunds führt zu Schlussfolgerungen, in denen die wichtigsten Erkenntnisse zusammengefasst und praktische sowie theoretische Implikationen diskutiert werden.

Hinweis: Zur besseren Lesbarkeit wird in dieser Arbeit das generische Maskulinum verwendet. Die in dieser Arbeit verwendeten Personenbezeichnungen beziehen sich – sofern nicht anders kenntlich gemacht – auf alle Geschlechter.

II. Juristische Analyse

Die Datenschutz-Grundverordnung (DSGVO) fungiert als rechtlicher Rahmen zur Gewährleistung des Schutzes personenbezogener Daten innerhalb der Europäischen Union. Das Ziel besteht in der Gewährleistung des Schutzes der Privatsphäre sowie der Förderung des freien Datenverkehrs innerhalb des Binnenmarktes. Auf nationaler Ebene wird das österreichische Datenschutzgesetz (DSG) als Instrument eingesetzt, um spezifisch nationale Anforderungen und Gegebenheiten zu berücksichtigen.

Von besonderer Relevanz ist hierbei Art. 17 DSGVO, der das Recht auf Löschung, auch bekannt als das „Recht auf Vergessenwerden", normiert.

Diese Bestimmung wird im österreichischen Datenschutzgesetz durch § 1 Z. 3 DSG als Verfassungsbestimmung weiter konkretisiert, was ihre herausragende Bedeutung im nationalen Rechtsrahmen unterstreicht.

Eine explizite Legaldefinition des Begriffs „Löschen" ist in der DSGVO sowie dem aktuellen österreichischen DSG jedoch nicht enthalten. Die fehlende Definition des Begriffs „Löschrecht" wirft wesentliche Fragen hinsichtlich der praktischen Umsetzung und der rechtlichen Implikationen auf. Die vorliegende Untersuchung widmet sich der Fragestellung, wie der Begriff des Löschens im Kontext moderner digitaler Technologien und der damit verbundenen Datenverarbeitung zu interpretieren und anzuwenden ist.

Ziel der vorliegenden Untersuchung ist die Analyse des Zwecks und der Tragweite des Rechts auf Löschung gemäß Art. 17 DSGVO sowie im Kontext des DSG. Der Fokus der Untersuchung liegt auf der teleologischen und historischen Auslegung, mit deren Hilfe der gesetzgeberische Wille und die zugrunde liegenden Ziele dieser Normen erfasst werden sollen. Ziel dieser Vorgehensweise ist es, die Anwendung der Normen in der Praxis zu erleichtern.

A. Primärquellen

Das sogenannte „Recht auf Vergessenwerden" ist als fundamentales Recht der informationellen Selbstbestimmung zu begreifen. Das in Art. 17 implementierte „Recht auf Löschung" ermöglicht die Löschung personenbezogener Daten auf Verlangen des Betroffenen oder wenn der Zweck der weiteren Aufbehaltung entfällt, wobei bestimmte Ausnahmen bestehen. Die Löschung personenbezogener Daten ist erforderlich, wenn diese für die ursprünglichen Zwecke nicht mehr erforderlich sind, die betroffene Person ihre Einwilligung widerruft (Art. 17 Abs. 1 lit. b), Widerspruch gegen die Verarbeitung einlegt (Art. 21 Abs. 1), die Daten unrechtmäßig verarbeitet wurden (Art. 17 Abs. 1 lit. d) oder eine rechtliche Verpflichtung zur Löschung besteht (Art. 17 Abs. 1 lit. e).

Sofern die Löschung aufgrund der Komplexität der Anfrage länger als einen Monat in Anspruch nimmt, ist der Verantwortliche dazu verpflichtet, den Betroffenen darüber in Kenntnis zu setzen (Art. 12 Abs. 3).

Im Falle veröffentlichter Daten ist es die Pflicht des Verantwortlichen, unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, einschließlich technischer Maß-

nahmen, zu ergreifen, um andere Verantwortliche darüber zu informieren, dass die betroffene Person die Löschung sämtlicher Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt (Art. 17 Abs. 2). Erwägungsgrund 66 konkretisiert das Recht auf Löschung aus Art. 17 Abs. 2 der DSGVO, indem er festlegt, dass der Verantwortliche unter Berücksichtigung der verfügbaren Technologien und der ihm zur Verfügung stehenden Mittel angemessene Maßnahmen treffen sollte, um andere Verantwortliche, die die Daten verarbeiten, über den Löschungsantrag zu informieren. Gemäß Erwägungsgrund 65 wird das Recht der betroffenen Person auf Löschung ihrer personenbezogenen Daten im Kindesalter explizit dargelegt. Es sei darauf hingewiesen, dass die betroffene Person dieses Recht insbesondere dann ausüben kann, wenn die Daten im Kindesalter erhoben wurden und eine Löschung zu einem späteren Zeitpunkt erfolgen soll.

§ 4 Z 4 DSG[3] erlaubt dem Verantwortlichen, die Verarbeitung der betreffenden personenbezogenen Daten mit der Wirkung nach Art. 18 Abs. 2 DSGVO („Recht auf Einschränkung der Verarbeitung") einzuschränken, wenn die Berichtigung oder Löschung von automationsunterstützt verarbeiteten personenbezogenen Daten nicht unverzüglich erfolgen kann, weil diese aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann. Das bedeutet, dass Daten, wenn es technisch nicht möglich ist, sie zu löschen, zeitweilig auch nur eine Einschränkung der Verarbeitung erfolgen darf.

Gemäß Art. 24 Abs. 1 verlangt der risikobasierte Ansatz vom Verantwortlichen, unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen angemessene technische und organisatorische Maßnahmen zu ergreifen. Der Aufwand soll im Verhältnis zu dem Risiko (für den Betroffenen) und den Kosten der Implementierung stehen, wobei ein hohes Maß an Schutz und Datensicherheit gewährleistet sein muss (Art. 25 Abs. 1).

Gemäß Art. 32 Abs. 1 lit. b werden Verantwortliche und Auftragsverarbeiter dazu verpflichtet, geeignete technische und organisatorische Maßnahmen zu ergreifen, um ein dem Risiko angemessenes Sicherheitsniveau zu gewährleisten. Dies umfasst die Gewährleistung der Vertraulichkeit, Inte-

3 Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), Fassung vom 29.06.2024, Art. 2 §4.

grität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten.

Die Vertraulichkeit ist im Hinblick der Löschung wichtig, denn sie stellt sicher, dass nur autorisierte Personen Zugriff auf personenbezogene Daten haben und dass diese Daten vor unbefugter Offenlegung geschützt sind. Die Integrität gewährleistet, dass die Daten korrekt und unverändert bleiben, indem Maßnahmen ergriffen werden, um unbefugte Änderungen zu verhindern, so zum Beispiel durch eine partielle Löschung. Verfügbarkeit bedeutet, dass personenbezogene Daten bei Bedarf zur Verfügung stehen und nicht unbefugt blockiert oder gelöscht werden können. Die Belastbarkeit bezieht sich auf die Fähigkeit des Systems, einem Angriff oder einer Störung standzuhalten und seine Funktionen auch unter widrigen Bedingungen aufrechtzuerhalten. Die Überlastung eines Systems darf also auch nicht zu einem Verlust von Daten führen.

Art. 25 Abs. 1 schreibt vor, dass Verantwortliche und Auftragsverarbeiter bereits bei der Planung von Verarbeitungsvorgängen technische und organisatorische Maßnahmen, unter Berücksichtigung der Risiken für die Betroffenen und der Implementierungskosten, ergreifen müssen, um die Datenschutzgrundsätze zu gewährleisten. Dabei sind insbesondere die Prinzipien „Datenschutz durch Technikgestaltung" bzw. „Datenschutz durch datenschutzfreundliche Voreinstellungen" zu berücksichtigen[4]. Die Implementierung solcher Maßnahmen von Beginn an ermöglicht eine effektive Umsetzung des Datenschutzes und trägt dazu bei, Datenschutzverletzungen zu verhindern. „Datenschutz durch Technikgestaltung" bezieht sich auf die systematische Integration von Datenschutzprinzipien in die Entwicklung von Produkten, Systemen und Prozessen von deren Anfangsphase an. Datenschutz durch datenschutzfreundliche Voreinstellungen[5] bedeutet, dass standardmäßig die höchstmöglichen Datenschutzeinstellungen angewendet werden sollen, ohne dass der Benutzer aktiv eingreifen muss.

Es sei darauf hingewiesen, dass Löschkonzepte, die mitunter in der Praxis Anwendung finden, nicht unmittelbar aus der DSGVO resultieren. Gemäß Art. 5 Abs. 1 unterliegt die Verarbeitung personenbezogener Daten dem Grundsatz der Speicherbegrenzung. Das Löschkonzept fungiert in diesem Zusammenhang als Instrument, um dieser Verpflichtung systema-

4 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), OJ L 2016/119 [DSGVO], ErwG 78.

5 ebd, Art. 25 Abs. 1.

tisch, risikoorientiert und dokumentierbar nachzukommen und eben zu dokumentieren, wann und wie gelöscht wird. Diese Verpflichtung ergibt sich aus dem Prinzip der Rechenschaftspflicht nach Art. 5 Abs. 2, wonach der Verantwortliche die Einhaltung aller Grundsätze der Datenverarbeitung nachweisen muss.

Die Bestimmungen der Artikel 32 und 25 sowie die entsprechenden Erwägungsgründe verdeutlichen die Relevanz adäquater technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten. Diese Maßnahmen sind von entscheidender Relevanz für die Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Systemen und Diensten im Rahmen der Datenverarbeitung. Die nachfolgend erörterten Leitlinien des European Data Protection Board (EDPB) stellen eine zusätzliche Orientierungshilfe für die praktische Umsetzung dieser Anforderungen dar.

Art. 32 Abs. 1 fordert die Berücksichtigung des Stands der Technik bei der Implementierung von Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. In Bezug auf das Löschen von Daten bedeutet Stand der Technik, dass Verantwortliche aktuelle Technologien und Verfahren einsetzen sollen, um die sichere und vollständige Löschung personenbezogener Daten zu gewährleisten. Diese müssen laut Abs. 1 lit. d regelmäßig geprüft und ggf. nachgebessert werden. In seinem Kommentar erörtert Piltz, dass gemäß Art. 32 Abs. 1 DSGVO der „Stand der Technik" eine autonome und einheitliche Interpretation innerhalb der EU erfordert, die unabhängig von nationalen Gesetzen ist. Die exakte Bedeutung des Terminus „Stand der Technik" bleibt indes unklar, insbesondere, ob dieser neueste technologische Entwicklungen einschließt oder ob branchenübliche Standards ausreichen. Die Argumentation fußt auf der Prämisse, dass es sich höchstwahrscheinlich nicht um den höchstmöglichen Technologiestandard handelt, da der EuGH diesen nur bei Verwendung des Begriffs „Stand der Wissenschaft und Technik" annimmt.

Piltz meint, es seien „Empfehlungen staatlicher Stellen zu berücksichtigen wie etwa die IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI)"[6]. Und die „enge Einbindung des BSI in den gesamten Verfahrensablauf beim Ausbau und Betrieb der IT kann die durch Art. 32 Abs. 1 angeordnete Berücksichtigung des Stands der Technik

6 *Piltz* in Datenschutz-Grundverordnung: VO (EU) 2016/679: Bundesdatenschutzgesetz: Kommentar, Art. 32 Rz. 19.

sichern“[7]. Einer der Löschstandards des BSI wird in Abschnitt III.F „BSI Grundschutz CON.6„ beschrieben.

B. Kommentare und Leitlinien

Die rechtlichen Rahmenbedingungen für die Löschung personenbezogener Daten gemäß der DSGVO erfahren durch nationale Entscheidungen eine Präzisierung. Artikel 17 und 12 der DSGVO geben keine spezifischen Methoden für die Löschung vor. Die Kommentare zum Art. 17 fokussieren sich primär auf die Voraussetzungen und Ausnahmen der Löschverpflichtung. In einigen Fällen erfolgt eine detaillierte Auseinandersetzung mit spezifischen Zeiträumen und Benachrichtigungen. Eine Diskussion über die Modalitäten der Löschung ist eine Seltenheit.

Die österreichische Datenschutzbehörde (DSB) stellt fest, dass die Löschung erreicht ist, wenn „die Verarbeitung und Nutzung der personenbezogenen Daten einer betroffenen Person [...] nicht mehr möglich ist“[8]. Dies beinhaltet sowohl physische als auch digitale Daten, wie vom OGH bestätigt wird[9]. Bei der Anonymisierung als eine zulässige Löschmethode muss „sichergestellt werden, dass weder der Verantwortliche selbst noch ein Dritter ohne unverhältnismäßigen Aufwand einen Personenbezug wiederherstellen kann“[10]. Des Weiteren wurde von der DSB entschieden, dass eine zeitweilige Löschung ausreicht, also, dass die Möglichkeit einer Rekonstruktion der Daten zu einem späteren Zeitpunkt, mit besseren technischen Möglichkeiten, nicht ausreicht, um keine Löschung durch Anonymisierung darzustellen[11]. Darüber hinaus wurde dies im selbigen Bescheid verallgemeinert beschrieben, dass generell keine „völlige Irreversibilität“[12], was einer Vernichtung der Daten nahekommt, gefordert ist. Knyrim sieht auch diese Irreversibilität nicht als notwendig, definiert aber die „physische Löschung“ neben der Anonymisierung als Löschung, sodass „Daten unter

7 ebd, Art. 32 Rz. 19.
8 Datenschutzbehörde 05.12.2018, DSB-D123.270/0009-DSB/2018, *DSB-D123.270/0009-DSB/2018*.
9 *Fritz*, Das Löschungsrecht nach Art 17 DSGVO in der Entscheidungspraxis und Rechtsprechung.
10 ebd.
11 Datenschutzbehörde 05.12.2018, DSB-D123.270/0009-DSB/2018, *DSB-D123.270/0009-DSB/2018*.
12 ebd.

Anwendung üblicher Verfahren nicht mehr ausgelesen werden können“[13]. Des Weiteren wird von Knyrim definiert, dass physische Medien durch Zerstörung des Datenträgers vernichtet werden.

Der Terminus „Vernichtung“ von Daten im Sinne des Art. 4 Abs. 12 zur Definition der „Verletzung des Schutzes personenbezogener Daten“ bzw. eines Data Breaches wurde von der EDPB frei aus dem Englischen übersetzt als „wenn die Daten nicht mehr existieren oder nicht mehr in einer Form vorliegen, die für den für die Verarbeitung Verantwortlichen von Nutzen ist“[14] definiert. Abbildung 1 stellt die verschiedenen Begriffe in Relation zum Grad des Personenzuges dar.

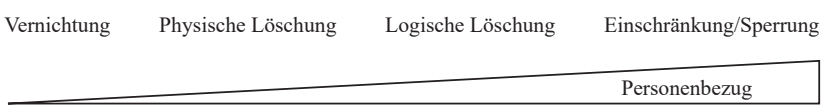

Abbildung 1 – Grade des Personenbezugs von Löschmaßnahmen

Zur Fragestellung der örtlichen Begrenzung beschäftigen sich Feiler und Forgo mit der Löschung aus Suchmaschinen und kommen in Referenz auf C-507/17 zum Schluss, dass es „kein Recht auf globale Löschung“ gibt, also eine Sperre des Datenzugriffs aus dem EWR ausreichend ist und dass generell eine Reduzierung der Verarbeitungstätigkeit auf ein Maß, dass die DSGVO nicht mehr Anwendung findet, einer Löschung nach DSGVO gleichkommt[15]. Knyrim differenziert das „Verarbeitungsverbot“ bzw die „Einschränkung“ auch zur Löschung, welches durch einen „Sperrvermerk bewerkstelligt werden“[16] kann. Er setzt dieses mit der „logischen Löschung“ gleich[17]. Kamann und Braun argumentieren, dass aus Art. 17 DSGVO, welcher beschreibt, dass der Betroffene die Löschung seiner personenbezogenen Daten verlangen kann, folgt, dass die betroffene Person den Umfang ihres Löschverlangens selbst bestimmen darf, wie etwa durch die Beschrän-

13 *Knyrim*, Praxiskommentar zum Datenschutzrecht - DSGVO und DSG 2019, Online, Art. 17 Rz. 63.
14 *EDPB*, Guidelines 9/2022 on personal data breach notification under GDPR Guidelines 9/2022: Data Breaches.
15 *Feiler/Forgó*, EU-DSGVO und DSG2. Auflage, Rz. 7.
16 *Knyrim*, Praxiskommentar zum Datenschutzrecht - DSGVO und DSG 2019, Online, Art. 17 Rz. 63.
17 ebd, Art. 4 Rz. 42.

kung auf bestimmte Daten, Datenkategorien, Verarbeitungsformen, Zwecke oder Teilverarbeitungsvorgänge[18].

Rechtlich ist eine geographische Einschränkung als Äquivalenz zur Löschung im örtlichen Anwendungsbereich nachvollziehbar, aber wegen der Tatsache, dass die Daten wiederum nicht unwiderruflich gelöscht sind, kann aus einer technischen Sicht, nur von einer „Einschränkung" ausgegangen werden, denn die Daten sind, zum Beispiel bei der Verwendung einer nicht Europäischen IP-Adresse wiederum öffentlich zugänglich. Das bedeutet, dass die Maßnahme nicht nur theoretisch, sondern auch leicht praktisch durch einen Laien aufgehoben werden kann. Knyrim beschreibt dieses Verfahren genauso als einen Spezialfall des Löschens und bezeichnet es als „delisting" [19] in Referenz auf C-131/12. Welches Verfahren zur Löschung verwendet wird, und damit wie sicher diese Löschung ist, kann laut Fritz nicht durch den Betroffenen verlangt werden. Er stellt klar, dass „kein Wahlrecht der Betroffenen hinsichtlich der Löschungsmethode besteht"[20]. Die EDPB formuliert den Begriff des „Rechts auf Auslistung" in ihrer Leitlinie 5/2019[21] zu dem Thema auf Basis des selbigen Urteils. Sie halten fest, dass Löschanträge, in diesem Fall „Auslistungsanträge" laut der Meinung des EDPB „nicht zur vollständigen Löschung der personenbezogenen Daten" führen, sondern eben nur eine Zugriffbeschränkung, sodass bei einer Suche nach einem Namen diese Ergebnisse nicht mehr gefunden werden, aber jegliche technische Speicherung der Daten (Index, Cache etc.) weiter erhalten bleibt, mit Ausnahmen wie zum Beispiel, dass der indizierte Webseitenbetreiber das indizieren der betroffenen Seite fortan verbietet. Dies wird über eine Datei „robots.txt" auf der Webseite automatisiert kundgetan. Neben weiteren Ausnahmen, bei denen die Löschung sofort passieren muss, werden auch Ausnahmen zur Behaltung der Daten formuliert, wie das Recht auf freie Meinungsäußerung.

Stellungnahmen und Empfehlungen, wie beispielsweise die Leitlinie 4/2019 des European Data Protection Board (EDPB), bieten praktische Hil-

18 *Braun/Kamann* in DS-GVO: Datenschutz-Grundverordnung: Kommentar, Art. 17 Rn. 72.

19 *Knyrim*, Praxiskommentar zum Datenschutzrecht - DSGVO und DSG 2019, Online, Art. 17 Rz. 63/1.

20 *Fritz*, Das Löschungsrecht nach Art 17 DSGVO in der Entscheidungspraxis und Rechtsprechung.

21 *EDPB*, Leitlinien 5/2019 zu den Kriterien des Rechts auf Vergessenwerden in Fällen in Bezug auf Suchmaschinen gemäß der DSGVO Leitlinien 5/2019 zum Recht auf Auslistung.

fe für die technische Umsetzung der Datenschutzanforderungen gemäß der DSGVO[22]. Die Leitlinien 4/2019 des EDPB zu Art. 25 DSGVO bieten eine detaillierte Analyse und praktische Anleitungen für die Umsetzung von Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen. Sie umfasst die Pflicht des Verantwortlichen zur Umsetzung geeigneter technischer und organisatorischer Maßnahmen gemäß Art. 25 Abs. 1 sowie die Verarbeitung nur erforderlicher personenbezogener Daten gemäß Art. 25 Abs. 2. Die Leitlinien behandeln verschiedene Aspekte, darunter Transparenz, Rechtmäßigkeit, Datenminimierung, Integrität, Vertraulichkeit und Rechenschaftspflicht.

Die technisch-organisatorischen Maßnahmen, inklusive dem dokumentierten Löschkonzept und damit den inkludierten Löschmechanismen müssen laut Art. 32 Abs. 1 lit. d regelmäßig überprüft werden. Zudem enthält sie Empfehlungen zur Zertifizierung nach Art. 25 Abs. 3 und Hinweise zur Durchsetzung von Art. 25 sowie deren Auswirkungen und Art. 32 Abs. 3 ähnlich lautende Empfehlungen zur Zertifizierung. Daher sind Verfahren und technische Normen wie in Kapitel III beschrieben, die in Zertifizierungen Anwendung finden, sinnvoll bei der Implementierung dieser Konzepte zu beachten.

C. Entscheidungen

In Fällen von besonderer Relevanz hinsichtlich der Vertraulichkeit sowie der Datenlöschung im Kontext der DSGVO bzw. der des DSG wurden wegweisende Entscheidungen durch den Europäischen Gerichtshof (EuGH), den österreichischen Obersten Gerichtshof (OGH) und die österreichische Datenschutzbehörde (DSB) getroffen.

Im Fall vom 15. April 2010 6Ob41/10p[23] entschied der OGH, dass eine „logische Löschung" nicht ausreicht und die Daten physisch gelöscht werden müssen, um eine Rekonstruktion unmöglich zu machen. Diese Entscheidung unterstreicht die Notwendigkeit einer irreversiblen Datenlöschung, um den Anforderungen des DSG 2000 zu entsprechen. In diesem Urteil wird die „logische Löschung" als „eine Maßnahme, mit der erreicht wird, dass Daten innerhalb der EDV-Anlage nicht mehr zur Verfügung

22 *EDPB*, Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen Leitlinien 4/2019 zu Artikel 25.

23 Oberster Gerichtshof 15.04.2010, 6Ob41/10p, *6Ob41/10p*.

stehen, unkenntlich gemacht werden sowie durch das Betriebssystem als nicht mehr vorhanden interpretiert werden“[24] definiert. Es wird klargestellt, dass ein rein logisches Löschen nicht ausreicht, um den Anforderungen von „Löschen“ zu genügen. Des Weiteren wird der Begriff „Sperre“ in Anlehnung an § 3 des Pre-DSGVO BDSG als „das Kennzeichnen gespeicherter personenbezogener Daten […], um ihre weitere Verarbeitung oder Nutzung einzuschränken“[25] definiert und klargestellt, dass auch diese nicht den Anforderungen von „Löschen“ zu genügen. Einzig das von der Vorinstanz bereits geurteilte „physische Löschen“ sei als „Unkenntlichmachen von Daten in der Weise, dass eine Rekonstruktion nicht möglich ist“[26], ausreichend. Des Weiteren wird festgestellt, dass die historische Interpretation, dass die Entfernung der Definition bei der Reformation des DSG 1978 zum DSG 2000 nicht bedeute, dass Löschen so interpretiert werden solle, dass der Betroffene schlechter gestellt werde.

Am 13. September 2012 bestätigte der OGH in einem weiteren Fall 6Ob107/12x[27], dass Daten aus einer Wirtschaftsdatenbank ebenfalls physisch gelöscht werden müssen, wenn der Betroffene dies fordert. Diese Entscheidung verdeutlicht die strikte Anwendung des physischen Löschens gegenüber bloßem Sperren der Daten, um den Datenschutz vollständig zu gewährleisten.

In einem Bescheid vom 5. Dezember 2018, DSB-D123.270/0009-DSB/2018[28] entschied die DSB, dass auch die Anonymisierung, also die Entfernung des Personenbezugs, als Löschung gelten kann. Dies bietet eine praktikable Alternative zur physischen Löschung, solange die Daten nicht mehr einer bestimmten Person zugeordnet werden können.

Zur „delisting“ Diskussion entschied der EuGH im Fall vom 8. Dezember 2022, Rechtssache C-460/20[29], dass ein Suchmaschinenbetreiber Links zu Inhalten mit offensichtlich unrichtigen Angaben auf Antrag der betroffenen Person aus der Ergebnisliste entfernen muss, ohne dass zuvor ein gerichtliches Verfahren gegen den Inhalteanbieter erforderlich ist. Die Löschung betrifft ausschließlich die De-Indexierung der Links und Vorschau-

24 ebd.
25 ebd.
26 ebd.
27 Oberster Gerichtshof 13.09.2012, 6Ob107/12x, *6Ob107/12x*.
28 Datenschutzbehörde 13.12.2018, DSB-D122.995/0003-DSB/2018, *DSB-D122.995/0003-DSB/2018*.
29 Europäischer Gerichtshof Rechtssache C-460/20, *TU und RE gegen Google LLC*.

bilder durch die Suchmaschine; eine Entfernung der Inhalte selbst ist nicht erforderlich.

Im Fall vom 13. Mai 2014, C-131/12[30], entschied der EuGH, dass Personen von Suchmaschinenbetreibern wie Google die Löschung von Links zu rechtmäßig veröffentlichten Informationen verlangen können, wenn diese bei Namenssuche erscheinen und ihre Grundrechte – insbesondere auf Datenschutz und Privatsphäre – verletzen. Dieses „Recht auf Vergessenwerden" gilt auch dann, wenn die Originalinformationen online bleiben und unabhängig von einem vorherigen Antrag an die Website selbst.

Im Fall vom 27. Oktober 2022, C-129/21[31] entschied der EuGH, dass ein Antrag eines Teilnehmers, seine personenbezogenen Daten aus öffentlich zugänglichen Teilnehmerverzeichnissen entfernen zu lassen, als Ausübung des Rechts auf Löschung gemäß Art. 17 DSGVO zu werten ist. Der Widerruf einer zuvor erteilten Einwilligung zur Veröffentlichung dieser Daten verpflichtet den Verantwortlichen zur unverzüglichen Löschung, sofern keine andere Rechtsgrundlage besteht (Art. 17 Abs. 1 lit. b DSGVO). Die Art der Umsetzung, wie etwa durch technische Maßnahmen oder die Änderung eines internen Kennungscodes, steht der rechtlichen Bewertung als „Löschung" nicht entgegen, sofern der Zugang zu den Daten faktisch beendet wird.

Im Bescheid der Datenschutzbehörde vom 13. Dezember 2018, DSB-D122.995/0003-DSB/2018[32] wurde entschieden, dass der Verantwortliche verpflichtet ist, die personenbezogenen Daten des Beschwerdeführers entweder zu löschen oder zu anonymisieren, wenn eine längere Speicherung als die gesetzlich erlaubte Frist erfolgt ist. Die DSB betont, dass die Anonymisierung als Löschmethode akzeptiert wird, solange der Personenbezug nicht ohne unverhältnismäßigen Aufwand wiederhergestellt werden kann. Die Einhaltung der Speicherfristen und die unverzügliche Umsetzung der Löschung oder Anonymisierung innerhalb von zwei Wochen wurden besonders hervorgehoben.

Im Urteil T-557/20[33] des EuGH wird die Pseudonymisierung, welche bisher als Datenschutzmaßnahme, jedoch nicht als Ausnahme von der

30 *Google Spain SL und Google Inc gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González*, No. Rechtssache C-131/12.

31 EuGH Rechtssache C-129/21, *Proximus NV gegen Gegevensbeschermingsautoriteit*.

32 Datenschutzbehörde 13.12.2018, DSB-D122.995/0003-DSB/2018, *DSB-D122.995/0003-DSB/2018*.

33 EuGH Rechtssache T-557/20, *Einheitlicher Abwicklungsausschuss gegen Europäischer Datenschutzbeauftragter*.

DSGVO galt, relativiert. Bisher waren lediglich anonyme Daten von der DSGVO ausgenommen und die Lehrmeinung, ob ein relativistischer Ansatz oder ein absoluter Ansatz bei der Pseudonymisierung anzuwenden ist, unklar[34]. Der relativistische Ansatz behauptet, dass es bei der Beurteilung des Personenzuges von vermeintlich personenbezogenen Daten für eine Partei ausreiche, die durch diese Partei zugreifbaren Daten in Betracht zu ziehen, im Gegensatz zum absoluten Ansatz, bei dem alle generell verfügbaren, also auch jene Daten bei Dritten, in Betracht gezogen werden müssen. Das Urteil T-557/20 stützt sich auf ein Urteil von 2016 C-582/14[35], in welchem IP-Adressen als personenbezogenes Datum angesehen wurden. Dort wurde aber auch festgehalten, dass die Möglichkeit bestände, dass der Verantwortliche legalen Zugriff auf die anonymisierenden Daten hätte, nämlich die Zuordnung der dynamischen IP-Adresse zu einer natürlichen Person bzw. deren Haushalt. Oft wird dieses Urteil missverstanden und eben IP-Adressen als generell personenbezogen interpretiert, also faktisch das Gegenteil, nämlich der absolute Ansatz, statt des ebendort beschriebenen relativistischen Ansatzes. Im vorliegenden aktuelleren Urteil aus 2023 T-557/20[36] wurde die damals fälschlicherweise als absoluter Ansatz interpretierte Entscheidung nun eindeutig klargestellt: Die EDSB muss, um festzustellen, ob es sich um personenbezogene Daten handelt, die Überprüfung vornehmen, ob das Unternehmen, dem die Daten zur Verfügung gestellt wurden, rechtlich befugt war, auf zusätzliche Informationen zuzugreifen, die für die Rückidentifizierung der betroffenen Personen erforderlich sind und ob dieser Zugriff auch tatsächlich durchführbar war. Daraus kann geschlossen werden, dass ein pseudonymisiertes Datum nur dann personenbezogen ist, wenn der Verantwortliche den Betroffenen rückidentifizieren könnte.

Das Urteil C-340/21[37] des EuGH erörtert aber dieses Risiko und die Fragestellung der Beweislast und Dokumentationspflicht von Unternehmen im Zusammenhang mit ihren Cybersicherheitsmaßnahmen im Kontext des Datenschutzes. Insbesondere wird betont, dass gemäß Art. 82 Abs. 1 der bloße Umstand, dass eine betroffene Person infolge eines Verstoßes gegen diese Verordnung befürchtet, dass ihre personenbezogenen Daten

34 *Piska/Bierbauer* in Blockchain Rules, Rn. 7.4.
35 EuGH Rechtssache C-582/14, *Patrick Breyer gegen Bundesrepublik Deutschland*.
36 EuGH Rechtssache T-557/20, *Einheitlicher Abwicklungsausschuss gegen Europäischer Datenschutzbeauftragter*.
37 Europäischer Gerichtshof Rechtssache C-340/21, *VB gegen Natsionalna agentsia za prihodite*.

durch Dritte missbräuchlich verwendet werden könnten, einen immateriellen Schaden im Sinne dieser Bestimmung darstellen kann. Damit wird die Befürchtung, welche unter Aussetzung des Risikos einhergeht, als Schaden anerkannt. Das in dem Urteil beschriebene Risiko ist wohlgemerkt nicht aus einem Löschvorgang herleitbar, sondern beruht auf einer unbefugten Offenlegung nach einem Cyberangriff. Dennoch ist das sichere Löschen eine Maßnahme zur dort verletzten Vertraulichkeit (Art. 5 Abs. 1 DSGVO), weil etwaige unbefugte nach einem unsicheren Löschen Zugriff auf die Daten erhalten könnten, ähnlich der beschriebenen unbefugten Offenlegung.

Das Urteil C-687/21[38] des EuGH befasst sich mit der Frage, ob der Verantwortliche für die Verarbeitung von Gesundheitsdaten gemäß Art. 9 Abs. 2 lit. h dazu verpflichtet ist, sicherzustellen, dass kein Kollege Zugang zu diesen Daten hat, also Vertraulichkeit herzustellen. Der EuGH entschied, dass eine solche Pflicht nicht unmittelbar aus den genannten Bestimmungen hervorgeht. Jedoch könnte ein Mitgliedstaat gemäß Art. 9 Abs. 4 eine solche Regelung erlassen oder der Verantwortliche könnte gemäß den Grundsätzen der Integrität und Vertraulichkeit in Art. 5 Abs. 1 lit. f und Art. 32 Abs. 1 lit. a und b dazu verpflichtet sein.

Abschließend lässt sich feststellen, dass die Entscheidungen des EuGH, OGH und der DSB sowohl vor als auch nach Einführung der DSGVO einen signifikanten Einfluss auf die Interpretation und Anwendung des Datenschutzrechts hatten. Die frühen Entscheidungen des OGH, wie das Urteil 6Ob41/10p aus 2010 und 6Ob107/12x aus 2012, legten den Fokus auf die Notwendigkeit der physischen Löschung von Daten, um rechtlichen Anforderungen zu genügen.

Die jüngeren Entscheidungen des EuGH, wie T-557/20 und C-582/14, zeichnen jedoch ein komplexeres Bild. Während der Fall C-582/14 die Möglichkeit der Behandlung von IP-Adressen als personenbezogene Daten thematisiert, widmet sich der Fall T-557/20 der Anwendung der Pseudonymisierung und relativiert damit vorherige, restriktive Ansätze. Diese Urteile legen nahe, dass sich die Rechtsprechung von einer strikten, klaren Linie hin zu einer differenzierteren Betrachtung bewegt. Zwar ermöglicht dies eine präzisere Anpassung an die technischen Realitäten, jedoch resultieren daraus auch Unsicherheiten.

38 EuGH Rechtssache C-687/21, *BL gegen MediaMarktSaturn Hagen-Iserlohn GmbH*.

D. Interpretation auf Basis des Normzwecks

Die teleologische Extension des Begriffs „Löschen" im Kontext der DSGVO und des DSG ist von grundlegender Bedeutung für die Auslegung und Umsetzung dieser Normen. Die DSGVO und das DSG zielen darauf ab, den Schutz personenbezogener Daten zu gewährleisten und das Recht auf Privatsphäre zu schützen. Gemäß der Rechtsprechung des Europäischen Gerichtshofs (EuGH) konstituiert das „Recht auf Vergessenwerden" eine zentrale Komponente des Datenschutzes.

Grundsätze und Prinzipien der DSGVO umfassen nach Art. 5 die Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie Rechenschaftspflicht. Diese Maßnahmen dienen dazu, dass die betroffene Person Risiken einschätzen und diese selbst beeinflussen kann. Der risikobasierte Ansatz zieht sich durch die gesamte DSGVO, und ist speziell bei der Bewertung von technisch organisatorischen Maßnahmen und Datenschutz-Folgenabschätzungen[39] zu erkennen. Artikel 25 der DSGVO führt das Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen ein, das darauf abzielt, Risiken für die Rechte und Freiheiten der betroffenen Personen durch geeignete technische und organisatorische Maßnahmen zu minimieren. Die Risiken für die betroffene Person sind bei der Verarbeitung personenbezogener Daten erheblich. Diese können Identitätsdiebstahl, Diskriminierung oder unberechtigte Profilbildung umfassen, wobei letztere eine Interessenabwägung benötigen[40]. Die vollständige, unwiderrufliche Löschung der Daten reduziert dieses Risiko effektiv auf null, indem sie sicherstellt, dass die Daten nicht wiederhergestellt oder für unzulässige Zwecke verwendet werden können. Jedoch berücksichtigt die DSGVO auch die Perspektive der Verantwortlichen und Auftragsverarbeiter. Es wird anerkannt, dass die Umsetzung von technisch organisatorischen Maßnahmen Ressourcen und Aufwendungen bedürfen, die bei der Auswahl der Maßnahmen Berücksichtigung finden dürfen. Das Telos der DSGVO zeigt deutlich, dass der Aufwand für die Risikobewältigung in einem angemessenen Verhältnis zu dem Risiko für die Betroffenen stehen muss[41]. Dies bedeutet, dass eine Risiko- und Aufwandsabschätzung unerlässlich ist, um

39 DSGVO, ErwG. 84.
40 *Albrecht* in Datenschutzrecht: DSGVO mit BDSG, Art. 6 Rz. 105-115.
41 DSGVO, ErwG. 84.

eine proportionale und effektive Umsetzung der Datenschutzmaßnahmen zu gewährleisten. Die Verantwortlichen sind verpflichtet, eine Risikoanalyse durchzuführen, um die potenziellen Auswirkungen der Datenverarbeitung auf die Betroffenen zu bewerten und entsprechende Maßnahmen zur Risikominderung zu ergreifen. Diese Maßnahmen sollten sowohl wirksam als auch verhältnismäßig sein, um den Aufwand der Verantwortlichen zu minimieren, ohne die Sicherheit und den Schutz der personenbezogenen Daten zu gefährden. Diese Balance zwischen Aufwand und Risikoreduzierung ist ein zentraler Bestandteil des Datenschutzkonzepts der DSGVO und spiegelt den pragmatischen Ansatz wider, den die Verordnung verfolgt.

Ein praxisnaher Ansatz zur Risiko- und Aufwandsabschätzung umfasst die Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung sowie der unterschiedlichen Risiken für die Rechte und Freiheiten natürlicher Personen. Auf dieser Grundlage können Verantwortliche und Auftragsverarbeiter Maßnahmen ergreifen, die nicht nur den gesetzlichen Anforderungen entsprechen, sondern auch praktikabel und effizient in der Umsetzung sind.

Diese Prinzipien der DSGVO bilden die Grundlage für die Auslegung des Begriffs „Löschen". Zur Abgrenzung des tatsächlich vereinbaren Risikos hilft die Einordnung des Löschens als äußerste Reduktion der Vereinbarkeit der Daten. Im Spektrum dieser Betrachtung stehen die in der DSGVO verwendeten Begriffe Anonymisierung, Pseudonymisierung und indirekt- und direkt personenbezogene Daten (siehe Abbildung 2).

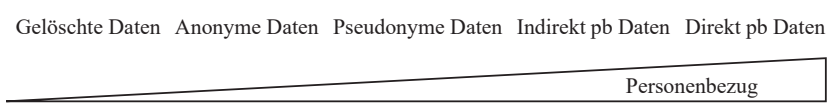

Abbildung 2 – Grade des Personenbezugs von Daten anhand DSGVO-Terminologie

Nahe zur Löschung, im Sinne des Grades des Personenbezuges, steht die Anonymisierung. Dieser Prozess, gemäß Erwägungsgrund 26 DSGVO, soll sicherstellen, dass die betroffene Person nicht identifiziert werden kann. Bei der Anonymisierung werden personenbezogene Daten so verändert, dass sie nicht mehr einer identifizierbaren natürlichen Person zugeordnet

werden können[42]. Dadurch wird ein noch hohes Maß an Datenschutz gewährleistet.

Die daraus resultierenden anonymisierten Daten unterliegen auch nicht mehr der DSGVO[43]. Dabei ist jedoch nicht jedes technische Verfahren gleich zu bewerten. Voigt und Von dem Bussche[44] unterscheiden in Referenz auf WP 216 zwei Kategorien von Anonymisierungen: Randomisierung und Verallgemeinerung. Die Randomisierung ist ein Verfahren, das die Präzision der Daten verändert, um die Reidentifizierbarkeit der betroffenen Person auszuschließen. Gemäß der vorliegenden Literatur wird unter dem Begriff der „Verallgemeinerung" die Modifikation der Merkmale von Daten verstanden, die durch eine Anpassung des Bezugspunkts oder der Granularität erfolgt. Zudem wird korrekterweise festgestellt, dass nicht jede Anonymisierungstechnik den gleichen Grad an Personenbezug entfernt. Es wird empfohlen, eine Anonymisierung anhand des Risikos zu wählen.

Im Vergleich dazu ist die Pseudonymisierung gemäß Art. 4 Abs. 5 eine Methode, bei der personenbezogene Daten ohne Zuhilfenahme zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, jedoch immer noch einem Risiko der Reidentifikation unterliegen können, wenn diese zusätzlichen Informationen zugänglich sind[45]. Pseudonymisierung wird zwar als technische und organisatorische Maßnahme (TOM) angesehen, die das Risiko für die betroffene Person reduziert, jedoch fallen die resultierenden Daten dennoch unter die DSGVO[46].

Der relativistische Ansatz (wie in den Urteilen T-557/20 und C-582/14 beschrieben), welcher davon ausgeht, dass es ausreiche, dass pseudonyme Daten aus der Sicht einer Partei anonym sein können, ohne dabei die Daten von anderen zu berücksichtigen, und damit das Risiko für den Betroffenen als vernachlässigbar bewertet, solange keine direkte Verbindung besteht, wird in der Diskussion näher behandelt.

42 *EDPB*, Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen Leitlinien 4/2019 zu Artikel 25, Rn. 26.
43 DSGVO, ErwG. 26.
44 *Voigt/Von Dem Bussche*, EU-Datenschutz-Grundverordnung (DSGVO), S. 16.
45 *Kühling ea*, Datenschutz-Grundverordnung, BDSG4. Auflage.
46 DSGVO, ErwG. 28.

E. Historische Analyse

Die Analyse der Änderungen im § 3 des Datenschutzgesetzes 1978 (DSG1978) zwischen den Versionen von 1980-1987[47] und 1987-1999[48] offenbart eine Erweiterung und Präzisierung der Methoden zum Löschen von Daten. In der Fassung von 1980 definiert das Gesetz das Löschen von Daten als „das Unkenntlichmachen von erfaßten oder gespeicherten Daten ohne die Möglichkeit ihrer Rekonstruktion“ [49]. Diese Definition konzentriert sich ausschließlich auf das physische Löschen, ohne spezifische Techniken zu differenzieren oder das logische Löschen zu adressieren.

Die Version von 1987 hingegen führt eine explizite Unterscheidung zwischen physischem und logischem Löschen ein. Das physische Löschen wird als „Unkenntlichmachen von Daten in der Weise, daß eine Rekonstruktion nicht möglich ist“[50] beschrieben, während das logische Löschen als „die Verhinderung des Zugriffs auf Daten durch programmtechnische Maßnahmen“[51] definiert wird (§ 3, DSG1978 Fassung 1987). Diese Differenzierung reflektiert eine Anpassung an technologische Entwicklungen und die wachsende Bedeutung von Software und digitalen Datenspeichern im Vergleich zu rein physischen Speichermedien.

Die differenzierte Betrachtung der Löschmethoden ermöglicht eine umfassendere und flexiblere Regulierung des Datenschutzes, die sowohl physische als auch digitale Realitäten abdeckt. Dieser Wandel in der Gesetzgebung kann als Reaktion auf die zunehmende Verbreitung von Computertechnologie und die Entwicklung komplexer Datenverarbeitungssysteme interpretiert werden, welche neue Risiken und Potenziale für Datenschutzverletzungen bergen.

Die im Datenschutzgesetz 1978, speziell in der Version von 1987, angeführten Bestimmungen zu den Löschmethoden von Daten, verdeutlichen eine klare und bewusste Unterscheidung zwischen physischer und logischer Löschung. Der Paragraph § 27 Z 2 konkretisiert diese Unterscheidung und stellt zudem sicher, dass die logische Löschung nur als vorübergehende

47 Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz - DSG1978), Fassung von 1980 01.01.1980.
48 Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz - DSG1978), Fassung von 1987 01.07.1987.
49 Datenschutzgesetz – DSG1978 (1980), § 3.
50 Datenschutzgesetz – DSG1978 (1987), § 3.
51 ebd, § 3.

Maßnahme dient, bis die physische Löschung unter wirtschaftlich vertretbaren Bedingungen umgesetzt werden kann.

Die in § 3 dargelegten Definitionen sowie die in § 27 Z 2 enthaltenen weiterführenden Regelungen verdeutlichen, dass der Gesetzgeber beide Löschmethoden als eigenständige und signifikante Prozesse im Kontext des Datenschutzes erachtet. Die physische Löschung wird als endgültige Maßnahme zur Datenvernichtung verstanden, bei der die Daten unwiederbringlich entfernt werden. Die logische Löschung wird als eine vorübergehende Einschränkung des Zugriffs auf die Daten definiert, bis die Bedingungen für eine physische Löschung gegeben sind.

Die temporäre Natur der logischen Löschung wird in § 27 Z 2 explizit betont, indem klargestellt wird, dass diese Methode nur bis zum nächstmöglichen, wirtschaftlich gerechtfertigten Zeitpunkt zur physischen Löschung angewendet werden darf. Diese Haltung reflektiert die Auffassung, dass die logische Löschung zwar als eine effektive Sofortmaßnahme zur Gewährleistung der Privatsphäre und des Datenschutzes erachtet wird, jedoch nicht als dauerhafte Lösung betrachtet wird. Der Gesetzgeber verdeutlicht mit dieser Regelung sein Ziel, einen dauerhaften Schutz personenbezogener Daten zu gewährleisten, der nur durch die irreversible physische Löschung der Daten erreicht werden kann.

Zusammenfassend lässt sich konstatieren, dass durch die Regelungen des DSG 1987 und insbesondere durch die spezifischen Vorgaben des § 27 Z 2 eine deutliche Unterscheidung und Hierarchisierung der Löschmethoden erfolgt. Die vorliegende Vorgehensweise berücksichtigt sowohl die technologische Entwicklung als auch die ökonomische Realität. Zudem wird ein hohes Maß an Datenschutz gewährleistet, da die logische Löschung lediglich eine temporäre Maßnahme darstellt, die bis zur Umsetzung der physischen Löschung dient.

F. Zwischenfazit

In der vorliegenden Analyse des Datenschutzes unter besonderer Berücksichtigung der Löschung personenbezogener Daten wurden verschiedenste Aspekte und deren Auswirkungen im Kontext der DSGVO und des österreichischen DSG beleuchtet.

Die Analyse der Rechtslage zur Löschung personenbezogener Daten im Lichte der DSGVO und des österreichischen DSG zeigt ein differenziertes Bild, das durch ein Spannungsverhältnis zwischen technischer Rea-

lität, rechtlicher Auslegung und normativer Offenheit geprägt ist. Eine Legaldefinition des Begriffs „Löschen" ist weder im Unionsrecht noch im nationalen Datenschutzgesetz enthalten. Diese Unbestimmtheit ist kein gesetzgeberisches Versehen, sondern Ausdruck eines bewusst gewählten Gestaltungsfreiraums für die Verantwortlichen. Der Begriff wird funktional interpretiert und ermöglicht eine an den spezifischen Gegebenheiten des Einzelfalls orientierte Auswahl geeigneter Maßnahmen, vorausgesetzt, diese genügen den datenschutzrechtlichen Zielvorgaben. Der rechtliche Rahmen wird durch die Grundsätze der Speicherbegrenzung (Art. 5 Abs. 1), der Rechenschaftspflicht (Art. 5 Abs. 2), der technischen und organisatorischen Sicherheit (Art. 32) sowie der Technikgestaltung (Art. 25) definiert.

Innerhalb dieses Rahmens ist eine Bandbreite zulässiger Löschformen anerkannt: von der physischen Datenvernichtung über softwarebasierte logische Löschung bis hin zur Anonymisierung. Dabei ist von entscheidender Relevanz, ob die Maßnahme tatsächlich und dauerhaft zur Beendigung der Verfügbarkeit personenbezogener Daten führt. Die historische Entwicklung, insbesondere die Differenzierung zwischen physischem und logischem Löschen im DSG 1987, unterstreicht, dass der österreichische Gesetzgeber bereits früh ein abgestuftes System zulässiger Löschmaßnahmen etabliert hat, wobei die logische Löschung ausdrücklich nur als temporäre Maßnahme anerkannt wurde. Die vor Inkrafttreten der DSGVO getroffenen Entscheidungen des OGH betonten daher konsequent die Notwendigkeit der physischen Unkenntlichmachung. Erst mit der Rechtsprechung des Europäischen Gerichtshofs, insbesondere der Sache T-557/20, wurde ein flexiblerer Zugriff eröffnet. Eine wirksame Anonymisierung oder auch eine risikoadjustierte Pseudonymisierung können in bestimmten Konstellationen als „Löschung" im Sinne der DSGVO angesehen werden, sofern das Risiko der Reidentifikation für den konkreten Verantwortlichen gegen null tendiert.

Diese Entwicklung darf jedoch nicht als Beliebigkeit missverstanden werden. Der weite Begriff des Löschens ist durch das Zusammenspiel von Risikoorientierung, Stand der Technik und Verhältnismäßigkeit begrenzt. Ein rechtskonformes Löschkonzept hat die Aufgabe, diesen Rahmen zu dokumentieren und eine Überprüfbarkeit zu gewährleisten. Die DSGVO verlangt keine absolute Irreversibilität, verlangt jedoch effektive Maßnahmen, die im Lichte der konkreten Gefährdungssituation angemessen und durchsetzbar sind. Die zulässigen Methoden der Datenlöschung umfassen demnach die physische Vernichtung als Goldstandard, restriktive logische Zugriffsbeschränkungen sowie die Anonymisierung. Die Auswahl der Me-

thode ist dabei abhängig von Zweck, Risiko, Umsetzbarkeit und dem jeweiligen Stand der Technik. Diese abgestufte Struktur ist Ausdruck eines modernen, technologieoffenen Datenschutzverständnisses, das weder durch formale Definitionen überreguliert noch durch vollständige Vagheit unterminiert wird. Stattdessen wird dem Verantwortlichen ein normativ gerahmter, aber technisch adaptiver Handlungsspielraum eingeräumt. Dies gewährleistet, dass sowohl dem Schutzziel der DSGVO als auch den realen Verarbeitungsbedingungen Genüge getan wird. Eine potenzielle Weiterentwicklung im Sinne der DSGVO sowie die Abgrenzung zur Überregulierung werden am Ende dieser Arbeit diskutiert.

III. Technische Analyse

Bei der sicheren Datenlöschung spielen technische Standards eine entscheidende Rolle, um sicherzustellen, dass Daten vollständig und irreversibel entfernt werden. Technische Standards erlauben eine einheitliche, von Standardisierungsinstituten oder Behörden verifizierte Methode. Die folgenden Abschnitte beschreiben technische Mechanismen Daten zu löschen.

A. Löschen durch das Betriebssystem

Ein Betriebssystem ist eine spezielle Software, die eine Abstraktionsschicht zwischen Hardware und Software bildet. Dadurch wird die eigenständige Implementierung grundlegender Funktionen sowie das Löschen obsolet. Die Implementierung des Löschvorgangs kann je nach Hardwarekonfiguration variieren. Es ist evident, dass jedes Betriebssystem eigene, spezifische Softwarelösungen aufweist, um Daten auf einer Hardware zu lagern und zu organisieren. Die gegenwärtig vorherrschende Form der Datenorganisation erfolgt in der Regel in Dateien. Dateien sind als abgeschlossene Daten mit Metainformationen definiert. Zu diesen Metainformationen zählen beispielsweise der Dateiname, das Erstellungsdatum oder das Format der Datei. Die vorliegende Untersuchung kommt zu dem Schluss, dass die gängigste Art der Organisation in hierarchischen Ordnerstrukturen besteht. Um diese abzubilden, bedient sich das Betriebssystem einer Software, nämlich dem Dateisystem. Im Grunde hilft das Dateisystem dem Benutzer und Programmen gleichermaßen Dateien mit einer Adresse, im Falle von

hierarchischen Ordnerstrukturen werden diese Pfade genannt, anzulegen, zu verändern, zu lesen oder zu löschen[52]. Dabei spielt die zuvor erwähnte Abbildung dieser Pfade auf Hardwareebene eine wichtige Rolle. So werden Daten auf einer Compact Disk (CD) anders abgelegt als auf einer Solid State Disc (SSD).

Die Löschmechanismen auf Betriebssystemebene sind also je Dateisystem unterschiedlich. Daher werden in den folgenden Unterabschnitten die drei gängigsten Dateisysteme und deren Löschmechanismen betrachtet.

1. NTFS

Das New Technology File System (NTFS) findet vornehmlich in Windows-basierten Betriebssystemen Anwendung und ist aufgrund seiner erweiterten Funktionalitäten und Stabilität weit verbreitet. Die Anwendung findet sowohl in Unternehmensservern als auch in herkömmlichen Windows-Workstations Verwendung.

Grundlegend arbeitet NTFS mit einer Master File Table (MFT), in der jede Datei und jedes Verzeichnis durch eine eindeutige Datei-ID und Metadaten beschrieben wird. Diese Metadaten umfassen Informationen wie Dateinamen, Größe, Erstellungsdatum und Dateiattribute[53]. NTFS unterstützt auch Journaling, das Änderungen an Dateien und Verzeichnissen protokolliert, um die Datenintegrität zu gewährleisten und eine schnelle Wiederherstellung nach einem Systemausfall zu ermöglichen. Des Weiteren ermöglicht NTFS Dateikomprimierung, Verschlüsselung und die Verwaltung von Zugriffsrechten. Durch die Verwendung von Clustern als Grundeinheit der Speicherung und die dynamische Zuweisung von Speicherplatz kann NTFS effizient große und kleine Dateien handhaben.

Beim Löschen einer Datei in NTFS wird der entsprechende Eintrag in der MFT als gelöscht markiert, die Datei selbst bleibt physisch auf dem Datenträger bestehen, bis sie von neuen Daten überschrieben wird. Der Speicherplatz der gelöschten Datei wird als verfügbar markiert und kann für neue Dateien genutzt werden. Um die Daten endgültig zu entfernen, muss der Speicherplatz mehrfach überschrieben oder ein spezielles Löschprogramm verwendet werden, das eine sichere Datenvernichtung gewährleistet.

52 *Silberschatz/Galvin/Gagne*, Operating system conceptsNinth edition.
53 *Bettany/Halsey*, Windows File System Troubleshooting.

2. ext4

Das Dateisystem ext4 (Fourth Extended Filesystem) findet vornehmlich in Linux-basierten Betriebssystemen Anwendung und repräsentiert eines der am häufigsten eingesetzten Dateisysteme in der Linux-Umgebung, sowohl auf Servern als auch auf Desktop- und mobilen Geräten. Aufgrund seiner Stabilität und Effizienz findet es weite Verbreitung und wird von zahlreichen Distributionen als Standarddateisystem eingesetzt.

Ext4 arbeitet mit einem erweiterten Superblock, der grundlegende Informationen über das Dateisystem enthält, sowie mit Inodes, die Metadaten jeder Datei speichern[54]. Diese Metadaten umfassen Dateigröße, Zugriffsrechte, Zeitstempel und Zeiger auf die Datenblöcke, in denen die eigentlichen Dateiinhalte gespeichert sind. Ext4 unterstützt sowohl Extents als auch Blockgruppen, was die Verwaltung von Speicherplatz effizienter macht und die Fragmentierung reduziert. Das Dateisystem verwendet ein Journal, um Änderungen zu protokollieren und die Konsistenz des Dateisystems nach unerwarteten Ausfällen sicherzustellen. Des Weiteren bietet ext4 Unterstützung für große Dateisysteme und Dateien, verzögerte Zuordnung (Delayed Allocation) und Multiblock-Allokation, um die Schreibvorgänge zu optimieren.

Beim Löschen einer Datei in ext4 wird der entsprechende Inode als frei markiert und die Referenzen auf die zugehörigen Datenblöcke werden entfernt, wodurch der Speicherplatz freigegeben wird.

54 *Baun*, Operating Systems / Betriebssysteme.

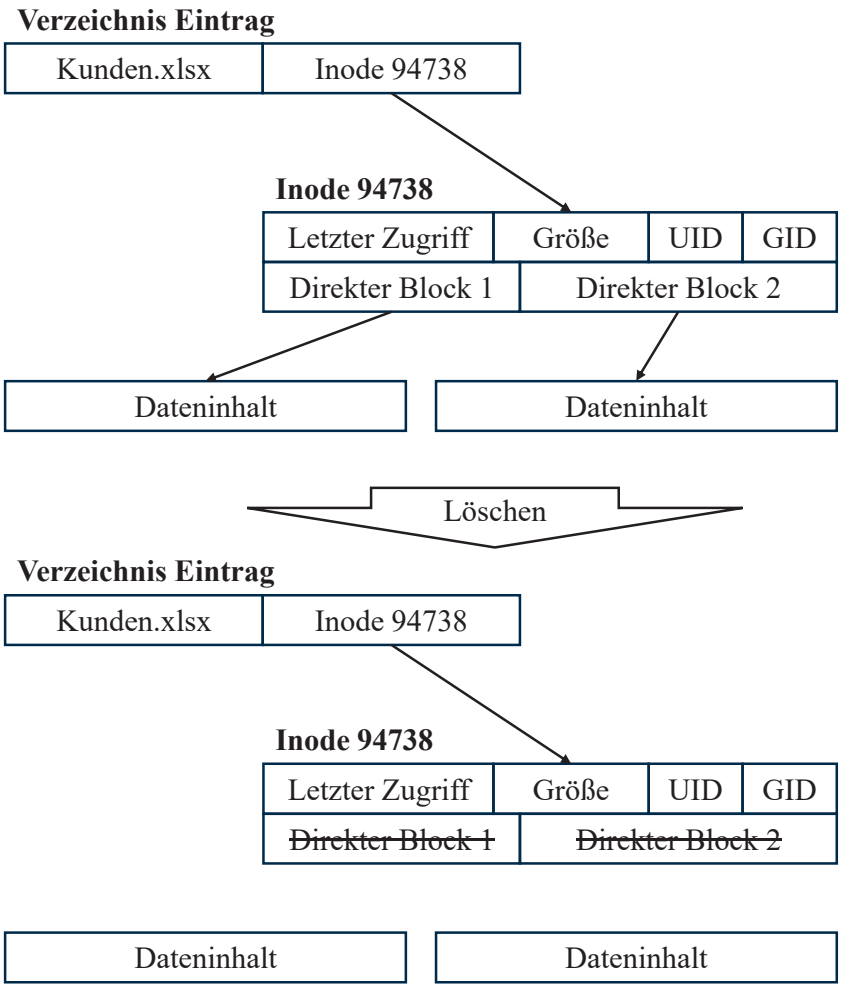

Abbildung 3 – Löschung einer Datei auf ext4 Dateisystemen

Abbildung 3 stellt die Löschung einer Datei auf einem ext4 Dateisystem dar. Eine einfache Datei („Kunden.xlsx“) besteht aus einem Verzeichniseintrag, der auf einen Inode zeigt, dieser beinhaltet die Metadaten (Zugriff, Rechte, Größe etc.), aber auch die Referenzen auf die tatsächlichen Speicherorte (zur Simplifizierung nur direkte Blöcke). Beim Löschen werden nun die Metadaten angepasst, die Referenzen gelöscht, aber die eigentlichen Daten

(Dateninhalte) nicht gelöscht. Die eigentlichen Daten bleiben auf dem Datenträger bestehen, bis sie von neuen Daten überschrieben werden. Um die Daten endgültig zu entfernen, ist es notwendig, den Speicherplatz zu überschreiben oder ein spezielles Löschprogramm zu verwenden, das eine sichere Datenvernichtung durchführt. Ein verschlüsseltes Dateisystem kann die Löschung auch sicherer machen.

3. APFS

Das Apple File System (APFS) wird hauptsächlich in Apple Produkten, wie macOS, iOS, watchOS und tvOS, verwendet und ist aufgrund seiner fortschrittlichen Funktionen und Leistung weit verbreitet. Es wurde entwickelt, um die speziellen Anforderungen moderner Applegeräte zu erfüllen und wird als Standarddateisystem genutzt.

Grundlegend basiert APFS auf einem 64-Bit-Architekturdesign und verwendet eine Kopier-auf-Schreib-Strategie (Copy-on-Write), um die Integrität von Daten bei Schreiboperationen zu gewährleisten. Es unterstützt Snapshots, die den Zustand des Dateisystems zu einem bestimmten Zeitpunkt erfassen und so eine schnelle und effiziente Datenwiederherstellung ermöglichen. Das Dateisystem ist auch für Flash-/SSD-Speicher optimiert, was zu schnellerem Zugriff und geringerer Latenz führt. APFS verwendet eine Baummodellstruktur (B-Trees) für das Management von Dateien und Metadaten, die die Effizienz bei der Datenorganisation und -suche verbessert. Zudem bietet es erweiterte Funktionen wie Verschlüsselung auf Dateiebene, effiziente Klon Erstellung und Space Sharing, wodurch mehrere Volumes denselben physischen Speicherplatz teilen können.

Beim Löschen einer Datei in APFS wird der entsprechende Verzeichniseintrag entfernt und die Speicherblöcke, die die Datei enthalten, werden als verfügbar markiert, aber die Daten selbst bleiben physisch vorhanden, bis sie überschrieben werden. APFS kann mithilfe seiner nativen Verschlüsselungsfunktionen dafür sorgen, dass gelöschte Daten schwerer wiederherstellbar sind, indem es verschlüsselte Blöcke unbrauchbar macht. Für eine endgültige Entfernung der Daten muss der Speicherplatz überschrieben oder ein spezielles Tool verwendet werden, das sichere Löschungsvorgänge durchführt.

B. NIST SP 800–88

Der Standard des US-Amerikanischen National Institute of Standards and Technology (NIST) bietet umfassende Richtlinien zur „Mediensanierung", die speziell auf die Löschung von Daten abzielen. NIST SP 800-88[55] unterscheidet zwischen drei Sanierungstypen: Löschen [„Clear"], Bereinigen [„Purge"] und Zerstören [„Destroy"]. Jede Methode ist für spezifische Szenarien und Medientypen geeignet. Beim Löschen werden Daten so überschrieben, dass sie durch Standarddateisystemmethoden nicht mehr zugänglich sind. Das Bereinigen erfolgt durch Methoden, die eine Wiederherstellung der Daten durch spezialisierte Techniken verhindern sollen. Das Zerstören von Medien führt dazu, dass eine Wiederherstellung der Daten unmöglich wird, sei es durch physikalische Zerstörung oder durch chemische Prozesse. Techniker müssen die Art der zu löschenden Daten sowie den erforderlichen Sicherheitsgrad berücksichtigen, um die geeignete Sanierungsmethode auszuwählen.

C. DoD 5220.22-M

Der Standard 5220.22-M[56] des US-Verteidigungsministeriums ist einer der bekanntesten und am häufigsten verwendeten Ansätze zur Datenlöschung. Er beschreibt ein Verfahren, bei dem Daten auf magnetischen Medien dreimal überschrieben werden. Jeder Durchgang verwendet ein anderes Muster, um alle Spuren der ursprünglichen Daten zu entfernen. Obwohl dieser Standard in einigen Kreisen als veraltet angesehen wird, bietet er immer noch eine solide Basis für die sichere Datenlöschung, besonders wenn kombinierte Überlagerungsmethoden verwendet werden. Für Techniker ist es wichtig, sich der Kritik bewusst zu sein und gegebenenfalls zusätzliche Maßnahmen zur Datensicherheit zu ergreifen.

Der Aufwand der Implementierung der DoD 5220.22-M ist zum Beispiel unter Windows mit Microsoft Sysinternals mittels SDelete[57] relativ gering. Es kann über die Microsoft Webseite gratis bezogen werden und über die

55 *National Institute of Standards and Technology*, Guidelines for Media Sanitization (SP 800-88).

56 *Department of Defense*, National Industrial Security Program Operating Manual (5220.22-M).

57 Microsoft Sysinternals, SDelete, https://learn.microsoft.com/de-de/sysinternals/downloads/sdelete

Eingabeaufforderung ausgeführt, in verschiedene Programme oder mittels Drittsoftware in das Windows Kontextmenü integriert werden, um mittels eines Rechtsklicks jede Datei sicher zu löschen.

Unter Linux kann der Befehl „scrub“[58] herangezogen werden, um sowohl DoD als auch BSI konform Dateien zu löschen.

D. ISO/IEC 27040:2024

Der ISO-Standard 27040:2024[59] konzentriert sich auf die Sicherheitsaspekte von Speichersystemen und umfasst Richtlinien für das sichere Löschen von Daten. Er bietet einen Rahmen für das Einrichten, Aufrechterhalten und Verbessern des Informationssicherheitsmanagements in Speichersystemen. Der Standard behandelt spezifische Techniken und Methoden zur Datenlöschung und betont die Bedeutung von Verfahren, die sicherstellen, dass Daten nicht wiederhergestellt werden können. Für Techniker, die mit der Speichersicherheit arbeiten, ist dieser Standard eine wertvolle Ressource, um aktuelle und effektive Praktiken zu implementieren.

Diese Standards bieten nicht nur Richtlinien für die praktische Durchführung der Datenlöschung, sondern betonen auch die Wichtigkeit einer sorgfältigen Planung und Durchführung im Prozess der Datenvernichtung, um die Sicherheit von Informationen zu gewährleisten.

E. DIN 66399

Die Deutsche Industrie Norm 66399[60] konzentriert sich auf die sichere Vernichtung von Datenträgern und legt Anforderungen an Verfahren und Maschinen zur Datenlöschung fest. Gemäß der Definition werden Schutzklassen, Sicherheitsstufen und Materialkategorien festgelegt, um den Schutzbedarf sensibler Daten strukturiert zu erfassen. Die Norm differenziert zwischen sieben Sicherheitsstufen, wobei die erste Stufe lediglich für allgemeine Informationen vorgesehen ist, während die siebte Stufe den höchsten Schutz für geheime Daten gewährleistet. Die Einteilung von Datenträgern

58 Scrub, https://linux.die.net/man/1/scrub

59 *International Organization for Standardization*, Information technology – Security techniques – Storage security (ISO/IEC 27040:2024).

60 DIN SPEC 66399-3:2013-02, Büro- und Datentechnik – Vernichten von Datenträgern, DIN SPEC 66399-3.

erfolgt in sechs Materialkategorien, darunter Papier, optische Medien und magnetische Datenträger.

Die vorliegende Norm DIN 66399 findet ausschließlich Anwendung auf die physische Vernichtung von Datenträgern. Das softwarebasierte Löschen von Daten auf Festplatten oder in Anwendungen ist hingegen nicht Gegenstand der Norm.

F. BSI Grundschutz CON.6

Das IT-Grundschutz-Konzept des Bundesamtes für Sicherheit in der Informationstechnik (BSI) stellt einen strukturierten Ansatz zur Identifizierung und Implementierung von Sicherheitsmaßnahmen in Organisationen bereit. Der BSI-Grundschutz-Baustein CON.6 „Löschen und Vernichten" umfasst Richtlinien und Verfahren für das sichere Löschen und Vernichten von Informationen auf unterschiedlichen Datenträgern. Hierzu zählen sowohl physische Medien, wie etwa Papier und Filme, als auch digitale Speichermedien, zu denen Festplatten und SSDs zählen. Das Ziel besteht darin, den Zugriff auf sensible Daten zu verhindern und die Einhaltung der Datenschutzgesetze zu gewährleisten.

Im Rahmen des BSI-Grundschutz-Bausteins CON.6 wird spezifiziert, dass nicht verschlüsselte, digitale wiederbeschreibbare Datenträger „vollständig mit einem Datenstrom aus Zufallswerten (z. Bsp. PRNG Stream) überschrieben werden"[61] müssen. Für verschlüsselte Datenträger gilt, dass sie „durch ein sicheres Löschen des Schlüssels unter Beachtung des Kryptokonzepts gelöscht werden"[62] müssen, um die Integrität der Datenlöschung zu gewährleisten.

Damit gibt die CON.6 konkrete und detaillierte Anweisungen zur sicheren und datenschutzkonformen Löschung digitaler Datenträger, um Vertraulichkeit und Integrität von Daten zu gewährleisten.

G. Verschlüsselung und Löschung des Schlüssels

Eine technisch-organisatorische Löschung kann durch die Verschlüsselung des Datensatzes oder der Datei vor der Speicherung und die separate Spei-

61 *Bundesamt für Sicherheit in der Informationstechnik*, CON.6 Löschen und Vernichten, Edition 2023.

62 ebd.

cherung des Schlüssels und anschließende Löschung des Schlüssels erreicht werden. Der Löschmechanismus, der auf der Verschlüsselung und anschließenden Löschung des Schlüssels basiert, wird in mehreren Jurisdiktionen als legal gelehrt und wird als effektive Methode zur sicheren Datenlöschung beschrieben.

Verschlüsselung und anschließende Schlüssellöschung (auch „Crypto-Shredding" genannt) ist eine Methode, um personenbezogene Daten faktisch momentan unzugänglich zu machen. Diese Methode wird oft als sicher und praktikabel angesehen, insbesondere für cloudbasierte Systeme, bei denen vollständige Kontrolle über die physische Löschung nicht möglich ist. Auch werden diese bei unveränderlichen Datenspeichern wie z.B. Blockchain Technologien angewandt.

Anderl und Schelling beschreiben in genau diesem Kontext ein Verfahren, bei dem personenbezogene Daten verschlüsselt auf einer öffentlichen Blockchain abgelegt werden und die dazugehörigen Schlüssel „off-chain", also bei dem Verantwortlichen selbst, in einer Datenbank gespeichert werden[63]. Das hätte eine „subjektiv anonymisierende Wirkung", da nur der Verantwortliche den Schlüssel kenne und die Daten verarbeiten könnte. Eine etwaige, durch die DSGVO notwendige, Löschung würde dann durch Löschen des Schlüssels passieren. Die Daten auf der Blockchain „durch Löschung des Schlüssels dauerhaft anonymisiert".

Dobrauz-Saldapenna und Rosenauer sehen im selben Blockchain Kontext die Verschlüsselung und Veröffentlichung von personenbezogenen Daten differenzierter, wenn auch nicht abschließend geklärt. Sie meinen es sei „zu prüfen, ob die Daten durch die Verschlüsselung als irreversibel anonymisiert gelten"[64], aber kommen weiters zu dem Schluss „Verschlüsselung oder Pseudonymisierung der Daten und die anschließende Vernichtung des Schlüssels."[65] seien eine Möglichkeit, um dem Recht auf Vergessenwerden nachzukommen, weil eine Entschlüsselung „technisch sehr Aufwändig", aber demnach möglich wäre. Sie sprechen dabei also das „Knacken" der Verschlüsselung an, welches meist mit „Brute Forcing", also dem Ausprobieren von allen Kombinationen bei intakten Verschlüsselungsverfahren, die korrekt implementiert wurden, gelöst wird. Dies benötigt auch die besagte Rechenleistung.

63 *Anderl/Schelling* in #Blockchain in der Rechtspraxis, S. 102.
64 *Dobrauz-Saldapenna/Rosenauer* in Datenschutz: Recht und Praxis, Rz. 17.
65 ebd, Rz. 37.

Piska und Bierbauer beschreiben ein ähnliches Verfahren „Key-Escrow", indem im Grunde auch ein Schlüssel verwendet wird, um Daten nachträglich zu anonymisieren und kommen zum Schluss, dass dies im „vollen Einklang mit den gebotenen Löschkriterien der DSGVO"[66] stehe und bereits von einigen Startups verwendet werde.

Tatsächlich werden die Daten unzugänglich gemacht. Obwohl die Methode der Schlüssellöschung viele Vorteile bietet, gibt es auch einige Herausforderungen:

Verwaltung der Verschlüsselungsschlüssel: Die Gewährleistung der Sicherheit ist dabei in hohem Maße von einer sicheren Verwaltung und Aufbewahrung der Schlüssel abhängig. Ein kompromittierter Schlüssel könnte potenziell zur Wiederherstellung der Daten führen.

Restdaten in Speichern: Nach der Löschung des Schlüssels sind die Risiken identisch mit denen bei der Löschung aller Daten, sofern diese nicht adäquat gelöscht werden. Es verbleiben Überreste, die nicht durch das einfache Löschen des Schlüssels unzugänglich gemacht werden können.

Sicherheit des Verschlüsselungsverfahrens: Es sei darauf hingewiesen, dass selbst im Falle des Nicht-Diebstahls des Schlüssels ein unsicheres Verschlüsselungsverfahren dazu führen kann, dass ein Dritter unberechtigten Zugriff auf die Daten erhält. Einerseits kann dies auf eine Sicherheitslücke im Verschlüsselungsverfahren zurückzuführen sein, andererseits auf eine unzureichende Schlüssellänge mit der Zeit. In einigen Fällen kann zudem eine bereits erwähnte „Brute-Force"-Attacke Anwendung finden. Dies kann insbesondere bei veröffentlichten oder auf einem unveränderlichen Medium gespeicherten Daten gravierende Konsequenzen nach sich ziehen, da eine nachträgliche Aktualisierung des Verschlüsselungsverfahrens bzw. der Schlüssellänge unmöglich ist.

Evidenz hierzu gibt die Technische Richtlinie (TR) des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI). Es publiziert in seiner TR-02102-1 kontinuierlich Empfehlungen zu kryptografischen Verfahren inklusive empfohlene Schlüssellängen. Ein Vergleich der Ausgabe von

66 *Piska/Bierbauer* in Blockchain Rules Rz. 7.49.

2021[67] und 2024[68] zeigt, dass bei einem der häufigsten verwendeten asymmetrischen Verschlüsselungsverfahren RSA (Rivest-Shamir-Adleman) die Schlüssellängenempfehlung von 2000 Bits Länge auf 3000 Bits Länge (also Faktor 1,5) innerhalb von nur drei Jahren erweitert wurde. Durch steigende Rechenleistung wird es daher passieren, dass gewisse Schlüssellängen nicht mehr als ausreichend angesehen werden, weil die Daten ohne viel Aufwand entschlüsselt werden können und Daten, die heute als sicher verschlüsselt galten, morgen nicht mehr sicher sind.

Zusammenfassend lässt sich festhalten, dass das Verfahren technisch-juristisch einer gewissen probabilistischen Absicherung entspricht, die nur begrenzt und unter einer (diskutablen) Wahrscheinlichkeit Gültigkeit besitzt. Aus technisch-juristischer Perspektive besteht demnach eine Verbindung der Daten (Personenbezug), die künstlich (durch Verschlüsselung) zuerst probabilistisch subjektiv und nach Löschung des Schlüssels probabilistisch objektiv getrennt wurde. Dies impliziert, dass es sich um Daten handelt, deren Verknüpfung zum gegenwärtigen Zeitpunkt nicht möglich ist. Wolff und Brink behandeln jene Daten und argumentieren die Möglichkeit eines vorbeugenden Unterlassungsanspruches, „wenn sich die rechtswidrige Datenverarbeitung hinreichend konkret anbahnt“[69]. Ob die Anbahnung hinreichend konkret ist, wird in der Diskussion behandelt.

H. Wiederherstellung von Daten

Daten, die auf Dateisystemebene gelöscht wurden, können oft durch spezielle Wiederherstellungssoftware wiederhergestellt werden, solange die Datenblöcke noch nicht überschrieben wurden. Diese Software durchsucht den Datenträger nach nicht referenzierten, aber noch vorhandenen Datenblöcken und rekonstruiert daraus die ursprünglichen Dateien. Das ist möglich, weil das Löschen in vielen Dateisystemen lediglich die Verweise auf die Daten entfernt, nicht aber die Daten selbst. Ein Expertenwissen oder ein hoher Aufwand ist dabei nicht notwendig.

67 *BSI*, Technische Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen (TR-02102-1)2021-01 S. 28.

68 *BSI*, Technische Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen (TR-02102-1)2024-01 S. 32.

69 *Wolff/Brink*, BeckOK DatenschutzR48. Edition BeckOK Datenschutzrecht, Art. 17 Rz. 77b.

Betriebssysteme wie Windows, Linux und macOS verwenden unterschiedliche Dateisysteme (NTFS, ext4, APFS) zum Löschen von Dateien, wobei die Daten häufig nur als gelöscht markiert werden und physisch auf dem Datenträger verbleiben, bis sie überschrieben werden. Spezielle Wiederherstellungssoftware kann diese Daten rekonstruieren, solange sie nicht überschrieben wurden.

Verfahren wie die oben genannten Standards des NIST, DoD, ISO oder BSI haben unterschiedliche Anwendungsgebiete im Sinne der Medien (Dokumente, Festplatten, SSD, etc.). Gemein haben sie aber, dass sie eine Reduktion des Risikos der Wiederherstellung der Daten schaffen.

I. Zwischenfazit

Die Analyse der technischen Methoden zur Datenlöschung zeigt, dass das Löschen von Daten, abhängig von den verwendeten Dateisystemen und Speichertechnologien, in den meisten Fällen nicht zu einer endgültigen und unwiederbringlichen Löschung der Daten führt. Vielmehr bleiben die Daten in den meisten Dateisystemen physisch auf dem Datenträger bestehen, bis sie von neue Daten überschrieben werden. Dies unterstreicht die Notwendigkeit, spezialisierter Löschverfahren oder Software, um die sichere und irreversible Vernichtung von Daten zu gewährleisten. Die gängigen Dateisysteme wie NTFS, ext4 und APFS markieren beim Löschen einer Datei primär die zugehörigen Metadaten als gelöscht und stellen den Speicherplatz für zukünftige Schreiboperationen zur Verfügung. Diese Vorgehensweise birgt jedoch erhebliche Risiken, da die eigentlichen Daten weiterhin auf dem Datenträger vorhanden bleiben und mit entsprechender Wiederherstellungssoftware rekonstruiert werden können. Dies ist besonders kritisch in Szenarien, in denen eine vollständige und rechtssichere Datenvernichtung erforderlich ist, um Datenschutzvorgaben und regulatorische Anforderungen zu erfüllen.

Normative Standards wie NIST SP 800–88, DoD 5220.22-M und ISO/IEC 27040:2024 bieten detaillierte Vorgaben für die sichere Löschung von Daten und betonen die Bedeutung der Auswahl geeigneter Methoden je nach Sicherheitsanforderungen und Medientyp. Während einige dieser Standards, insbesondere DoD 5220.22-M, als veraltet gelten, bleiben sie weiterhin eine Grundlage für die praktische Umsetzung sicherer Datenlöschung. Dennoch müssen Techniker die Aktualität und Relevanz dieser Normen kontinuierlich überprüfen, um sicherzustellen, dass die angewand-

ten Methoden den neuesten technologischen Entwicklungen und Bedrohungsszenarien entsprechen.

Die Verschlüsselung und anschließende Löschung des Schlüssels (Crypto-Shredding) stellt eine technisch-organisatorische Methode dar, die insbesondere in cloudbasierten und blockchainbasierten Systemen Anwendung findet. Diese Methode wird oft als sicher und praktikabel angesehen, da sie die Daten faktisch unzugänglich macht. Allerdings weist sie auch wesentliche Schwächen auf, insbesondere in Bezug auf die sichere Verwaltung der Verschlüsselungsschlüssel, die verbleibenden Restdaten auf den Speichern und die Langzeitsicherheit des Verschlüsselungsverfahrens selbst. Da die Sicherheit stark von der Stärke und Verwaltung der Schlüssel sowie der Integrität des Verschlüsselungsalgorithmus abhängt, stellt dies eine probabilistische Absicherung dar, deren langfristige Wirksamkeit unsicher ist.

Was die beschriebenen Verfahren zur Datenlöschung gemeinsam haben, ist, dass sie aus der grundlegenden Notwendigkeit entstanden sind, Daten unzugänglich zu machen. Technologische Gegebenheiten, Innovationen und veränderte Rahmenbedingungen haben zur Entwicklung und Weiterentwicklung dieser Lösungen geführt. Abhängig von der Risikobereitschaft des Anwenders können günstige und schnelle Verfahren in bestimmten Kontexten ausreichend sein. Allerdings gilt: Je kritischer oder sensibler die Daten sind, desto sicherere und umfassendere Verfahren sollten angewendet werden. Technisch gesehen, existieren diese fortschrittlichen Lösungen bereits. Ob und wie diese jedoch eingesetzt werden sollten oder müssen, wird in der abschließenden Diskussion behandelt.

V. Strukturierte Analyse

Die Ergebnisse der Analyse werden anschließend bewertet und in tabellarischer Form präsentiert, um die Ergebnisse der Analyse zu veranschaulichen. In der nachfolgenden Diskussion erfolgt eine Analyse der Klassifikation diverser Löschmethoden und Standards hinsichtlich ihrer Zuordnung zu physischen und logischen Löschverfahren (vgl. Kapitel II du III). Tabelle 1 zeigt die Ergebnisse der Analyse zwischen den technischen Löschmethoden (siehe Kapitel II) anhand der juristischen Definitionen von physischem und logischem Löschen (siehe Kapitel IIII.E).

Tabelle 2 – Ergebnisse der Analyse der technischen Löschmethoden anhand der juristischen Definitionen von physischem und logischem Löschen

	Physisches Löschen	Logisches Löschen
Löschen durch das Betriebssystem		●
NIST SP 800–88	●	●
DoD 5220.22-M	●	
ISO/IEC 27040:2024	●	
BSI Grundschutz CON.6	●	
Verschlüsselung und Löschung des Schlüssels		●

Löschen durch das Betriebssystem wird ausschließlich als logische Löschmethode klassifiziert. Diese Methode impliziert, dass die Datenverweise im Dateisystem entfernt werden, während die physischen Daten auf dem Datenträger bestehen bleiben, bis sie durch neue Daten überschrieben werden. Dies entspricht den konventionellen Funktionen moderner Betriebssysteme, die nicht unmittelbar die physikalische Zerstörung der Daten vornehmen, sondern lediglich ihre Zugänglichkeit limitieren.

Der **NIST SP 800–88** Standard ist sowohl unter physischem als auch logischem Löschen kategorisiert. Diese doppelte Zuordnung spiegelt die umfassenden Richtlinien des Standards wider, der Techniken für das Überschreiben von Daten sowie für deren physische Zerstörung umfasst. Dieser Standard bietet somit eine flexible Grundlage für die Implementierung von Datenlöschvorgängen, die sowohl die Unzugänglichkeit als auch die endgültige Zerstörung der Daten sicherstellen können.

DoD 5220.22-M wird ausschließlich als eine Methode des physischen Löschens geführt. Obwohl dieser Standard auch das Überschreiben von Daten beinhaltet, welches als logische Löschmethode betrachtet werden könnte, dominiert in der Praxis die Perzeption seiner Rolle bei der gründlichen und irreversiblen Zerstörung von Daten.

ISO/IEC 27040:2024 wird ebenfalls nur unter physischem Löschen geführt. Der Standard konzentriert sich auf die Sicherheit von Speicherdiensten und inkludiert Anleitungen sowohl für das physische als auch für das logische Löschen, jedoch mit einem starken Akzent auf die physische Vernichtung der Speichermedien.

Der **BSI Grundschutz CON.6** wird konsequent als physische Löschmethode aufgeführt. Dies reflektiert die Schwerpunktsetzung des Bausteins

auf sichere Vernichtungsprozesse, die sicherstellen, dass die Daten nicht nur unzugänglich gemacht, sondern auch physisch zerstört werden.

Schließlich wird die **Verschlüsselung und Löschung des Schlüssels** eindeutig als logische Löschmethode kategorisiert. Diese Methode macht Daten durch die Entfernung des Schlüssels unlesbar, ohne die Notwendigkeit einer physischen Zerstörung der Daten selbst, die typisch für logische Löschverfahren ist.

Diese Klassifikationen verdeutlichen die breite Palette von Löschmethoden, die in der Informationssicherheit zur Anwendung kommen, und reflektieren die Vielfalt der Ansätze zur Datenlöschung, die von rein softwarebasierten Lösungen bis hin zu physischen Vernichtungsprozessen reichen.

Die Betrachtung und tabellarische Analyse der verschiedenen technischen Löschmethoden im Kontext der gesetzlichen Vorgaben und der gesellschaftlichen Erwartungen, wie in den Kapiteln II und III dargestellt, erlauben eine systematische Evaluierung der Effektivität und Anwendbarkeit der einzelnen Verfahren. Die differenzierte Darstellung in Tabelle 1 verdeutlicht die spezifischen Stärken und Einschränkungen jeder Methode in Bezug auf physische und logische Löschprozesse sowie deren Ausrichtung auf Endgültigkeit, Sicherheit, Transparenz, Datenintegrität, Zuverlässigkeit, Schnelligkeit, einfache Durchführung, Regelkonformität, Nachvollziehbarkeit und das Fehlen einer Selbstzerstörungsfunktion. Diese strukturierte Analyse bietet nicht nur einen klaren Überblick über die vorhandenen technologischen Möglichkeiten und deren rechtliche Adäquanz, sondern legt auch den Grundstein für weiterführende Forschungen, die auf der Optimierung von Löschverfahren basieren könnten, um sowohl technologische als auch rechtliche Anforderungen effizienter zu adressieren und die Resilienz von Datenschutzmaßnahmen in einer sich ständig weiterentwickelnden digitalen Landschaft zu stärken.

VI. Diskussion

Die vorliegende Untersuchung kommt zu dem Schluss, dass sowohl die DSGVO als auch das österreichische DSG einen umfassenden, jedoch in Bezug auf den Begriff des „Löschens" unpräzisen Rechtsrahmen bieten. Eine klare Definition des Begriffs ist essenziell, insbesondere im Hinblick auf dessen praktische Umsetzung. Die fehlende klare Definition hat zur Folge, dass Unternehmen und Organisationen Unsicherheiten haben, da

unklar bleibt, welche Maßnahmen tatsächlich als „Löschen" im Sinne der Gesetzgebung zu betrachten sind. Dies erschwert nicht nur die Einhaltung der gesetzlichen Vorgaben, sondern erhöht auch das Risiko von Fehlinterpretationen und möglichen Sanktionen. Zudem können unterschiedliche Interpretationen dazu führen, dass Unternehmen unterschiedliche Lösungsansätze verfolgen. Dies kann zu einer uneinheitlichen Umsetzung und potenziellen Nachteilen im Wettbewerb führen. Darüber hinaus erschwert die unpräzise Definition die Entwicklung standardisierter technischer Lösungen, was insbesondere bei neuen Technologien wie der Blockchain problematisch ist, da dort eine physische Löschung oft nicht möglich ist. Eine präzise und konsistente Definition wäre daher von essenzieller Bedeutung, um Rechtssicherheit zu gewährleisten und eine effektive und konsistente Umsetzung der gesetzlichen Anforderungen zu gewährleisten. Die DSGVO normiert mit dem Recht auf Löschung nach Art. 17 eine bußgeldbewehrte Pflicht, unterlässt es jedoch, den Begriff „Löschen" inhaltlich zu konkretisieren. Angesichts der in Art. 83 ausgesprochenen Sanktionsandrohung ist eine eindeutige, normative Festlegung erforderlich. Diese Festlegung ermöglicht es dem Adressatenkreis, das gesetzlich Gebotene zu erkennen und rechtssicher umzusetzen. Die fehlende Differenzierung zwischen physischem und logischem Löschen eröffnet einen weiten Interpretationsspielraum, der mit rechtsstaatlichen Anforderungen an Normklarheit und Rechtsfolgensicherheit unvereinbar ist.

Die teleologische Auslegung des Begriffs „Löschen" ist von zentraler Bedeutung, um den gesetzgeberischen Willen zu erfassen und die Ziele des Datenschutzes zu erreichen. Die Analyse hat ergeben, dass eine einheitliche Auslegung im Rahmen der DSGVO nicht vorliegt. Die mangelnde Klarheit bezüglich der Art der Löschung (logisch vs. physisch) kann in der Praxis zu Unsicherheiten führen. In der digitalen Welt, in der Daten bei verschiedenen Verantwortlichen vorliegen oder als unveränderlich gelten (z. B. Blockchain), besteht ein Bedarf an klareren Regelungen.

Die Entscheidungen des EuGH, OGH und der österreichischen DSB zeigen eine gewisse **Uneinheitlichkeit in der Bewertung von Löschmethoden**. Diese Unterschiede führen zu Unsicherheiten bei der praktischen Anwendung und Interpretation des Löschrechts.

Die technische Untersuchung zeigt, dass die Anwendung unzureichender Löschmethoden, insbesondere der bloßen logischen Löschung, potenziell schwerwiegende Risiken für die betroffenen Personen birgt. Dies verdeutlicht die Relevanz eines risikobasierten Ansatzes. Die fortschreitende technologische Entwicklung bedingt eine kontinuierliche Anpassung der

rechtlichen Rahmenbedingungen, um den effektiven Schutz personenbezogener Daten zu gewährleisten. Dies ist insbesondere im Kontext der Löschung und Pseudonymisierung von Daten von signifikanter Relevanz. Die vorliegende Arbeit kommt zu dem Schluss, dass die Verschlüsselung und Löschung des Schlüssels als eine juristisch akzeptierte Alternative zur physischen Löschung zu betrachten ist. Allerdings sind damit auch Herausforderungen und Risiken verbunden.

Gemäß der DSGVO ist ein dem Aufwand des Verantwortlichen angemessenes Verhältnis zu dem Risiko des Betroffenen erforderlich, auch in Bezug auf die Implementierung von Löschmethoden. Dies stellt die Verantwortlichen vor Herausforderungen, erfordert jedoch auch eine präzise gesetzliche Regelung.

Das Kernproblem besteht darin, dass Verantwortliche nicht nur die Verarbeitungstätigkeiten, sondern auch die damit verbundenen Risiken im Kontext der Datenlöschung vollumfänglich verstehen und darauf basierend eine geeignete Lösung auswählen müssen, sei es durch technische Systeme oder organisatorische Maßnahmen. Je weniger technisch versiert der Verantwortliche ist, desto mehr ist er auf validierte Standards und standardisierte Systeme angewiesen, die, wie in Kapitel III dargelegt, bereits existieren.

Die gegenwärtige Interpretation des Begriffs „Löschen" durch die DSB und den EuGH lässt jedoch Spielraum für Verantwortliche, die, obwohl sie das Risiko der Datenverarbeitung durchaus verstehen, versuchen, den Aufwand zu minimieren. Dies eröffnet die Möglichkeit, den Begriff des Löschens im Sinne einer beneficium sibi tribuendi zulasten der Betroffenen möglichst weit zu fassen. Hierdurch etablieren große Unternehmen Quasi-Standards, denen kleinere Unternehmen aus Kostengründen folgen, da individuelle Implementierungen wirtschaftlich kaum tragbar sind. Dies führt zu einer de facto Harmonisierung durch wirtschaftliche Macht, anstatt durch klare gesetzliche Vorgaben, was den Schutzzweck der DSGVO zu unterlaufen droht. Derzeitige Unsicherheiten über die datenschutzrechtliche Zulässigkeit bestimmter Löschmethoden führen zu einer strukturellen Ungleichheit zwischen datenverarbeitenden Stellen. Große Unternehmen sind regelmäßig in der Lage, eigene technische Standards zu etablieren und durchzusetzen, während kleinere Verantwortliche sich mangels Ressourcen an diese faktischen Quasi-Normen anlehnen müssen. Eine verbindliche und differenzierende Definition der Löschmethoden würde nicht nur Rechtssicherheit schaffen, sondern auch Chancengleichheit im Wettbewerb und gleichmäßige Rechtsanwendung gewährleisten.

Die Ergebnisse zeigen, dass eine **gesetzliche Präzisierung des Begriffs „Löschen" erforderlich** ist, um den praktischen Anforderungen gerecht zu werden. Eine klare Unterscheidung zwischen logischer und physischer Löschung wäre notwendig. Die Rechtsprechung hat bereits wichtige Impulse zur Auslegung des Löschrechts gegeben, doch bleibt eine endgültige Klärung aus. Die Arbeit legt nahe, dass die Zukunft des Löschrechts von einer stärkeren Differenzierung der Löschmethoden und einer präziseren gesetzlichen Regelung abhängen wird. Eine Anpassung der Gesetzgebung an die technologische Realität ist unerlässlich. Die Gerichte haben dabei sowohl physische Löschung als auch Anonymisierung als wirksame Methoden anerkannt; logische Löschung ist uneinheitlich ausgelegt.

Im Rahmen der Implementierung der Löschung ist es unerlässlich, die Vorgaben des Standes der Technik zu berücksichtigen (Art. 32). In vorliegender Arbeit werden technische Standards erörtert, darunter auch der BSI-Grundschutz CON.6. Es wird explizit darauf hingewiesen, dass dieser kontinuierlich aktualisiert wird und daher wird empfohlen, seine Implementierung zu prüfen.

Die Abwägung der Risiken und Implementierungskosten des Stands der Technik darf zur Auswahl der Technik herangezogen werden. Jedoch kann mit der Implementierung einfacher Mittel (wie in Abschnitt III.C dargestellt) eine Lösung zum sicheren Löschen umgesetzt werden, die sowohl von Benutzern als auch Programmen verwendet werden kann.

Art. 32 Abs. 1 lit. d fordert auch eine regelmäßige Überprüfung dieser Maßnahmen. Sollten also Verfahren eingesetzt werden, die technisch nur kurzlebig sind, so müssen diese spätestens bei der nächsten Prüfung gewechselt werden. Somit ist nicht nur aus technisch-juristischer Sicht, sondern auch aus wirtschaftlicher Sicht eine weitsichtige Auswahl der Verfahren sinnvoll.

Die Ergebnisse der Arbeit legen nahe, dass **logische Löschung aus technischer Sicht eine kurzlebige und stark risikobehaftete Methode ist** und daher **im Falle der Löschung von personenbezogenen Daten ein Risiko für den Betroffenen darstellt und sollte daher nicht als Löschen im Sinne der DSGVO ausgelegt werden**. Löschverfahren sollten mit dem Stand der Technik vereinbar sein, und in der bereits zum Einsatz des Verfahrens absehbaren Zukunft nicht zu einer Deanonymisierung führen.

Des Weiteren liegt nahe, dass ein risikobasierter Ansatz erforderlich ist, um zu definieren, zu welchem Zeitpunkt und auf welche Art und Weise die Löschung von Daten erfolgen sollte. Diese Vorgehensweise steht im Einklang mit den Grundprinzipien der DSGVO, welche eine Abwägung

zwischen Risiko und Aufwand fordern. Eine Differenzierung zwischen dem physischen und logischen Löschen könnte dieses Risiko in der Implementierung darstellen.

Die vorliegende Arbeit kommt zu dem Schluss, dass der Gesetzestext derzeit eine Unklarheit aufweist, die durch eine Interpretation zugunsten einer logischen Löschung im Sinne des Löschbegriffes der DSGVO überkompensiert wird. Die vorliegende Untersuchung kommt zu dem Schluss, dass klare Vorgaben für technische und organisatorische Maßnahmen erforderlich sind, um die Löschung von Daten sicher und effektiv zu gestalten. Dies entspricht den fundamentalen Prinzipien sowie den Anforderungen der DSGVO.

Die Kosten und eingesetzten Ressourcen, die mit der Umsetzung effektiver Löschmethoden verbunden sind, müssen im Verhältnis zum Datenschutzrisiko stehen. Ein risikobasierter Ansatz ermöglicht eine wirtschaftlich sinnvolle Umsetzung. Die Gefahr der Reidentifikation pseudonymisierter Daten stellt ein erhebliches Risiko dar, das bei der Auslegung und Umsetzung des Löschrechts berücksichtigt werden muss. Dies unterstreicht die Bedeutung eines strikten Datenschutzes. Die Arbeit legt nahe, dass der Gesetzestext dahingehend präzisiert werden sollte, dass zwischen logischer und physischer Löschung unterschieden wird. Dies würde sowohl die Rechtssicherheit erhöhen als auch die praktische Umsetzung erleichtern.

Die in der Forschungsfrage „*Inwieweit erfüllen verschiedene juristisch-technische Löschmechanismen im menschenzentrierten Datenschutz die technischen Anforderungen, sind rechtlich konform und entsprechen den Erwartungen der Benutzer?*“ aufgeworfene Thematik spiegelt sich umfassend in der Analyse der Löschmechanismen wider. Diese Diskussion reflektiert, dass die betrachteten Methoden eine Spannbreite von streng regelkonformen bis hin zu benutzerzentrierten Lösungen aufzeigen. Während einige Methoden wie NIST SP 800-88 und BSI Grundschutz CON.6 durch ihre umfassenden Richtlinien und strengen Protokolle hohe Sicherheit und Endgültigkeit der Datenlöschung garantieren und somit technische Anforderungen sowie rechtliche Konformität hervorragend erfüllen, zeigt die Analyse auch, dass Methoden wie das Löschen durch das Betriebssystem vor allem auf die Benutzererwartungen mit ihrer Schnelligkeit und einfachen Durchführung abzielen. Die umfassende Bewertung aller Methoden hinsichtlich verschiedener Kriterien ermöglicht es, die komplexen Interdependenzen zwischen technischer Machbarkeit, rechtlicher Notwendigkeit und Benutzerakzeptanz herauszuarbeiten und somit einen ganzheitlichen

Blick auf den aktuellen Stand der Technik und dessen Eignung im Rahmen des Datenschutzes zu bieten.

A. Implikationen für die Rechtswissenschaft und Praxis

Die aktuelle juristische Interpretation des Löschbegriffs, wie er in der DSGVO verwendet wird, offenbart signifikante technische Risiken für die Betroffenen. Die Ergebnisse der vorliegenden Analysen verdeutlichen, dass eine konsequente Unterscheidung zwischen logischem und physischem Löschen notwendig ist, um den Schutz personenbezogener Daten effektiv zu gewährleisten. Diese Notwendigkeit manifestiert sich insbesondere bei der Analyse der historischen Entwicklung der rechtlichen Rahmenbedingungen zur Datenlöschung, insbesondere der Änderungen, die im österreichischen Datenschutzgesetz (DSG) 1978 implementiert wurden.

Die Revision des DSG im Jahr 1987 führte präzise Definitionen für das physische und das logische Löschen ein. Physisches Löschen wurde als „Unkenntlichmachen von Daten in der Weise, dass eine Rekonstruktion nicht möglich ist", definiert, während das logische Löschen als „die Verhinderung des Zugriffs auf Daten durch programmtechnische Maßnahmen" beschrieben wurde. Diese Differenzierung reflektierte eine fortschrittliche Anerkennung der technologischen Realitäten sowie der Notwendigkeit, sowohl den Zugriff als auch die Existenz der Daten selbst zu kontrollieren.

Die aktuelle Auslegung der DSGVO bietet jedoch keine solch klaren Abgrenzungen. Dies stellt ein Risiko dar, weil logisches Löschen, also die bloße Sperrung der Daten ohne deren physische Zerstörung[70], den Daten subjektiv einen Schutzstatus verleiht, der objektiv nicht gegeben ist. Die Daten bleiben physisch vorhanden und potenziell rekonstruierbar, was insbesondere bei mangelnder physischer Sicherung der Datenträger ein erhebliches Sicherheitsrisiko bedeutet. Darüber hinaus folgt die Notwendigkeit einer ausdrücklichen Unterscheidung aus dem unionsrechtlich verankerten Prinzip des effektiven Grundrechtsschutzes und den datenschutzrechtlichen Vorgaben der Art. 5 und Art. 17 DSGVO. Das Ziel der Löschpflicht ist nicht lediglich die Zugriffsbeschränkung, sondern die tatsächliche Beendigung der Verfügbarkeit personenbezogener Daten. Logische Löschmethoden, die lediglich die Adressierung oder Sichtbarkeit der Daten aufheben, lassen

70 *Knyrim*, Praxiskommentar zum Datenschutzrecht - DSGVO und DSG 2019, Online, Art. 4 Rz. 42.

die physische Existenz der Information unberührt. Diese verbleibende Rekonstruierbarkeit widerspricht dem Schutzzweck des Art. 17 DSGVO, insbesondere bei sensiblen Datenkategorien. Eine Löschmaßnahme kann nur dann als effektiv gelten, wenn sie die Möglichkeit des Wiederzugriffs technisch ausschließt. Dies ist ausschließlich durch physische oder kryptographisch finalisierende Maßnahmen gewährleistbar.

Es wird daher vorgeschlagen, eine rechtliche Revision der DSGVO zu erwägen, die eine ähnliche Differenzierung zwischen physischem und logischem Löschen einführt, wie sie bereits im österreichischen DSG von 1987 vorhanden war. Eine solche Änderung würde die juristische Klarheit erhöhen und sicherstellen, dass die technische Handhabung von Datenlöschungen den tatsächlichen Anforderungen des Datenschutzes entspricht. Konkret sollte die DSGVO um die Definitionen des physischen Löschens als „Unkenntlichmachen von Daten in der Weise, dass eine Rekonstruktion nicht möglich ist" und des logischen Löschens als „die Verhinderung des Zugriffs auf Daten durch programmtechnische Maßnahmen" ergänzt werden. Gleichzeitig ist jedoch auch das Verhältnismäßigkeitsprinzip zu beachten. Eine ausnahmslose Pflicht zur physischen Löschung würde in bestimmten technischen Konstellationen, etwa bei unveränderlichen Speichermodellen wie der Blockchain, zu unüberwindbaren Umsetzungshindernissen führen. Die Zulässigkeit logischer Löschung sollte daher gesetzlich eng gefasst und nur für solche Ausnahmefälle vorgesehen werden, in denen physische Vernichtung derzeit technisch unmöglich oder unzumutbar ist. Eine solche Regelung wahrt die erforderliche Flexibilität, ohne den Schutzzweck des Datenschutzrechts zu unterlaufen, und stellt ein ausgewogenes Verhältnis zwischen den Interessen der betroffenen Personen und den faktischen Möglichkeiten der Verantwortlichen her.

Des Weiteren ist es angebracht, klarzustellen, **dass logisches Löschen nur als temporäre Maßnahme in streng geregelten Ausnahmefällen zulässig sein sollte**. Diese Einschränkung würde die Rechtssicherheit für die Datenverarbeiter erhöhen und die Rechte der betroffenen Personen effektiver schützen. Die Inkorporation dieser klaren und differenzierten Definitionen würde dazu beitragen, die Lücke zwischen der rechtlichen Regelung und der technischen Praxis zu schließen und somit den Datenschutz auf ein neues, zeitgemäßes Niveau zu heben.

Die vorgeschlagenen Änderungen dienen nicht nur der Stärkung des Schutzes der Betroffenen, sondern auch der Bereitstellung klarer rechtlicher Rahmenbedingungen für die Verantwortlichen. In der Folge könnten Datenverarbeitungsprozesse sowohl effizienter als auch konformer gestaltet

werden, wodurch die Vertrauenswürdigkeit und Rechtskonformität der Datenverarbeitung im digitalen Zeitalter gefördert werden würde.

B. Abwägung zwischen Heteronomie, Überregulierung und Risiken

Um eine Überregulierung zu vermeiden, sollte geprüft werden, ob eine detaillierte Regulierung zur Definition der Löschbegriffe tatsächlich notwendig ist. Brownsword betont, dass die regulatorische Herausforderung darin besteht, „nützliche Innovationen zu fördern und gleichzeitig inakzeptable Risiken für Mensch und Umwelt zu kontrollieren“[71]. Aus technologischer Perspektive ist der Löschbegriff im Gegensatz zur Selbstverantwortung und der damit verbundenen Flexibilität bei der Implementierung weniger einschränkend. Die vorliegende Untersuchung zielt darauf ab, den Terminus „Löschung“ einer präzisen Definition zu unterziehen. Sofern sich aus technischer Sicht, wie es beispielsweise bei der später erwähnten Technologie unveränderlicher Speicher, wie etwa der Blockchain-Technologie, nicht realisieren lässt, wäre eine logische Löschung im Sinne der DSGVO und DSG bis zu dem Zeitpunkt ausreichend, an dem eine physische Löschung möglich wird. Eine differenzierte Definition von physischem und logischem Löschen kann mit dem technologischen Fortschritt Schritt halten, indem sie Raum für Anpassungen lässt, ohne dass ständig neue, restriktive Regelungen eingeführt werden müssen. Allein der Umstand, dass die vorgeschlagene Definition über mehrere Generationen der Automatisierung und Digitalisierung immer noch zutreffend ist, ist eine starke Evidenz dafür, dass diese technologieneutral und nicht zu speziell ist. Dies unterstützt die Balance zwischen Sicherheit und Innovationsförderung. Ein starker Eingriff in die Innovation ist durch die Abgrenzung der bereits etablierten Verfahren daher nicht zu erwarten. Die Risiken, gegen die abgewogen werden muss, bleiben jedoch, wie bereits erwähnt, evident.

Es sei jedoch die Frage aufgeworfen, ob eine zu detaillierte Ausdifferenzierung des Löschbegriffs nicht paradoxerweise zu den von der Verhaltensökonomie beschriebenen Effekten wie Überregulierung und reduzierter Eigenverantwortung führen könnte. Insbesondere der Peltzman-Effekt[72] könnte in diesem Zusammenhang relevant werden, wenn Datenverarbeitende aufgrund explizit definierter Löschvorgänge eine falsche Sicherheit

71 *Brownsword*, Rethinking Law, Regulation, and Technology, Übers. d. Verf., S. 6.
72 *Specht*, The Journal of SH&E Research 4 (2007) 3.

empfinden und infolgedessen eine kritische Auseinandersetzung mit Risiken und dem tatsächlichen Schutz personenbezogener Daten vernachlässigen. Die rechtliche Notwendigkeit, präzise und unmissverständlich zu definieren, was unter Löschung zu verstehen ist, könnte daher in einer unerwünschten Heteronomie resultieren, bei der der Fokus mehr auf die Einhaltung spezifischer Vorgaben als auf das übergeordnete Ziel des Datenschutzes gelegt wird. Diese Überlegungen bedürfen einer sorgfältigen Abwägung, um sowohl die Compliance als auch die datenschutzrechtliche Sensibilisierung zu fördern.

C. Limitationen der Studie und mögliche Verbesserungen

Die Studie basiert auf einer begrenzten Anzahl von Quellen und könnte durch die Einbeziehung weiterer empirischer Daten oder expliziter Studien verbessert werden, um umfassendere Ergebnisse zu erzielen. Eine Limitation der Studie ist das Fehlen empirischer Untersuchungen, die die praktische Umsetzung der Löschvorschriften in verschiedenen Organisationen analysieren. Eine vertiefte Analyse der technischen Aspekte der Datenlöschung, insbesondere in Bezug auf moderne Technologien (KI, Blockchain etc.), könnte die Studie ergänzen. Die vorliegende Untersuchung fokussiert sich auf eine Auswahl von Gerichtsurteilen. Eine umfassendere Analyse könnte zu einer detaillierteren Bewertung der Rechtsprechung führen. Die vorliegende Studie fokussiert sich in hohem Maße auf das EU-Recht und könnte durch einen Vergleich mit internationalen Datenschutzregelungen ergänzt werden. Die vorliegende Untersuchung könnte durch die Berücksichtigung von Sonderfällen, wie beispielsweise der Löschung von publizierten oder verteilten Daten, detailliertere Informationen liefern. So wäre es möglich, die Notwendigkeit einer spezialisierten Regelung für diese zu ermitteln. Eine wesentliche Limitation besteht in der Vernachlässigung einer Analyse der langfristigen Implikationen der Löschung von Daten, insbesondere unter Berücksichtigung des Datenschutzes und der Datensicherheit. Eine vertiefte Analyse der Perspektive der betroffenen Personen könnte zu einem besseren Verständnis der Auswirkungen der Löschung auf die individuellen Rechte beitragen.

D. Ausblick für zukünftige Forschung

Zukünftige Forschung könnte empirische Studien berücksichtigen, um die tatsächliche Umsetzung und Wirksamkeit von Löschmaßnahmen in der Praxis zu evaluieren. Es besteht Bedarf an der Entwicklung klarer, praxisorientierter Leitlinien für die Datenlöschung für Unternehmen, die sowohl logische als auch physische Löschmethoden umfassen. Die Auswahl der adäquaten Löschmethode für die entsprechende Risikoklasse soll auf diese Weise optimiert werden.

Die Implikationen neuer Technologien auf die Datenlöschung sollten einer verstärkten Untersuchung unterzogen werden, um rechtliche und technische Anpassungen frühzeitig zu identifizieren. Entwicklungen im Bereich der Quantencomputer und -algorithmen können potenziell zu abrupten Veränderungen im Risikoprofil spezifischer Verfahren führen. Unternehmen, die technische Datenschutzmaßnahmen implementieren, sollten in die Lage versetzt werden, diese Entwicklungen einfach aufzufinden und zu konsumieren, um entsprechende Änderungen vorzunehmen.

Mit weiterer Forschung und praxisnaher Entwicklung könnte damit Unternehmen geholfen werden, ihren Verpflichtungen, speziell auch, aber nicht beschränkt auf Löschrechte nachzukommen und diese technisch-juristisch sicher zu implementieren.

E. Zusammenfassung der Diskussion

In Anbetracht der **ratio legis der DSGVO**, welche primär darauf abzielt, eine ausgewogene Balance zwischen den Rechten der betroffenen Personen und den Pflichten der Verantwortlichen zu schaffen, ist es unerlässlich, dass die **Risiken**, denen die Betroffenen ausgesetzt sind, sowohl für diesen **transparent** als auch **minimiert** werden. Die DSGVO verfolgt das Ziel, die Grundrechte der betroffenen Personen zu schützen und zugleich den Verantwortlichen eine gewissenhafte Abwägung von Aufwand und Risiko zu erlauben.

Die derzeitige Interpretation führt zu einer **Erhöhung des Risikos** eines möglichen Verstoßes gegen die Datenminimierung, Transparenz, Speicherbegrenzung, Integrität und allen voran **Vertraulichkeit** der betroffenen Daten (vgl. Art. 5, welcher die Grundsätze und Prinzipien der DSGVO beschreibt). Die gesellschaftliche Erwartungshaltung, vor allem Endgültigkeit, Sicherheit und Transparenz, deckt sich stark mit diesen Grundsätzen, aber

nicht mit der derzeitigen Interpretation dieser. Der teleologische Ansatz erfordert, dass die etablierten, standardisierten Verfahren, welche zur Reduktion dieses Risikos beitragen und bereits lange etabliert sowie technisch unaufwändig implementierbar sind, vollumfänglich Berücksichtigung finden.

Die **historische Exegese** zeigt zudem, dass eine ähnliche Problematik bereits im DSG1978 durch eine gesetzliche Klarstellung im Jahr 1987 adressiert wurde. Diese Gesetzeserweiterung diente der Präzisierung und Verbesserung des Datenschutzes und es ist daher nur folgerichtig, eine vergleichbare Erweiterung für die DSGVO anzustreben, um dem ursprünglichen gesetzgeberischen Willen gerecht zu werden und die Schutzintention der Norm zu wahren.

VII. Conclusio

Die vorliegende Arbeit zielte darauf ab, die Eignung juristisch-technischer Löschmechanismen im menschenzentrierten Datenschutz zu bewerten. Die vorliegenden Ergebnisse zeigen, dass logische Löschmethoden mit technischen Risiken assoziiert sind, während das physische Löschen eine sicherere Alternative darstellt.

Die vorliegende Untersuchung kommt zu dem Schluss, dass der Begriff des „Löschens" in der DSGVO sowie im österreichischen DSG rechtlich nicht präzise definiert ist. Diese Unbestimmtheit erweist sich insbesondere im Kontext der technischen Umsetzung als problematisch. Eine Analyse der Rechtsprechung des EuGH, OGH und der österreichischen Datenschutzbehörde offenbart eine uneinheitliche Auslegung und Anwendung des Löschbegriffs, insbesondere hinsichtlich der Abgrenzung zwischen physischer und logischer Löschung. Die Tatsache, dass die logische Löschung als rein programmtechnische Zugriffsbeschränkung keinen tatsächlichen Datenverlust verursacht, steht im Spannungsverhältnis zum in Art. 17 DSGVO normierten Anspruch auf Löschung und den Grundprinzipien des Datenschutzrechts, insbesondere dem der Integrität und Vertraulichkeit gemäß Art. 5 Abs. 1 lit. f DSGVO. Gemäß der technischen Analyse ist festzustellen, dass insbesondere logische Löschmethoden das Risiko einer Reidentifikation personenbezogener Daten nicht hinreichend ausschließen. Somit kann in bestimmten Fällen keine endgültige Löschung der Daten gewährleistet werden. Gemäß dem Stand der Technik, wie er in Art. 32 DSGVO und in einschlägigen Standards wie dem BSI Grundschutz CON.6 konkretisiert

ist, ist eine risikoadäquate Auswahl und Überprüfung der eingesetzten Verfahren erforderlich. In diesem Zusammenhang ist die von der DSGVO geforderte Verhältnisbestimmung zwischen dem Aufwand für den Verantwortlichen und dem Risiko für die betroffene Person von maßgeblicher Relevanz. Die Ergebnisse der Untersuchung legen nahe, dass eine gesetzliche Präzisierung des Begriffs „Löschen" erforderlich ist, insbesondere durch die ausdrückliche Unterscheidung zwischen logischem und physischem Löschen. Eine solche Differenzierung würde nicht nur die Kohärenz der Auslegung fördern, sondern auch eine unionsweit einheitliche und effektive Anwendung des Löschrechts gewährleisten. Der Gesetzgeber sieht sich folglich in der Pflicht, den Löschbegriff normativ zu präzisieren, um den datenschutzrechtlichen Schutzzielen zu entsprechen und bestehende Auslegungsspielräume im Sinne der Betroffeneninteressen zu limitieren.

VIII. Rechtsquellenverzeichnis

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

Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz - DSG1978), Fassung von 1980.

Bundesgesetz vom 18. Oktober 1978 über den Schutz personenbezogener Daten (Datenschutzgesetz - DSG1978), Fassung von 1987.

Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG), Fassung vom 29.06.2024.

IX. Literaturverzeichnis

Albrecht, in Datenschutzrecht: DSGVO mit BDSG (2019).

Anderl/Schelling, in #Blockchain in der Rechtspraxis (2020).

Baun, Operating Systems / Betriebssysteme – Bilingual Edition: English – German / Zweisprachige Ausgabe: Englisch – Deutsch (2020) http://link.springer.com/10.1007/978-3-658-29785-5 [Operating Systems / Betriebssysteme].

Bettany/Halsey, Windows File System Troubleshooting (2015).

Brand ea, in Datenschutz-Grundverordnung: VO (EU) 2016/679: Bundesdatenschutzgesetz: Kommentar (2022).

M. Braun/Kamann, in DS-GVO: Datenschutz-Grundverordnung: Kommentar (2024).

Brownsword, Rethinking Law, Regulation, and Technology (03.04.2022) https://www.elgaronline.com/view/9781800886469.xml.

BSI, Technische Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen (TR-02102-1)[2024-01] (2024) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=5.

BSI, Technische Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen (TR-02102-1)[2021-01] (2021) https://web.archive.org/web/20220120061112/https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf;jsessionid=5FAA6C5F75A71422772001A3C9EED482.internet481?__blob=publicationFile&v=2.

Bundesamt für Sicherheit in der Informationstechnik, CON.6 Löschen und Vernichten, Edition 2023 (2023) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2023/03_CON_Konzepte_und_Vorgehensweisen/CON_6_Loeschen_und_Vernichten_Edition_2023.pdf?__blob=publicationFile&v=2.

Department of Defense, National Industrial Security Program Operating Manual (5220.22-M) (2006).

DIN SPEC 66399-3:2013-02, Büro- und Datentechnik – Vernichten von Datenträgern https://dx.doi.org/10.31030/1935106 [DIN SPEC 66399-3].

Dobrauz-Saldapenna/Rosenauer, in Datenschutz: Recht und Praxis (2020).

Dodge/Kitchin, Outlines of a World Coming into Existence – Pervasive Computing and the Ethics of Forgetting, Environment and Planning B: Planning and Design 34 (06.2007) 3, 431 ['Outlines of a World Coming into Existence'].

EDPB, Guidelines 9/2022 on personal data breach notification under GDPR (2022).

EDPB, Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (2020).

EDPB, Leitlinien 5/2019 zu den Kriterien des Rechts auf Vergessenwerden in Fällen in Bezug auf Suchmaschinen gemäß der DSGVO (2020).

Feiler/Forgó, EU-DSGVO und DSG – EU-Datenschutz-Grundverordnung und Datenschutzgesetz: Kommentar[2. Auflage] (2022) [EU-DSGVO und DSG].

Fritz, Das Löschungsrecht nach Art 17 DSGVO in der Entscheidungspraxis und Rechtsprechung, Datenschutzrecht Jahrbuch 2022 (19.01.2023).

Gürses/Troncoso/Diaz, Engineering privacy by design, Computers, Privacy & Data Protection (CPDP) 14 (2011).

Halsey/Bettany, Windows file system troubleshooting, Expert's voice in Microsoft Windows (2015).

International Organization for Standardization, Information technology – Security techniques – Storage security (ISO/IEC 27040:2024) (Published: ISO/IEC 27040:2024 2024).

Knyrim, Der DatKomm, Praxiskommentar zum Datenschutzrecht - DSGVO und DSG 2019, Online.

Koops, Forgetting Footprints, Shunning Shadows – A Critical Analysis of the „Right to Be Forgotten" in Big Data Practice, SSRN Electronic Journal 2011 http://www.ssrn.com/abstract=1986719 [Forgetting Footprints, Shunning Shadows].

Kranenborg, Article 17 Right to erasure ('right to be forgotten'), in *Kuner ea* (Hrsg), The EU General Data Protection Regulation (GDPR) (13.02.2020) 475 https://academic.oup.com/book/41324/chapter/352298059.

Kühling ea, Datenschutz-Grundverordnung, BDSG – Kommentar[4. Auflage] (2024) [Datenschutz-Grundverordnung, BDSG].

Mayer-Schönberger, The Virtue of Forgetting in the Digital Age (2011) https://doi.org/10.1515/9781400838455.

National Institute of Standards and Technology, Guidelines for Media Sanitization (SP 800-88) (2014).

Nepal ea, Editorial – Human-Centric Security and Privacy, Frontiers in Big Data 5 (17.02.2022) https://www.frontiersin.org/articles/10.3389/fdata.2022.848058/full [Editorial].

Nissenbaum, Privacy in context – technology, policy, and the integrity of social life (2010) [Privacy in context].

Norman, The design of everyday things[Revised and expanded edition] (2013).

Piltz, Sicherheit personenbezogener Daten, in Datenschutz-Grundverordnung: VO (EU) 2016/679: Bundesdatenschutzgesetz: Kommentar (2022).

Piska (Hrsg), Blockchain rules – das FinTech-Handbuch[2. Auflage] (2024) [Blockchain rules].

Piska/Bierbauer, in Blockchain Rules (2024).

Purtova, The Law of Everything – Broad Concept of Personal Data and Future of EU Data Protection Law, Law, Innovation and Technology 10 (2018) 1, 40.

Silberschatz/Galvin/Gagne, Operating system concepts[Ninth edition] (2013).

Specht, The Peltzman effect – Do safety regulations increase unsafe behavior, The Journal of SH&E Research 4 (2007) 3.

Tzanou, The unexpected consequences of the EU Right to Be Forgotten – Internet search engines as fundamental rights adjudicators, in Personal Data Protection and Legal Developments in the European Union (2020) 279.

Voigt/Von Dem Bussche, EU-Datenschutz-Grundverordnung (DSGVO) (2018) http://link.springer.com/10.1007/978-3-662-56187-4.

Wolff/Brink, BeckOK Datenschutzrecht[48. Edition] (2023).

CMS Hasche Sigle Partnerschaft von Rechtsanwälten und Steuerberatern mbB, GDPR Enforcement Tracker – List of GDPR fines, (abgefragt 8. 3. 2024).

X. Entscheidungsverzeichnis

EuGH 26. 4. 2023, Rechtssache T-557/20, *Einheitlicher Abwicklungsausschuss gegen Europäischer Datenschutzbeauftragter*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62020TJ0557&qid=1709927171181.

EuGH 19.10.2016, Rechtssache C-582/14, *Patrick Breyer gegen Bundesrepublik Deutschland*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62014CJ0582.

EuGH 16.7.2020, Rechtssache C-311/18, *Data Protection Commissioner gegen Facebook Ireland Limited und Maximillian Schrems*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62018CJ0311&qid=1709931086167.

EuGH 27 Oktober 2022, Rechtssache C-129/21, *Proximus NV gegen Gegevensbeschermingsautoriteit*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62021CJ0129&qid=1751209049981.

EuGH 5.12.2023, Rechtssache C-807/21, *Deutsche Wohnen SE gegen Staatsanwaltschaft Berlin*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62021CJ0807&qid=1709927140384.

EuGH 14.12.2023, Rechtssache C-456/22, *VX und AT gegen Gemeinde Ummendorf*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62022CJ0456&qid=1709930921739.

EuGH 25.01.2024, Rechtssache C-687/21, *BL gegen MediaMarktSaturn Hagen-Iserlohn GmbH*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62021CJ0687&qid=1709926727671.

Europäischer Gerichtshof 8 Dezember 2022, Rechtssache C-460/20, *TU und RE gegen Google LLC*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62020CJ0460&qid=1751208855425.

Europäischer Gerichtshof 14.10.2023, Rechtssache C-340/21, *VB gegen Natsionalna agentsia za prihodite*, https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62021CJ0340&qid=1709927018251.

Bescheid (AEPD) 28.07.2023 (Bescheid PS/00331/2022 der Spanischen Datenschutzbehörde (AEPD)).

Bescheid (HDPA) 27.01.2022 (Bescheid 4/2022 der Griechischen Datenschutzbehörde (HDPA)).

Beschluss (EDSA) (Verbindlicher Beschluss 2/2022 zur Streitigkeit nach Artikel 65 Absatz 1 Buchstabe a der DSGVO über den Beschlussentwurf der irischen Aufsichtsbehörde bezüglich Meta Platforms Ireland Limited (Instagram)) [28.7.2022].

Datenschutzbehörde 05.12.2018, DSB-D123.270/0009-DSB/2018, *DSB-D123.270/0009-DSB/2018*, https://www.ris.bka.gv.at/JudikaturEntscheidung.wxe?Abfrage=Dsk&Dokumentnummer=DSBT_20181205_DSB_D123_270_0009_DSB_2018_00.

Datenschutzbehörde 13.12.2018, DSB-D122.995/0003-DSB/2018, *DSB-D122.995/0003-DSB/2018*, https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181213_DSB_D122_995_0003_DSB_2018_00/DSBT_20181213_DSB_D122_995_0003_DSB_2018_00.html.

Oberster Gerichtshof 15.04.2010, 6Ob41/10p, *6Ob41/10p*, https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20100415_OGH0002_0060OB00041_10P0000_000&Suchworte=RS0125838.

Oberster Gerichtshof 13.09.2012, 6Ob107/12x, *6Ob107/12x*, https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20120913_OGH0002_0060OB00107_12X0000_000&Suchworte=6Ob107/12x.

Google Spain SL und Google Inc gegen Agencia Española de Protección de Datos (AEPD) und Mario Costeja González, No. Rechtssache C-131/12 (EuGH 13 Mai 2014), https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62012CJ0131.