

Datenschutzgrundverordnung, Archivgesetze und Archivpraxis. Datenschutz im Archiv vor neuen Herausforderungen

von Clemens Rehm

Prolog

„Sie saß viele Jahre in der Stadtverordnetenversammlung ihrer Stadt und hat Entscheidungen mitbeschlossen. Nach ihrem Ausscheiden hat sie sich nun entschieden, dass alle persönlichen Daten von ihr gelöscht werden – begründet mit der Datenschutzgrundverordnung DSGVO. Für die Stadt begann ein enorm aufwändiger Prozess, selbst Internetgigant Google musste helfen.“¹

Auf eine Rückfrage zum Sachverhalt schrieb die Stadt Friedberg: „Der Bericht ist größtenteils richtig. Ein ehemaliges Mitglied der Stadtverordnetenversammlung hat von seinem Recht nach Art. 17 DSGVO Gebrauch gemacht und um unverzügliche Löschung seiner/ihrer personenbezogenen Daten gebeten. Dieser Aufforderung sind wir nach Rücksprache mit unserem Datenschutzbeauftragten sowie dem Hessischen Städte- und Gemeindebund nachgekommen.“²

Der Name wurde aus den digitalen Ratsinformationssystemen mit Hilfe eines Dienstleisters und im Netz mit Hilfe von Google entfernt;³ im Rathaus Friedberg saß eine Mitarbeiterin drei volle Tage daran, den Namen der An-

tragstellerin in allen gedruckten Protokollen zu schwärzen. Unter Bezugnahme auf die DSGVO wurden in diesem Fall authentische Dokumente nachträglich verändert, dadurch das gesellschaftliche Gedächtnis beschnitten und die Transparenz politischer Entscheidungen verunmöglicht. Das bedeutet zugleich eine Be- und Verhinderung der archivischen Aufgabenerfüllung und im Kern eine grundsätzliche Infragestellung von Archiven.

1 Christian Erhardt, DSGVO: Gemeinderat pocht auf das Recht, vergessen zu werden, in: Kommunal vom 2. Juli 2020 <https://kommunal.de/dsgvo-gemeinderat-vergessen> [Stand: 13.01.2022, gilt ebenfalls für alle nachfolgenden Hinweise auf Internetquellen].

2 Mail der Stadt Friedberg vom 9. Juli 2020.

3 Erhardt (wie Anm. 1): „Somit musste der Dienstleister eingeschaltet werden um sicher zu gehen, dass alle Daten aus dem System gelöscht werden konnten. Die Fraktionen im Gemeinderat mussten ebenfalls überprüfen, ob sie etwa auf ihren Webseiten Informationen zur Person zur Verfügung gestellt haben. Etwa in alten Pressemitteilungen, in der möglicherweise eine Aussage des ehemaligen Gemeinderats zitiert wurde. Im Zweifelsfall kann diese Meldung Jahre zurück liegen, aber noch irgendwo im Internet vorhanden sein. Daher wurde sogar Google eingeschaltet, um das Recht auf Vergessen der ehemaligen Stadtverordneten durchzusetzen.“

Fragestellung

Nachdem die ersten Erfahrungen mit den Auswirkungen der seit Mai 2018 geltenden Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) auf die Praxis vorliegen, stellt sich die Frage nach einer Zwischenbilanz. Dabei sollen im Folgenden drei Felder v.a. unter Bezug auf den archivischen Alltag angesprochen werden.

Vergessenwerden und „Recht auf Erinnerung“

Mit der Regelungssystematik der DSGVO wurden dem Datenschutz Schranken gesetzt, um die Aufgabenerfüllung und Arbeitsfähigkeit von Archiven überhaupt zu ermöglichen bzw. weiter zu gewährleisten. Neben dem zentralen „Recht auf Vergessenwerden“ wurde in der DSGVO auch ein „Recht auf Erinnerung“ verankert – auch wenn es *expressis verbis* nicht so genannt wird, sondern (nur) von der Verpflichtung gesprochen wird „Aufzeichnungen von bleibendem Wert für das allgemeine öffentliche Interesse zu erwerben, zu erhalten, zu bewerten, aufzubereiten, zu beschreiben, mitzuteilen, zu fördern, zu verbreiten sowie Zugang dazu bereitzustellen“.⁴ Diesen Sachverhalt der herausragenden Privilegierung von Archiven in der DSGVO gilt es den Archivträgern, den Datenschützern, den Medien und der Öffentlichkeit nahe zu bringen. Offen scheint oder zumindest zu diskutieren wäre, welche Archivtypen von dieser Privilegierung profitieren sowie wozu die Privilegierung diese Archive berechtigt und welche Grenzen ihr gesetzt wurden. Die Antwort darauf wird auch Konsequenzen für die Sicherung z.B. von Forschungsdaten haben. Darüber hinaus ist zu fragen, ob dieses erstmals juristisch fundierte Recht einer Gesellschaft auf die Dokumentation ihrer Geschichte in diesem Kontext nicht zu einer „Pflicht zur Erinnerung“ weiterentwickelt werden kann.

Privilegiert arbeiten – Neue Herausforderungen in der Archivpraxis

Die Privilegierung der Archive gab es in der DSGVO nicht völlig bedingungslos. Bei allen Arbeitsfeldern in den Archiven, v.a. bei der Überlieferungsbildung und der Speicherung, der Erschließung, der Zugänglichmachung sowie der Verbreitung von archivierten Informationen, ist sich vielleicht deutlicher als bisher bewusst zu machen und zu prüfen, inwieweit die Vorgaben der DSGVO eine Änderung in der Praxis nach sich ziehen sollten oder sogar müssen. Dabei werden künftig für den Archivbereich komplett neue Verfahren wie die Pseudonymisierung eine Rolle spielen; hierzu ist in den Archiven Expertise zu erwerben und es sind Anwendungsszenarien zu entwickeln.

Vertrauen erhalten

Die digitale Welt ermöglicht in bisher nicht gekannter Weise die Präsentation von Informationen. Diese Chance haben Archive auf vielfältige Weise genutzt, indem sie zum einen Metadaten über Bestände und digitalisiertes Archivgut online gestellt haben und zum zweiten neue Wege der digitalen Kommunikation z.B. über *social media* ge-

gangen sind.⁵ In vielen Fällen gingen und gehen bis heute solchen Aktivitäten rechtliche Prüfungen voraus. Urheberrechtsgesetz und der Schutz von Persönlichkeitsrechten sind die Ursachen für vielerlei Verunsicherungen bei der archivischen Onlineaktivität.⁶

Kaum im Blick ist bei diesem Prozess, dass im Internet präsentierte Daten inzwischen in bisher in vor Jahren noch unvorstellbarer Weise und Häufigkeit gefunden und zudem verknüpft werden können. So wünschenswert diese Auffindbarkeit von archivierten Informationen ist, die auch eine Sichtbarkeit der Archive bedeutet, so wenig sind die möglichen Auswirkungen auch historischer Daten auf die aktuelle Gesellschaft und Individuen angemessen bedacht worden. Hier stellt sich die Frage, ob Archive wirklich alles im Netz machen sollen und können, was ihnen an Verbreitung von Informationen erlaubt ist. Oder anders formuliert: Gibt es eine Grenze für Archive bei der Verbreitung von Informationen, um das Vertrauen zu bewahren und zu erhalten, das sie bisher erhalten, d.h. das ihnen bisher entgegengebracht wird?

Vergessenwerden und „Recht auf Erinnerung“

Die seit 25. Mai 2018 geltende DSGVO ersetzt als unmittelbar geltende EU-Regelung bisher bestehende nationale Regelungen im Bereich Datenschutz. Für die Arbeit im Archivwesen sind die Grenzen der Anwendung der DSGVO und die Privilegierung der Archive in der DSGVO relevant; dabei sind die Ermächtigung der Archive einerseits und die Einschränkung von Betroffenenrechte andererseits zu unterscheiden.⁷ Damit liegen die Instrumente vor, mit denen im Archivalltag entstehende Fragestellungen abgewogen werden können.

4 Erwägungsgrund 158 Satz 2 DSGVO: „Behörden oder öffentliche oder private Stellen, die Aufzeichnungen von öffentlichem Interesse führen, sollten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten rechtlich verpflichtet sein, Aufzeichnungen von bleibendem Wert für das allgemeine öffentliche Interesse zu erwerben, zu erhalten, zu bewerten, aufzubereiten, zu beschreiben, mitzuteilen, zu fördern, zu verbreiten sowie Zugang dazu bereitzustellen.“

5 Vgl. Archivar 71 (2018): Schwerpunktthema: Offene Archive – Archive im Web 2.0 https://www.archive.nrw.de/sites/default/files/media/files/Archivar-1_2018_0.pdf.

6 Die sehr große Resonanz des 2017 durchgeführten 22. Archivwissenschaftlichen Kolloquiums der Archivschule Marburg zu „Archivarinnen und Archivare auf schwankendem rechtlichem Boden?“ belegt diese Unsicherheit; vgl.: Irmgard Becker/Clemens Rehm/Udo Schäfer (Hrsg.), Nicht nur Archivgesetze ... Archivarinnen und Archivare auf schwankendem rechtlichem Boden? Best Practice – Kollisionen – Perspektiven (Veröffentlichungen der Archivschule Marburg 66), Marburg 2019. Einen Überblick (ohne DSGVO) liefert Clemens Rehm, Die ständig wachsende Bedeutung rechtlicher Fragestellungen im Alltag der Archive, in: Torsten Musial/Yves A. Pillep (Hrsg.), Kulturelle Vielfalt. Archive in Berlin, Fulda 2021, S. 77–92.

7 Vgl. Clemens Rehm, Das „Recht auf Erinnerung“. Zur Relevanz des Archivwesens im Zeitalter der EU-Datenschutzgrundverordnung, in: RECHTSicher – Archive und ihr rechtlicher Rahmen, 89. Deutscher Archivtag Suhl (Tagungsdokumentation zum Deutschen Archivtag 24), Fulda 2020, S. 45–72; Jakob Wührer, Die EU-Datenschutzgrundverordnung – eine Chance für Archive. Die Vergleichsperspektive Österreich, in: RECHTSicher, S. 27–44.

Geltungsbereich und Grenzen des Anwendungsbereichs der DSGVO

Für die Arbeit in Archiven sind die Geltungsbereiche wesentlich, innerhalb derer die DSGVO greift. Eine wichtige Einschränkung des Geltungsbereichs der DSGVO betrifft die Art der Verarbeitung von Daten. In Artikel 2 Absatz 1 DSGVO ist als Kriterium der Anwendung die digitale Verarbeitung festgelegt:

„Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.“

Während eine Entscheidung über Kriterien wie „lebend/verstorben“ und „nicht anonym/anonym“ in der Regel leicht zu fällen ist (s. u.), steht die Anwendung dieses Kriteriums auf Archive noch in der Diskussion. Für digitale Informationen ist die Anwendung unstrittig, aber was gilt für analoge Unterlagen? Der überwiegende Teil der archivischen Erschließungsdaten liegt in papiergebundener Form vor, sei es in Karteien, Findbüchern oder Einlieferungslisten, und wird auch nicht digital verarbeitet, wenn diese Informationen Nutzerinnen und Nutzern im Lesesaal vorgelegt werden. Diese Daten – auch wenn sie Daten lebender Personen enthalten – fallen dann nicht unter die DSGVO. Was aber, wenn diese Daten durch Maßnahmen der Retrokonversion oder andere technische Verfahren digital verfügbar und einsetzbar werden? Unter Erwägung der grundsätzlichen Ziele des Datenschutzes und der Definition von „Verarbeitung“ in Artikel 4 DSGVO als „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang“ spricht viel dafür, auch diese Daten den Regelungen der DSGVO zu unterwerfen.

Eine weitere wichtige Grenze ist die Tatsache, dass sich die DSGVO ausschließlich auf lebende Personen bezieht (Artikel 1 DSGVO⁸). Anders als beim deutschen Archivrecht, in dem mit einer personenbezogenen Schutz- bzw. Sperrfrist von in der Regel 10 Jahren nach Tod der betroffenen Person generell ein postmortaler Datenschutz verankert ist,⁹ greift die DSGVO bei Verstorbenen nicht.

Ferner beziehen sich die Regelungen der DSGVO auf Informationen zu einer identifizierten oder identifizierbaren natürlichen Person. Das bedeutet, dass die Information mit einer Person verknüpft sein muss oder über einen Schlüssel mit dieser Person verbunden werden kann („Pseudonymisierung“; Definition in Artikel 4 Nr. 5). Anonyme und anonymisierte Daten fallen nicht unter die DSGVO.¹⁰

Privilegien für Archive

Gegen das „Recht auf Vergessenwerden“ wird in der DSGVO im Erwägungsgrund 158 Satz 2 die „Pflicht zur Erinnerung“ gesetzt, bei der nicht zufällig Verben verwendet werden, die den in deutschen Archivgesetzen beschriebenen Tätigkeiten entsprechen:

„Behörden oder öffentliche oder private Stellen, die Aufzeichnungen von öffentlichem Interesse führen, sollten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten rechtlich verpflichtet sein, Aufzeichnungen von bleibendem Wert für das allgemeine öffentliche Interesse zu erwerben, zu erhalten, zu bewerten, aufzubereiten, zu beschreiben, mitzuteilen, zu fördern, zu verbreiten sowie Zugang dazu bereitzustellen.“ [kursive Hervorhebung Rehm]

Im darauf folgenden Satz 3 wird die dafür notwendige Verarbeitung personenbezogener Daten direkt angesprochen.¹¹ In diesem Zusammenhang wurde in der DSGVO mit dem Begriff der „Archivzwecke im öffentlichen Interesse“ ein Weg entwickelt, um trotz des Rechts auf Vergessenwerdens eine Gestaltung der Erinnerung zu erlauben.¹² Von diesem Tatbestand des öffentlichen Interesses werden Rechte abhängig gemacht, durch die eine archivische Arbeit erst ermöglicht wird und die ein funktionierendes Archiv ausmachen. Diese Archivlegitimation ist neu und tritt an die Seite archivwissenschaftlicher Definitionen zur Sicherungs- und Erinnerungsfunktion sowie der gesellschaftlichen Transparenzfunktion von Archiven.

Im Text der DSGVO findet sich diese Grundlegung grundsätzlich in Artikel 6 Abs. 1 Satz 1 Buchstabe e): Archive erfüllen eine Aufgabe, die „im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde“. Diese Übertragung ist in Deutschland in den sieben Archivgesetzen in unterschiedlicher Form verankert worden.¹³ Wesentlich ist, dass im Artikel 17 DSGVO selber – dem Herzstück der DSGVO mit dem Recht auf Löschung („Recht auf Vergessenwerden“) – in Absatz 3 Buchstabe d) die Löschung „für im öffentlichen Interesse liegende Archivzwecke ...“ außer Kraft gesetzt wird. Damit ist auch in der DSGVO das Lö-

8 Erwägungsgrund 27 Satz 1 DSGVO: „Diese Verordnung gilt nicht für die personenbezogenen Daten Verstorbener.“

9 Überblick bei Christine Axer/Jenny Kotte, Zugangsbeschränkungen durch Archivrecht, in: Irmgard Becker/Clemens Rehm (Hrsg.), Archivrecht für die Praxis. Ein Handbuch, München 2017, S. 142–170.

10 Erwägungsgrund 26 Satz 5 und 6 DSGVO: „Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymen Daten, auch für statistische oder für Forschungszwecke.“

11 Erwägungsgrund 158 Satz 3 DSGVO: „Es sollte den Mitgliedstaaten ferner erlaubt sein vorzusehen, dass personenbezogene Daten zu Archivzwecken weiterverarbeitet werden, beispielsweise im Hinblick auf die Bereitstellung spezifischer Informationen im Zusammenhang mit dem politischen Verhalten unter ehemaligen totalitären Regimen, Völkermord, Verbrechen gegen die Menschlichkeit, insbesondere dem Holocaust, und Kriegsverbrechen.“ Die Art der personenbezogenen Daten ist dabei nicht entscheidend. In Artikel 9 Abs. 2 Buchstabe j) DSGVO („Verarbeitung besonderer Kategorien personenbezogener Daten“) wird auch die archivische Verarbeitung besonders schützenswerter Daten erlaubt.

12 Von einer „Quadratur des Kreises“ spricht Ansgar Hense, Art. 89 Rn. 2, in: Gernot Sydow (Hrsg.), Handkommentar-EuDSchVO, Baden-Baden 2. Aufl. 2018, S. 1493.

13 Eine Zusammenstellung bei Rehm (wie Anm. 7), „Recht auf Erinnerung“, S. 70–72.

schungssurrogat – also die Ersetzung der Löschung durch Archivierung – verankert.¹⁴ Verknüpft wird dieses Privileg mit der grundsätzlichen Einhaltung der in der DSGVO geforderten Garantien (Art. 89 Abs. 1 DSGVO), zu denen in Archiven beispielsweise technisch-organisatorische Maßnahmen für den kontrollierten Zugang von Mitarbeiterinnen und Mitarbeitern zu schutzwürdigen Daten gehören.

Betroffenenrechte und Archive

Betroffenenrechte im Archiv wurden bisher in den Archivgesetzen in der Regel in zwei Weisen gewährt. Zum einen konnten Betroffene (bzw. Verwandte von Betroffenen) die betreffenden Unterlagen auf Grundlage eines entsprechenden Auskunftersuchens einsehen (Auskunftsrecht). Zum zweiten konnten sie, wenn sie die Richtigkeit von Angaben zu ihrer Person bestritten, zwar keine Änderung beantragen, aber stattdessen eine Gegendarstellung beifügen.

In der DSGVO wurden verschiedene Betroffenenrechte verankert:

- Art. 15 Auskunftsrecht (bereits in Archivgesetzen),
- Art. 16 Berichtigung (bereits in Archivgesetzen),
- Art. 18 Recht auf Einschränkung der Verarbeitung,
- Art. 19 Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung,
- Art. 20 Recht auf Datenübertragbarkeit,
- Art. 21 Widerspruchsrecht.

Diese vollständig zu erfüllen, hätte die Arbeit in Archiven zum Erliegen gebracht.¹⁵ In Art. 89 Abs. 3 DSGVO wurde deshalb die Möglichkeit geschaffen, diese Betroffenenrechte letztlich bis auf null einzuschränken (*Derogation*), wenn sie „voraussichtlich die Verwirklichung der spezifischen Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind.“ Die dafür erforderliche Umsetzung im nationalen Recht ist in Deutschland in Datenschutz- bzw. Archivgesetzen geschaffen worden.¹⁶

Grenzen der Privilegierung

Die beschriebene Privilegierung von Archiven beschränkt sich auf „im öffentlichen Interesse liegende Archivzwecke“. Damit stellt sich die Frage, welche Archive dieses Kriterium erfüllen und auch wer darüber entscheidet, ob die Kriterien erfüllt sind. Eine zusätzliche Schwierigkeit ergibt sich, weil das öffentliche Interesse in der DSGVO selbst nicht definiert ist. Nach der DSGVO sind als im öffentlichen Interesse anerkannt z. B. der Zugang der Öffentlichkeit zu amtlichen Dokumenten (Art. 86), wissenschaftliche und historische Forschungszwecke (Art. 5 und mehrfach), Funktionieren des demokratischen Systems (Art. 9) und die Ausübung von Pressefreiheit (Art. 9 und mehrfach). Für alle diese Zwecke wird bzw. muss teilweise auf archivierte Information zurückgegriffen werden können. Das bedeutet, dass weitere öffentliche Interessen (die nicht primär Archivzwecke

sind) durch die Nutzung von archivierten Informationen erreicht werden; Archive dienen damit in vielfältiger Weise dem öffentlichen Interesse, nicht zuletzt als Werkzeug der Demokratie, weil sie Daten zur Kontrolle von Verwaltungshandeln bereitstellen.¹⁷ Demnach sind Archivzwecke sowohl mittelbar als auch unmittelbar im öffentlichen Interesse.¹⁸

Grundsätzlich gäbe es zwei Varianten für die Entscheidung über die Privilegierung: Zum einen könnten Zulassungsinstanzen und -verfahren geschaffen werden, die über die „Archiv“-Eigenschaft im Sinne der DSGVO entscheiden, wie es beispielsweise in Österreich geschehen ist.¹⁹ In § 7 Absatz 3 Satz 1 Österreichisches Datenschutzgesetz heißt es zum Verfahren:

„Eine Genehmigung der Datenschutzbehörde für die Verarbeitung von personenbezogenen Daten für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke ist auf Antrag des Verantwortlichen der Untersuchung zu erteilen, wenn

1. die Einholung der Einwilligung der betroffenen Person mangels ihrer Erreichbarkeit unmöglich ist oder sonst einen unverhältnismäßigen Aufwand bedeutet,
2. ein öffentliches Interesse an der beantragten Verarbeitung besteht und
3. die fachliche Eignung des Verantwortlichen glaubhaft gemacht wird.“

Auch wenn die genannten Kriterien für die Genehmigung der Verarbeitung den Kriterien ähneln, die in Deutschland bei Schutz- bzw. Sperrfristverkürzungen angewandt werden, so ist doch der ausschlaggebende Punkt, dass hier die Entscheidung über die Genehmigung bei der Datenschutzbehörde liegt. Die in der Regel eher restriktive Herangehensweise des Datenschutzes auch an den Archivbereich ist hier zu bedenken.

Selbst wenn für die Privilegierung eines Archivs ein Verfahren mit einer Genehmigungsstelle favorisiert würde, wäre das Genehmigungsverfahren an Archivfachbehörden

14 Zum Löschungssurrogat vgl. Clemens Rehm, Löschverpflichtung und Archivierung. Ein Zwischenruf zum Löschungssurrogat, in: RuZ – Recht und Zugang. Zugang zum kulturellen Erbe und Wissenschaftskommunikation, Jahrgang 1 (2020), Heft 2, S. 219–229 und ders., Löschkultur versus Anbietungspflicht. Standortbestimmung und Perspektiven, in: Becker/Rehm/Schäfer (wie Anm. 6), S. 85–117.

15 Rehm, „Recht auf Erinnerung“ (wie Anm. 7), hier S. 56–59.

16 Eine Zusammenstellung der Begründungen für die Einschränkungen und die Würdigung der Gründe aus juristischer Sicht bei Hannes Berger, Öffentliche Archive und staatliches Wissen. Die Modernisierung des deutschen Archivrechts, Baden-Baden 2019, S. 322–335.

17 Zuletzt Christoph J. Partsch B, § 16 Rn. 10, in: ders. (Hrsg.), Handkommentar Bundesarchivgesetz, Baden-Baden 2019, S. 256 mit Verweis auf Art. 20 Abs. 2 GG. Darüber hinaus ist für diesen Gedanken Art. 19 Abs. 3 GG heranzuziehen.

18 Jakob Wührer/Martin Stürzlinger, Die DSGVO und die Folgen für die Privatarchive, in: Archiv und Wirtschaft 52 (2019), S. 26, 27f., schlagen vor, Erwägungsgrund 158 beizuziehen.

19 Datenschutzgesetz Österreich § 7; vgl. Wührer (wie Anm. 7), hier S. 29–30, 32.

– entweder im Archivgesetz oder im Datenschutzgesetz – zu binden.

Insofern hat der auf den ersten Blick weniger bestimmte Weg über Kriterien weiterhin seine Berechtigung. Dabei werden für die Nutzung der Archivprivilegien überprüfbare inhaltliche Voraussetzungen gefordert. In der aktuellen deutschen Diskussion haben sich bisher als Kriterien herauskristallisiert:

- die öffentliche Zuwendung – d. h. öffentliche Hand als Träger des Archivs oder das Archiv wird von der öffentlichen Hand gefördert –,
- ein allgemeiner, geregelter und öffentlicher Zugang, der z. B. durch eine an archivgesetzlichen Regelungen orientierte Satzung angelehnt ist und
- die Einhaltung der Bedingungen der DSGVO.

Diese Kriterien erzeugen in ihrer Kombination Wirkung: Damit fallen Privatarchive, Vereinsarchive, alle Archive mit interessegeleiteter Nutzungseinschränkung, aber auch Forschungsdatenarchive²⁰ aus der Archiv-Privilegierung der DSGVO heraus.²¹

Ein erstes Zwischenfazit

Der Geltungsbereich und die Grenzen der DSGVO bedeuten, dass sich dieses Regelwerk im Archivalltag derzeit nur auf einen kleinen Teil der bereits archivierten Unterlagen und Informationen bezieht. Personenbezogene Informationen liegen in öffentlichen Archiven überwiegend zu Verstorbenen vor, und selbst wenn sie Lebende oder kürzlich Verstorbene betreffen, ist die besondere Schutzwürdigkeit ihrer Belange den Archivarinnen und Archivaren bewusst; der postmortale Datenschutz gehört zur DNA des Archivwesens.

Zu beachten ist allerdings, dass schon jetzt, vor allem zum Zeitpunkt der Übernahme archivwürdiger Daten, digitale Personenbetriebe alltäglich sind und damit die DSGVO greift. Zudem wird mit dem weiteren Fortschreiten der digitalen Welt die Beachtung und Anwendung der DSGVO bei allen Arbeitsprozessen im Archiv zum Alltag gehören.

Privilegiert arbeiten – Neue Herausforderungen in der Archivpraxis

Für die digitale Verarbeitung von personenbezogenen Daten sind in Artikel 5 DSGVO Grundsätze aufgestellt, die auch von privilegierten Institutionen zu beachten sind. Die „im öffentlichen Interesse liegende[n] Archivzwecke“ sind in Buchstabe e) als Zweckbindung ausdrücklich genannt. Die Grundsätze der Datensparsamkeit und Datenminimierung sowie – als neue Form – die Methode der Pseudonymisierung wirken sich auf die tägliche Archivarbeit aus. Es wird von Archivarinnen und Archivaren auf diesem Feld ein geschärftes Bewusstsein für Datensensibilität zu entwickeln sein.

Im Folgenden werden einzelne Punkte beispielhaft herausgegriffen, bei denen die DSGVO im archivischen

Alltag Veränderung nach sich ziehen wird. Vollständigkeit wird dabei nicht angestrebt.

Überlieferungsbildung

Gemeinsame Verarbeitung

Nach Auffassung des Datenschutzes ist jeder Umgang mit digitalen oder digital verarbeiteten personenbezogenen Daten ein Verarbeitungsvorgang; das gilt auch für den ersten Kontakt des Archivs mit potentielltem Archivgut, die Einsicht in Daten bei einer Behörde bzw. einem Amt und die darauf erfolgende Bewertung. Da diese zu bewertenden Daten fast immer von der später abgebenden Stelle verwaltet werden, liegt eine Situation vor, dass datenschutztechnisch zwei Stellen gleichzeitig die gleichen Daten verarbeiten. Für den Datenschutz ist das eine problematische Situation, weil nicht geklärt ist, wer „Verantwortlicher“ (vgl. Artikel 4 Nr. 7 DSGVO) für die Daten ist und z. B. Auskunft an Betroffene gibt. Es bedarf daher einer Regelung, um die Verarbeitung der Archive in den Registern und an den Datenbanken (z. B. zur Vorbereitung eines Datenschnitts) zu erlauben. Das kann über einzelne Vereinbarungen zwischen Archiv und Behörde geschehen, was sich aber als aufwändig erweisen wird. Eine Alternative bestünde darin, mit Rückgriff auf Artikel 26 DSGVO „Gemeinsame Verantwortliche“ in einer gesetzlichen Lösung die Zuständigkeit für einzelne Verarbeitungsprozesse an gleichen Daten festzulegen: Die für die Aufgabenerledigung notwendige Verarbeitung verantwortet die Verwaltung; Einsichtsrecht und Bewertung werden dem Archiv eingeräumt. Dieser Punkt wäre bei künftigen Archivgesetznovellierungen zu beobachten.²²

Datensparsamkeit / Datenminimierung

Die Privilegien für Archive in der DSGVO werden stets von der Bedingung begleitet, dass sie gelten, „soweit das in Absatz 1 genannte Recht [i. e. Verlangen auf Löschung] voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt“ (Artikel 17 Absatz 3d). Damit wird von den Archiven verlangt, begründen zu können, zu welchen Zwecken welche Daten übernommen wurden. Das dürfte auf der Grundlage einer transparenten Bewertungsentscheidung im Regelfall gelingen. Zudem wurde mit dem Zusatz „voraussichtlich“ aus-

20 Zur Diskussion um die Forschungsarchive vgl. Clemens Villinger/Kathrin Zöller, Tagungsbericht: Sind das Daten und muss das (deshalb) weg?: Rechtliche und ethische Grundlagen zeithistorischer Forschung mit Sozialdaten, 05.10.2020 – 06.10.2020 Bad Homburg und digital, in: H-Soz-Kult, 15.12.2020, <https://www.hsozkult.de/conferencereport/id/tagungsberichte-8839>.

21 Vgl. Wührer/Stürzlinger (wie Anm. 18), S. 26–31; Hense (wie Anm. 12) Art. 89 Rn. 17, S. 1499 f.: „Bei privaten Archiven (Archive von nicht öffentlichen Stellen) wird es auf die Ein[zel]fallumstände ankommen; private Unternehmensarchive werden im Zweifel vielleicht eher nicht umfasst sein.“ Klar die privaten Archive von Wirtschaftsunternehmen ausgrenzend Jakob Nolte, in: Sibylle Gierschmann u. a. (Hrsg.), Kommentar Datenschutzgrundverordnung, Art. 89 Rn. 17, S. 1483.

22 Dazu auch Jakob Wührer, Überlieferungsbildung im Schatten oder Windschatten der DSGVO? Die EU-DSGVO als Basis für die archivische Überlieferungsbildung im 21. Jahrhundert, in: Scrinium 74 (2020), S. 58–86.

gedrückt, dass nicht sicher prognostizierbar ist, welche Informationen zu welchen Zeiten tatsächlich genutzt werden. Die Jahrzehnte nach Entstehung und Übernahme erfolgreichen Nutzungen von personenbezogenen Informationen z. B. für die Entschädigung von ehemaligen Zwangsarbeitern oder zur Aufarbeitung der Heimerziehung sind hier einschlägige Beispiele. Zudem sind sie ein Beleg dafür, dass die Archivierung personenbezogener Daten im Interesse Betroffener sein kann.²³

Für die Übernahme von besonderen Kategorien personenbezogener Daten – u. a. zu ethnischer Herkunft, politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen, sowie genetischen und biometrischen Daten, Gesundheitsdaten, Daten zur sexuellen Orientierung²⁴ – ist von den Archiven wegen der hohen Sensibilität dieser Daten nachzuweisen, dass die archivische Verarbeitung „erforderlich“ ist. Auch das wird mit Hinweis auf absehbares Forschungsinteresse möglich sein.

Speicherung

Bei diesem Arbeitsfeld ist mit Blick auf die Praxis der digitalen Speicherung auf einen Regelungsbedarf hinzuweisen. Die gemeinsame Archivierung/Speicherung mehrerer Stellen in einer Einrichtung, die Speicherung bei Dritten (z. B. Kommunalarchive bei Kreisarchiven) und das Speichern für Dritte (z. B. Kreis für Kommune) bedarf klarer, DSGVO-konformer Regelungen. Dabei ist immer zu klären und zu fixieren, welche Institution für welche Verarbeitungsschritte – von der Bewertung über die Erschließung bis zur Zugänglichmachung – und wer als Daten-Verantwortlicher für das Auskunftersuchen zuständig ist. Das kann über die Vereinbarungen zur Auftragsdatenverarbeitung gelöst werden.²⁵ Hier wäre auch vorstellbar, eine Art Auffangregelung u. a. unter Rückgriff auf Artikel 26 DSGVO in den Archivgesetzen zu verankern.

Erschließung

Bei der Erschließung werden die Grundsätze der Datenminimierung und Datensparsamkeit verlangt. Nun stehen Personen in sehr vielen archivischen Nutzungsszenarien im Fokus des Interesses und eine Unterdrückung von Namen bei der Erschließung wäre im Hinblick auf die Archivzwecke kontraproduktiv. Allerdings wird in der DSGVO, vor allem im Hinblick auf künftige rein digitale Überlieferungen, die Pseudonymisierung²⁶ als Form des Zugangs von personenbezogenen Informationen ausdrücklich im Zusammenhang mit der Privilegierung der Archive genannt.²⁷ Definiert wird Pseudonymisierung in (Artikel 4 Nr. 5 DSGVO):

„Im Sinne dieser Verordnung bezeichnet der Ausdruck [...] ‚Pseudonymisierung‘ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und tech-

nischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden [...].“

Die Pseudonymisierung ermöglicht, dass personenbezogene Daten unterschiedlicher Herkunft ohne Verwendung des Klarnamens dennoch zusammengeführt und z. B. für Forschungszwecke ausgewertet werden können. Gleichzeitig ist gewährleistet, dass in anderen Kontexten die Klarnamen über einen Schlüssel dem Pseudonym wieder zugeordnet werden können.

Das Verfahren ist Archiven grundsätzlich nicht unbekannt. Wenn die Auswertung von Unterlagen, die einer Schutzfrist unterliegen, nur in anonymisierter Weise erfolgen darf, verschlüsselt der Forschende und verwendet Pseudonyme wie „Max N.“. Durch die DSGVO wird dieser Prozess bei digitalen Daten um eine Ebene verschoben: Das Archiv – oder eine andere Instanz – vergibt die Pseudonyme (einen „Schlüssel“) und der Nutzer bzw. die Nutzerin kann damit ohne weitere Prozesse arbeiten.²⁸ Mit den unterschiedlichen Verfahren – digitale Schlüssel, kryptografische Verfahren – wird sich das Archivwesen in den nächsten Jahr(zehnt)en näher beschäftigen müssen.

Zugänglich machen/verbreiten

Mit dem Einzug des Digitalen hat sich auch die Zugänglichmachung von Daten verändert; eine Präsentation von Findmitteln im Netz wird inzwischen als Standard angesehen. Die einfachste Transformation besteht darin, vorliegende Findmittel und Findbehelfe wie Ablieferungslisten ins Netz zu stellen. Fragen kommen dabei von zwei Seiten: Zum einen verlangen Datenschützer und Datenschützerinnen vermehrt eine Ermächtigung für Archive, personenbezogene Daten online zu stellen, und zum anderen sind viele Erschließungsdaten zu gut, sprich zu detailliert, um online gestellt zu werden. Dem Verlangen des Datenschutzes nach einer rechtlichen Grundlage ist am ehesten zu begegnen, indem eine entsprechende Ermächtigung im

23 Zur Sicherung im Interesse von Betroffenen vgl. Clemens Rehm, Recht auf Erinnerung: Rechtssicherung durch Überlieferungsbildung, in: Claudia Kauertz (Red.), Archive im Rechtsstaat. Zwischen Rechtssicherung und Verrechtlichung, 51. Rheinischer Archivtag 2017 in Essen (Archivhefte, Schriftenreihe des Landschaftsverbands Rheinland 49), Bonn 2018, S. 43–61.

24 Vgl. Artikel 9 Absatz 1 DSGVO.

25 Dazu Christian Reinhardt, Archivrechtliche Anforderungen an die Digitalisierung von Personenstandsregistern und die Veröffentlichung der Digitalisate im Internet, in: Monika Storm (Hrsg.), Neue Wege ins Archiv: Nutzer, Nutzung, Nutzen. 84. Deutscher Archivtag 2014 in Magdeburg (Tagungsdokumentation zum Deutschen Archivtag 19), Fulda 2016, S. 181–189; dazu auch Andreas Hedwig, Perspektive Familienforschung, in: Archivnachrichten aus Hessen 19/2 (2019), S. 10–13.

26 Vgl. David Gniffke, Pseudonymisierung in der DSGVO. Grundlagen und Folgen für Überlieferungsbildung und digitale Langzeitarchivierung, Marburg 2020; https://landesarchiv-bw.de/sixcms/media.php/120/Transferarbeit2020_Gniffke.pdf.

27 „Zu diesen Maßnahmen kann die Pseudonymisierung gehören, sofern es möglich ist, diese Zwecke auf diese Weise zu erfüllen.“ Artikel 89, Absatz 1 Satz 3 DSGVO.

28 Zu den unterschiedlichen Verfahren vgl. Gniffke, wie Anm. 26.

Archivgesetz verankert wird. Als frühes Beispiel kann § 8 Abs. 1 Bremisches Archivgesetz herangezogen werden, in dem die Veröffentlichung und Weitergabe von Archivalien sowie Findmitteln geregelt wird. Satz 1 hebt die Onlinepräsentation auf die Ebene eines gesetzlichen Auftrags:

„Um der Öffentlichkeit den Zugang zu historischen und familienkundlichen Unterlagen zu ermöglichen oder zu erleichtern, ist das Staatsarchiv berechtigt, Archivgut, Reproduktionen von Archivgut und die dazu gehörigen Findmittel im Rahmen seiner gesetzlichen Aufgaben zu veröffentlichen.“

In Satz 2 werden die bekannten schutzwürdigen Belange betroffener Personen als Entscheidungskriterium über die Online-Stellung eingeführt:

„Durch die Veröffentlichung dürfen keine überwiegenden schutzwürdigen Belange betroffener Personen oder Dritter beeinträchtigt werden; insoweit sind insbesondere auch die Art, die Form und die Zugänglichkeit der Publikation zu berücksichtigen.“

In Satz 3 wird für den Teil der „besonderen Kategorien personenbezogener Daten“ (Artikel 9 DSGVO), der genetische Informationen enthält, der Kreis der Betroffenen um zwei Generationen erweitert. Eine Online-Stellung genetischer Daten ist nicht erlaubt, wenn Belange der Kinder- bzw. Enkelgeneration betroffen sein können:

„Biometrische oder genetische Daten im Sinne von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 dürfen nicht veröffentlicht werden, wenn Belange betroffener Personen berührt sein könnten. Im Fall genetischer Daten gilt dies auch für die Belange von leiblichen Kindern oder Kindeskindern betroffener Personen.“

Je mehr solche Daten in die Archive gelangen – und das dürfen sie auch nach Geltung der DSGVO –, desto intensiver wird sich das Archivwesen mit den Grenzziehungen beschäftigen müssen. Deutlich ist aber auch, dass die Ausweitung der Belange Betroffener um zwei Generationen sich auf einen sehr klar umgrenzbaren Bereich bezieht und auf andere Daten nicht beliebig ausgedehnt werden kann.²⁹

Vertrauen erhalten

1994 stellte die amerikanische Archivarin Elsie Freeman Finch ihrem Plädoyer für die Öffnung der Archive das Motto voran „We acquire, preserve, and maintain archives, so that they will be used by anyone who seeks to use them, for whatever reason.“³⁰ Dieser Weg der Nutzerorientierung gegen alle „Gatekeeper“-Tendenzen sollte allumfassend („for whatever reason“) sein. Im 21. Jahrhundert, in dem die Auswirkungen von Informationen im Netz immer deutlicher sichtbar sind, stellt sich die Frage, ob diese bedingungslose Zugänglichmachung tatsächlich ein Ziel bleiben

kann. Es geht dabei im Kern darum, ob Archive auf diesem Feld alles machen sollten, was sie rechtlich dürften.

Anders als bei selbstbestimmt in sozialen Netzwerken veröffentlichten persönlichen Daten steigt die Sensibilität für öffentliche persönliche Daten, die von Dritten publiziert werden. Entsprechend werden Archive mit Löschforderungen von online stehenden Erschließungsdaten konfrontiert. Anhand von drei Beispielen sollen mögliche Vorgehensweisen von Archiven skizziert werden. In allen Fällen waren bei der Online-Stellung die archivgesetzlichen Regelungen und die Empfehlungen der damaligen Archivreferentenkonferenz zur Online-Stellung von Erschließungsdaten³¹ beachtet worden.

Website

Ein Dozent einer Universität verlangte die Löschung aller seiner Daten, die auf einer archivierten Website der Universität zugänglich waren. Die von der Universität 1:1 in das digitale Archiv übernommene und präsentierte Seite enthielt den Namen des Dozenten, die Themen seiner Vorlesung, seine Zimmernummer, seine Telefonnummer und ein Bild des Dozenten, das von ihm für die Website der Universität zur Verfügung gestellt worden war.

Die Angaben zu Vorlesung, Zimmernummer etc. beschrieben seine amtliche Funktion und waren öffentlich zu halten. Anders stellte sich die Lage bei dem Bild heraus, weil die Universität von dem Dozenten nur die Zustimmung für die aktuelle Onlinepräsentation erbeten hatte, nicht aber für die Weitergabe zum Zweck einer späteren Archivierung. Damit überwog hier das Recht am eigenen Bild und das bewirkte – anders als bei den Daten – die Löschung des Bildes durch das Archiv.

Diese Konstellation verweist auf ein grundsätzliches Problem. Viele Ämter und Dienststellen lassen Erklärungen über die Verarbeitung der Daten von Betroffenen unterschreiben, ohne darauf hinzuweisen, dass die Daten auch archiviert werden könnten. Manches Amt hat aus diesem Fehlen einer solchen Passage – unzulässiger Weise – abgeleitet, dass damit keine Abgabe an ein Archiv möglich ist. Dem ist entgegenzuhalten: Die fehlende Aufklärung kann kein geltendes Gesetz aushebeln. Dennoch wäre in solchen Fällen den Betroffenen vorgelegten Erklärungen zur Datenverarbeitung ein hinweisender Satz wünschenswert wie z. B. „personenbezogene Daten können ggf. gemäß Landesarchivgesetz verarbeitet werden“.

29 Dieser Sachverhalt begrenzt auch weitergehende Forderungen von Seiten des Datenschutzes gegenüber Archiven, wie sie von Kai Engelbrecht, Gläserne Abstammung?, in: Die öffentliche Verwaltung 10 (2017), S. 393–403 vorgetragen wurden.

30 Elsie Freeman Finch (Hrsg.) *Advocating Archives*, Metuchen/ N. J. und London 1994, S. 1 (Hervorhebung im Original).

31 Archivreferentenkonferenz des Bundes und der Länder, Bereitstellung elektronischer Findmittel in öffentlich zugänglichen Netzen, 20.03.2007 (<https://www.bundesarchiv.de/DE/Content/Artikel/Ueber-uns/Partner/KLA/kla-ausschuss-aur.html>).

Öffentlich gesendeter Fernsehbeitrag

Eine Betroffene hatte sich an einen Fernsehsender gewandt, um mit einer öffentlichen Darstellung über die Entführung ihres Kindes durch den Vater ins Ausland Zugang zu diesem Kind, im besten Fall dessen Rückführung, zu erreichen. Die Magazinsendung mit einem Interview mit der Betroffenen war archiviert worden; das Findbuch mit dem Namen der Betroffenen, der im Fernsehbeitrag auch genannt und gesendet worden war, stand online. Die Betroffene verlangte die Löschung des Findbucheintrags, weil sich die Sache inzwischen erledigt hätte und sie den privaten Sachverhalt nicht länger öffentlich zugänglich sehen wollte.

Da in allen deutschen Archivgesetzen verankert ist, dass öffentlich gewesene (bzw. für die Öffentlichkeit vorgesehene) Daten im Nachhinein im Archiv keiner Sperrung unterliegen,³² erfolgte eine Prüfung. In diesem Fall stellte sich heraus, dass diese Entführungsgeschichte im Netz ausschließlich im Findmittelsystem des angefragten Archivs aufzufinden war. Bei der Abwägung von privatem und öffentlichem Interesse wurde entschieden, dass der Sachverhalt als solcher durchaus auffindbar sein sollte, um Forschungen nicht einzuschränken; dieser Zugang benötigte aber weder den Namen der Betroffenen noch den Namen des (sehr kleinen) Ortes, an dem das Ereignis stattgefunden hatte. Daher wurden der Datensatz im Findmittelsystem belassen, aber anonymisiert, d. h. der Name des Betroffenen und der Ortsbezug wurden entfernt. Der Fernsehbeitrag selbst blieb selbstverständlich unverändert.

Akte außerhalb der Schutz- bzw. Sperrfrist

In den letzten Jahren wurde immer wieder öffentlich darüber gestritten, ob Namen von Opfern des Nationalsozialismus auf Denkmälern und im Internet, z. B. auf Gedenkseiten von Archiven, präsentiert werden dürften.³³ Diese Debatte hat durch die im Netz umfangreich vorhandenen Personendaten und die intensive Nutzung von sozialen Netzwerken noch einmal an Brisanz gewonnen. Bisher verhielten sich v. a. Nachfahren von Opfergruppen reserviert, weil sie durch die öffentliche Namensnennung eine erneute Diskriminierung befürchteten; das galt gerade für Familien, deren Angehörige im Rahmen der sogenannten Aktion T4 ermordet worden waren.

Inzwischen entwickeln auch Daten aus Archivgut für jederfrau und jedermann durch die mögliche Verschneidung mit anderen im Netz verfügbaren eine neue Dynamik. So erhielt ein Archiv die Löschforderung zu Erschließungsdaten zu einer Spruchkammerakte und zu einem Strafverfahren wegen Missbrauchs von Minderjährigen, die beide seit Jahrzehnten außerhalb von Schutz- bzw. Sperrfristen lagen. Es ging aber nicht um postmortalen Datenschutz. Zwar waren die Betroffenen verstorben, aber in beiden Fällen wurde mit den Auswirkungen auf die noch lebenden Nachfahren argumentiert. Im Fall der Spruchkammerakte hatte der Enkel – wie vielfach üblich – den Vornamen seines Großvaters erhalten; da der Familienname sehr selten war, führte die Suche nach dem im

Berufsleben stehenden Enkel regelmäßig zu der Spruchkammerakte seines Großvaters.

Dieser Wunsch nach Namenslöschung wurde abgelehnt, weil die Existenz einer Spruchkammerakte nicht per se diskriminierend ist, das Archiv aufgrund seines Transparenzauftrags keinen Täterschutz fördern darf und schließlich aufgrund der Lebensdaten keine echte Verwechslungsmöglichkeit bestand.

Etwas anders lag der Fall bei dem verurteilten Vergewaltiger. Auch hier war aufgrund des Namens und des Ortes ein direkter Bezug zu den Nachfahren herstellbar. Hier war das allgemeine öffentliche Interesse abzuwägen mit der Frage, ob und inwieweit der digital vorliegende Tat-Sachverhalt mit Strafurteil in Kombination mit dem Familienbezug zum Schaden der Nachfahren verwendet werden könnte. Dabei waren bei online stehenden Daten deren leichte und weite Verbreitungsmöglichkeit für inzwischen bekannte Phänomene wie *Cybermobbing* unter Jugendlichen einzubeziehen.³⁴ Da die wissenschaftliche Forschung sowie die regionale Forschung nicht behindert wird, wenn der Name des Täters im Netz entfällt, dagegen eine missbräuchliche Verwendung ausgeschlossen wird, wurde bei der Onlinepräsentation auf den Namen verzichtet.

Ein zweites Zwischenfazit

In allen Fällen geht es um nach rechtlicher Prüfung im Netz öffentlich zugänglich gemachte Erschließungsdaten mit Personennamen. Die vorgestellten Beispiele stehen für Abwägungen zum erweiterten Datenschutz im Archiv. Innerhalb der archivischen Mauern, d. h. im Lesesaal, sind diese Fragen rechtlich eindeutig geklärt und – wie die Praxis der letzten Jahrzehnte zeigt – unproblematisch. Bei der Nutzung vor Ort können diese Unterlagen unter entsprechenden Auflagen unverkürzt genutzt werden. Bei der Entwicklung der Archivgesetze und auch bei den letzten Novellierungen waren aber die enormen digitalen Verbreitungsmöglichkeiten mit erheblicher Reichweite und die unbeschränkten Verknüpfungsmöglichkeiten noch nicht bis ins Letzte mitgedacht. Die 1994 geäußerte Vision „for whatever reason“ kann heute so nicht mehr uneingeschränkt gelten. Archivarinnen und Archivare haben eine Mitverantwortung für das, was mit den von ihnen öffentlich bereitgestellten Daten missbräuchlich ange stellt werden kann. Und das bedeutet, sich zu überlegen,

32 Axer, Handbuch (wie Anm. 9), S. 145.

33 Vgl. Ehrhart Körting Persönlichkeitsrecht und Archivrecht, in: Archive im Rechtsstaat (wie Anm. 18), S. 126–131; Vinzenz Lübben, Stolperfallen im Netz: postmortaler Persönlichkeitsschutz und die Belange von Hinterbliebenen, in: Becker/Rehm/Schäfer (wie Anm. 6), S. 151–169 und ders., Nutzung und Veröffentlichung personenbezogener Daten im Rahmen von Erinnerungs- und Gedenkarbeit, in: Archivpflege in Westfalen-Lippe 95 (2021), S. 12–20.

34 Cybermobbing ist kein Randphänomen. Nach der JIM-Studie von 2016 sind acht Prozent der jugendlichen Internetnutzer bzw. -nutzerinnen zwischen 12 und 19 Jahren bereits Opfer von Cybermobbing gewesen; 34 Prozent der Befragten haben jemanden im Bekanntenkreis, der durch Cybermobbing fertiggemacht wurde; vgl. Bundesministerium für Familie, Senioren, Frauen und Jugend <https://www.bmfsfj.de/bmfsfj/themen/kinder-und-jugend/medienkompetenz/was-ist-cybermobbing--86484>.

wie und welche Daten im Netz präsentiert werden sollten – und welche Kriterien dafür zusätzlich zu der gesetzlichen Grundlage entwickelt werden könnten.

Das wird vermutlich in erster Linie Auswirkung auf die Erschließung und die Überlieferungsbildung haben. Wenn die *Erschließung* von ihrer Wirkung auf Lebende bzw. auf die Verwendungsmöglichkeit her gedacht wird, ist das Risiko eines möglichen Missbrauchs bei Online-Stellung einzubeziehen: Es wäre zu überlegen – weitergehend als bei der bisher üblichen Verlängerung der Schutzfristen bei Netzpräsentationen –, Namen oder andere Merkmale zur Identifikation von Personen in der zentralen, online verfügbaren Erfassungsinformation wie der Titelaufnahme zu vermeiden oder zu anonymisieren (z. B. „Einzelfälle Aa–Ae“) und die Detailangaben nur kontrolliert zugänglich zu machen.

Bei der *Überlieferungsbildung* soll an dieser Stelle nur auf den digitalen Sammlungsbereich verwiesen werden. Selbstverständlich muss es Ziel der Archive sein, rechtlich und technisch im Stande zu sein, Social-Media-Kanäle, Websites von Initiativen und handelnden Personen (Politik, Wirtschaft, ...), Blogs etc. zu archivieren; erste Erfolge sind hier schon greifbar.³⁵ Aber auch bei diesen Medien, die stets vorher öffentlich zugänglich waren, ist die Auswirkung einer späteren archivischen Präsentation zu bedenken. Während Informationen im Netz schon nach wenigen Tagen durch die nachfolgende Flut neuer Informationen verdrängt und vergessen sind, werden sie in archivierter Form (erneut) durchsuchbar und können noch nach Jahren direkte Auswirkungen auf das aktuelle Geschehen haben.³⁶

Archive tragen bei der Präsentation von Informationen aus Archivgut im Netz eine Mitverantwortung für die Folgen der Nutzung. Auch von ihnen wird verlangt, sich mit den Gedanken auseinanderzusetzen, die in der DSGVO Artikel 35 als Datenschutz-Folgenabschätzung (*Dataprotect – Impact Assessments*) eingeführt werden: „Grundsätzlich ist die Datenschutz-Folgenabschätzung immer dann durchzuführen, wenn die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.“³⁷

Ausblick: Vertrauen erhalten

Der rechtliche Rahmen für die archivische Arbeit ist durch die DSGVO mit dem enthaltenen „Recht auf Erinnerung“ grundsätzlich besser verankert; die stärkere Absicherung und Privilegierung zieht aber auch eine höhere Sensibilität in der täglichen Arbeit nach sich. Nachjustierungen werden in den nächsten Jahren vermutlich bei der Absicherung der Onlinepräsentation von Archivdaten, des Zugangs zu Daten in der Verwaltung, dem digitalen Sammlungsauftrag und der Definition der „Archivzwecke im öffentlichen Interesse“ erfolgen.³⁸

Die Privilegierung wird aber auch dazu führen, sich mit neuen Methoden wie der Pseudonymisierung, der Anpassung der Erschließung für die Online-Stellung und der Verantwortung der Archive für, die von ihnen verbreiteten Da-

ten (Datenschutz-Folgenabschätzung) intensiv im Alltag sowie in Aus- und Fortbildung zu beschäftigen.

Archive sind Institutionen von hoher Glaubwürdigkeit, nicht zuletzt, weil die Sicherung authentischer Informationen einer ihrer Aufträge ist, den sie ernst nehmen und seit Jahrzehnten erfolgreich umsetzen. Datenintegrität und Datensicherheit sind die Voraussetzung, dass ihnen Behörden, Dienststelle, Institutionen wie Vereine und Privatpersonen Unterlagen und Informationen anvertrauen. In diesen Bereichen Fehler zu machen, erschüttert das in die Archive gesetzte Vertrauen massiv. „Vertrauen erhalten“ ist daher zum einen eine Beschreibung dessen, was den Archiven entgegengebracht wird – und zugleich ist es ein Auftrag, in dem neuen Kosmos, der mit der DSGVO aufgespannt worden ist, weiterhin als sichere Datenhäfen und nicht als verantwortungslose Datenkraken ihren Alltag zu gestalten. Dann können Archive als für die Demokratie konstitutive, unverzichtbare Gedächtnisinstitutionen gegen eine gesellschaftliche Amnesie durch Löschung selbstbewusst(er) auftreten. ■



Dr. Clemens Rehm
Landesarchiv Baden-Württemberg, Stuttgart
clemens.rehm@la-bw.de

35 Z. B. Blogs zu „Stuttgart 21“ im Landesarchiv Baden-Württemberg, J 126 Webdokumentation Stuttgart 21 (Intranet). Die Aktivitäten von Befürwortern und Gegnern des Projekts fanden spätestens seit 2010 reichhaltigen Niederschlag im Internet. Die Archivierung der einzelnen Webseiten wurde mit den Domaininhabern/Webseitenbetreibern vertraglich vereinbart. Erste Spiegelungen von Seiten des Landesarchivs erfolgten im April/Mai 2013.

36 Vgl. Stefanie Witterauf/Laura Dahmer, Jugendsünden im Netz: „Wir haben früher alle dumme Dinge getan und gesagt“, in: DIE ZEIT, 18.10.2021, <https://www.zeit.de/zett/politik/2021-10/jungpolitiker-social-media-jugendsuenden-netz-umgang-digitale-vergangenheit>.

37 „Mit der EU-Datenschutz-Grundverordnung wird das Instrument der Datenschutz-Folgenabschätzung (DSFA) eingeführt (Art. 35 EU-DSGVO).“ <https://dsgvo-gesetz.de/themen/datenschutz-folgenabschaetzung/>.

38 Zur Diskussion des neuen Terminus vgl. Clemens Rehm, Landesdatenschutzgesetz Baden-Württemberg. Kommentar zu § 10, § 14, in: Alfred G. Debus (Hrsg.), Handkommentar LDSG Baden-Württemberg, Baden-Baden [Erscheinen 2022 vorgesehen].