Transferarbeit im Rahmen der Laufbahnprüfung für den höheren Archivdienst an der Archivschule Marburg (53. wissenschaftlicher Lehrgang)

Pseudonymisierung in der DSGVO

Grundlagen und Folgen für Überlieferungsbildung und digitale Langzeitarchivierung

Von David Gniffke
(Landesarchiv Baden-Württemberg)

Betreuung:
Dr. Clemens Rehm, Landesarchiv Baden-Württemberg
Dr. Irmgard Christa Becker, Archivschule Marburg

Vorgelegt am 1. April 2020

Zusammenfassung

Die am 25. März 2018 in Kraft getretene Datenschutzgrundverordnung (DSGVO) unterwirft auch die Archive einer Einhaltung von technischen und organisatorischen Maßnahmen bei der Verarbeitung personenbezogener Daten und schlägt dafür insbesondere die Pseudonymisierung vor. Die vorliegende Arbeit nimmt erstmals ausführlicher die Grundlagen und Auswirkungen der Pseudonymisierung aus archivischer Perspektive in den Blick.

Die Betrachtung der Definition in Zusammenhang mit den Regelungen in der gesamten DSGVO, den Datenschutz- und Archivgesetzen ergab einen nicht unerheblichen Einfluss, besonders auch auf die Bestandsbildner. Unter Berücksichtigung der technischen und organisatorischen Umsetzungen der Pseudonymisierung wurden Überlegungen zu den Auswirkungen auf die Überlieferungsbildung und digitale Archivierung angestellt.

Die Entscheidung zur Pseudonymisierung und ihre konkrete Umsetzung werden stets durch die Rahmenumstände des Einzelfalls bestimmt, weshalb sich mögliche Konsequenzen kaum generalisieren lassen. Neben dem Bedarf einer Erforderlichkeitsprüfung für ihren Erhalt ist die Übernahme der Zuordnungsregel von der genauen Kenntnis der technischen und organisatorischen Umsetzung in der Behörde abhängig. Es wird vorgeschlagen, pseudonymisierte und nicht pseudonymisierte Daten wie angeboten zu speichern und eigene Rechte- und Rollenkonzepte für das Archiv zu entwickeln. Die Entwicklungen bei den Bestandsbildnern verdienen eine wachsame Beobachtung und Begleitung.

Gliederung

I. Einleitung

Die seit dem 25. Mai 2018 geltende Datenschutzgrundverordnung (DSGVO, auch Verordnung 2016/679), verabschiedet am 14. April 2016, hat im Vorfeld für eine Menge Wirbel und Verunsicherung gesorgt. Noch mehr als das Archivwesen waren und sind die Bestandsbildner davon betroffen. Mitunter kam es zu offenen Aufforderungen, Daten zu löschen, trotz der Kenntnis archivgesetzlicher Regelungen.[1] Die Bekanntheit der DSGVO hat vor allem die Androhung und Durchsetzung hoher Bußgelder befördert. Besondere Popularität erlangte das sogenannte „Recht auf Vergessenwerden" im Zuge eines Urteils gegen Google im Jahr 2014, das das Auffinden per Suchmaschine von sozial diskreditierenden Zeitungsberichten eines spanischen Klägers unterband.[2]

Der Anwendungsbereich der DSGVO ist in seinen Auswirkungen auf das Archivwesen beträchtlich: Sie erstreckt sich auf die personenbezogenen Daten aller lebenden natürlichen Personen.[3] Anders als eine EU-Richtlinie gilt eine EU-Verordnung unmittelbar, ohne dass die Mitgliedstaaten sie erst in nationales Recht umsetzen müssten, hier für öffentliche und nichtöffentliche Stellen.[4] Nicht erfasst werden mit Art. 2 Abs. 2 DSGVO Tätigkeiten außerhalb des Anwendungsbereichs des Unionsrechts (lit. a)[5] oder persönlich-private

---

1 Beispielsweise wurden in Belgien die Archive von Datenschutzbeauftragen vorgeladen mit der Aufforderung, „alle persönliche Informationen enthaltenden Dokumente, die keinen administrativen Nutzen mehr haben, zu vernichten, selbst wenn das Archivgesetz und die Schriftgutbewertungsverzeichnisse die Aufbewahrung besagter Dokumente vorschreiben", vgl. van Honacker: EU, S. 27f; Pahl: Archivrecht, S. 38 (für die ausführlichen Literaturangaben siehe auch im Folgenden das Literaturverzeichnis).

2 Siehe das Urteil EuGH v. 3. Mai 2014, C131/12, EU:C:2014:317. Zuletzt erfolgte auch ein Beschluss des Bundesverfassungsgerichts (Urteile 1 BvR 16/13; 1 BvR 276/17) zu einem ähnlichen Sachverhalt: „Axel L." hatte nach Mord und Körperverletzung über 20 Jahre Gefängnisstrafe abgebüßt und sich resozialisiert – dennoch waren in Online-Archiven der Zeitungsverlage bei Eingabe seines Namens die Berichte über seinen Mordprozess zu finden. Der erste Senat entschied schließlich unter anderem, dass Betroffene in solchen Fällen die Berichte beanstanden müssen, die Betreiber der Online-Archive dann ein zielgerichtetes Auffinden dieser Berichte technisch verhindern sollen, vgl. Krüger: Vergesst ihn (für den Hinweis danke ich Dr. Irmgard Christa Becker, Marburg).

3 Vgl. ausdrücklich ErwG 27 DSGVO. Die Zugangsgewährung im Kontext der DSGVO ist daher immer ein Eingriff in das informationelle Selbstbestimmungsrecht, vgl. nur Keitel: Aussonderung, S. 73. Das Konzept eines postmortalen Persönlichkeitsschutzes und Schutzfristen auf personenbezogene Daten Verstorbener in deutschen Archivgesetzen gehen in ihrer Schutzwirkung noch weiter als die DSGVO, vgl. Steinert: Datenschutz, S. 7.

4 Vgl. BfDI: DSGVO - BDSG, S. 14–16; die Einflussmöglichkeit der EU auf eine Harmonisierung des Datenschutzes im Archivwesen leitet sich dabei weder aus der Kulturkompetenz noch der Forschungskompetenz, sondern aus den Tätigkeiten der Bestandsbildner ab, die regelmäßig unter den Anwendungsbereich des Unionsrechts fallen, vgl. Art. 2 Abs. 2 lit. a DSGVO; Berger: Öffentliche Archive, S. 96–110.

5 Dazu zählen etwa auch Nachrichtendienste, Verteidigung und Verfassungsorgane wie der parlamentarische Bereich des Deutschen Bundestages, vgl. BfDI: DSGVO - BDSG, S. 17, sofern die Regelungen

Verarbeitungen wie Adressbuchführung (lit. c), darüber hinaus aber auch nicht Verarbeitungen im Rahmen von Tätigkeiten der Sicherheits- und Außenpolitik (lit. b) sowie die über die sogenannte JI-Richtlinie (EU 2016/680) geregelten Bereiche Justiz und Inneres (lit. d).[6] Letztere fallen dann wieder unter die DSGVO, wenn mit Erlaubnis aus Unionsrecht oder Recht der Mitgliedstaaten eine Verarbeitung u. a. zu im öffentlichen Interesse liegenden Archivzwecken stattfindet.[7]

Sachlich hat die DSGVO zwar die „ganz oder teilweise automatisierte Verarbeitung" im Blick, bezieht sich aber ebenfalls auf „nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen".[8] Dabei ist unter „Dateisystem" nicht zwingend eine elektronische Ablage gemeint, sondern jede strukturierte Sammlung, die eine Verwaltung von Daten ermöglicht.[9] Insofern zählt darunter auch Archivgut, sofern es nach personenbezogenen Kriterien ausreichend erschlossen oder auch nur geordnet ist und sich auf personenbezogene Daten bezieht.[10]

Sind nun alle Verarbeitungen in diesem großen Anwendungsbereich dem „Recht auf Vergessenwerden" unterworfen? Mittlerweile dürfte bekannt sein, dass die DSGVO die Arbeit der Archive nicht ad absurdum führt. Dem „Recht auf Vergessenwerden" steht ein „Recht auf Erinnerung" entgegen, etwa im Rahmen berechtigter Belange betroffener Personen oder der Pflege kultureller Identität.[11] Zurecht privilegiert Art. 89 der DSGVO unter anderem „im öffentlichen Interesse liegende Archivzwecke", indem dieser es Mitgliedsstaaten möglich macht, diverse Artikel zu den Rechten betroffener Personen, die eine

---

nicht über bereichsspezifisches Datenschutzrecht oder das BDSG n.F. wieder eingeführt werden, ebenso (Landesverfassungsschutzbehörden) bei den Ländern, vgl. ebd., S. 18.

6 Vgl. BfDI: DSGVO - BDSG, S. 17.

7 Vgl. Art. 4 Abs. 3 iVm Art. 9 Abs. 1 und 2 Richtlinie EU 2016/680.

8 Vgl. Art. 2 Abs. 1 DSGVO.

9 Vgl. Art. 4 Nr. 6 DSGVO; sie soll „technologieneutral" gelten, vgl. ErwG 15 DSGVO; Schreiber, in: Plath DSGVO/BDSG, Art. 4, Rn. 24; Schwartmann/Hermann, in: Schwartmann/Jaspers/Thüsing, DSGVO/BDSG, Art. 4, Rn. 89–97; Gola, in: Gola DSGVO, Art. 4, Rn. 43f; dagegen Schlagk: Die datenschutzrechtliche Privilegierung, S. 40. Einige Datenschutzgesetze weiten die Geltung auch auf personenbezogene Daten außerhalb von Dateisystemen aus, vgl. § 2 Abs. 4 ThürDSG.

10 Schwartmann/Hermann, in: Schwartmann/Jaspers/Thüsing, DSGVO/BDSG, Art. 4, Rn. 96. Es steht außer Frage, dass somit die meisten der unter Art. 4 Nr. 2 DSGVO genannten Verarbeitungsformen auf die Bestandsbildner und die Archive zutreffen.

11 Vgl. nur Rehm: Recht, bes. S. 46–55; Duranti: Right, S. 37; die European Archives Group hatte im Vorfeld der DSGVO Überzeugungsarbeit zu leisten, vgl. Hänger: Recht.

Arbeit der Archive erschwert oder verhindert hätten, im nationalen Recht zu derogieren.[12] Die Grundpfeiler archivischer Arbeit werden durch die DSGVO nicht in Frage gestellt.

Dies bedeutet jedoch keineswegs, dass alles beim Alten bleibt. Die vorliegende Arbeit wirft das Schlaglicht auf den dritten Satz in Art. 89 Abs. 1 DSGVO. Dieser verleiht der Pseudonymisierung als datenschutzrechtliche Maßnahme ein besonderes Gewicht. Aber was ist eigentlich jenseits von Agentenfilmen mit Pseudonymisierung gemeint? Wie wirken sich die Bestimmungen zur Pseudonymisierung in der DSGVO auf die Arbeit der Archive aus? Müssen künftig „große Massen von Archivgut" pseudonymisiert werden?[13]

Während insbesondere die Anonymisierung und weniger die Pseudonymisierung als Maßnahme der Schutzfristenverkürzung geläufig ist und bisweilen auch den Bereich der Überlieferungsbildung betreffen kann,[14] ist die Pseudonymisierung im Kontext der DSGVO in der Archivwissenschaft ein bislang kaum beschrittenes Terrain.[15] Es ist daher das vordringliche Ziel dieser Arbeit, sich einen ersten Überblick über die rechtlichen Normen und technischen Verfahren der Pseudonymisierung zu verschaffen. Ausgehend von diesen Beobachtungen sind erste Überlegungen über die Konsequenzen archivischer Arbeit möglich. Diese sind hier auf die Überlieferungsbildung und digitale Langzeitarchivierung begrenzt.[16] Zudem erfolgt der Blick vor allem aus der Sicht staatlicher, auf jeden Fall öffentlicher Archive.

Unverzichtbar ist zunächst eine nähere Bestimmung des Begriffs und seiner Spielarten im Datenschutzrecht, da sich Abweichungen vom intuitiven Verständnis ergeben (II). Anschließend erfolgt eine Sammlung und vergleichende Analyse der Normen, die sich mit der Pseudonymisierung befassen, angefangen mit der DSGVO und fortgesetzt mit den Datenschutzgesetzen und Archivgesetzen, die explizit oder implizit diese Normen spezifizieren (III). Die Auswirkungen auf die Überlieferungsbildung und digitale Archivierung

---

[12] Vgl. Art. 89 Abs. 3 DSGVO, die Betroffenenrechte laut Art. 15, 16, 18, 19, 20, 21 DSGVO; siehe ferner Rehm: Europäische Regelungen, S. 39f; Hänger: Europäische Datenschutzgrundverordnung, S. 48–51; Steinert: Datenschutz; außerdem sind im öffentlichen Interesse liegende Archivzwecke über Art. 17 Abs. 3 lit. d DSGVO vom „Recht auf Vergessenwerden" ausgenommen.

[13] Dies wäre wohl kaum zu leisten, vgl. Rehm: Europäische Regelungen, S. 38; Schlagk: Die datenschutzrechtliche Privilegierung, S. 39.

[14] Vgl. dazu unten, Abschnitt III.3.

[15] Vgl. nur Schumacher: Vorschläge, S. 6f; Rehm: Europäische Regelungen, S. 38; Hänger: Europäische Datenschutzgrundverordnung, S. 54f; Schlagk: Die datenschutzrechtliche Privilegierung, S. 23f, 31f; im Vorfeld Taylor: Archive, S. 36.

[16] Pseudonymisierungsmaßnahmen an analogem Archivgut selbst (nicht an seinen Erschließungsdaten, vgl. Schumacher: Vorschläge) sind an dieser Stelle abwegig und auch nicht von der datenschutzrechtlichen Forschungsrezeption der DSGVO erfasst.

werden unter besonderer Berücksichtigung der Bestandsbildner und ihrer Verpflichtungen betrachtet (IV). Gleiches verbindet sich mit einer Übersicht über mögliche organisatorische und technische Verfahren der Pseudonymisierung, die als Konkretisierung und Ergänzung der Auswirkungen zu begreifen ist (V).

II. Definitionen

II.1 Pseudonymisierung – Anonymisierung

Über die Verwendung der Begriffe Pseudonymisierung und Anonymisierung gibt es unterschiedliche Deutungen.[17] Intuitiv besagt der Begriff der Pseudonymisierung die Ersetzung eines Namens durch eine andere, „falsche" Bezeichnung, etwa „James Bond" durch „007". Unter Anonymisierung wäre dagegen zu verstehen, einen Namen nicht durch einen anderen zu ersetzen, sondern Identifikationsmerkmale gänzlich zu löschen. Diese Definitionen finden sich in den Begriffsbestimmungen unter § 3 BDSG a.F.[18]

Die Legaldefinitionen der DSGVO verschieben den Schwerpunkt von der Methode zur Wirkung.[19] Die Pseudonymisierung ist in Art. 4 Nr. 5 bestimmt als

> „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 technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden".[20]

---

[17] Taylor: Archive, S. 36, verweist auf die Debatte, ob der Terminus überhaupt genügend definiert werden kann.

[18] Siehe § 3 Nr. 6 BDSG a.F. für Anonymisierung als „das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können", vgl. auch Manegold: Archivrecht, S. 110 („faktische Anonymisierung"), ferner § 3 Nr. 6a BDSG a.F. die Pseudonymisierung als „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren", ist also enger gefasst als Art. 4 Nr. 5 DSGVO, vgl. Schwartmann/Mühlenbeck, in: Schwartmann/Jaspers/Thüsing, DSGVO/BDSG, Art. 4, Rn. 63.

[19] Für Gola, in: Gola DSGVO, Art. 4, Rn. 37 und Rn. 41, deckt sich Art. 4 Nr. 5 mit den Aussagen in § 3 Abs. 6 bzw. Abs. 6a BDSG aF; vgl. zur Abweichung auch GMDS: Arbeitshilfe, S. 9.

[20] In § 46 Nr. 5 BDSG n.F. wird die Definition der DSGVO fast wortgleich übernommen.

Es handelt sich also um Daten, deren Zuweisung zu einer Person aufgehoben wird. Mit Hilfe zusätzlicher Informationen, die einer „Zuordnungsregel“[21] unterliegen, ist die Zuweisung zu einer konkreten natürlichen Person aber grundsätzlich wiederherstellbar.[22] Diese Informationen sind „gesondert“ aufzubewahren und durch Maßnahmen technischer und organisatorischer Art zu schützen. Bei einer Anonymisierung besteht dagegen überhaupt keine realistische Möglichkeit der Zuordnung mehr, sodass „die betroffene Person nicht oder nicht mehr identifiziert werden kann“ (ErwG 26 DSGVO), ihre Daten somit auch nicht personenbezogen sind und nicht unter den Anwendungsbereich der DSGVO fallen.[23] Eine „identifizierte“ Person ist nach einer Pseudonymisierung ihrer Daten in Einklang mit Art. 4 Abs. 1 DSGVO noch „identifizierbar“, sodass ihre personenbeziehbaren Daten weiter zu den personenbezogenen Daten zählen, denn

> „als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.“

Entscheidendes Merkmal der Pseudonymisierung ist also die Einschränkung, aber (grundsätzliche) Wiederherstellbarkeit des Personenbezugs.[24] Die Vergabe eines Pseudonyms ist dabei eine mögliche, aber für diese Definition nicht notwendige Maßnahme: Codes, „Nutzererkennungen, E-Mail-Adressen, öffentliche bzw. private Schlüssel (z. B. in Blockchain), und Künstler- oder Decknamen“ können ebenfalls als Pseudonyme

---

21 Roßnagel: Pseudonymisierung, S. 243.

22 Vgl. Ernst, in: Paal/Pauly: DSGVO BDSG, Art. 4, Rn. 49.

23 Vgl. Roßnagel: Pseudonymisierung, S. 246; Ernst, in: Paal/Pauly: DSGVO BDSG, Art. 4, Rn. 48–50; ENISA: Recommendations, S. 13: „[R]ecalling the relevant definitions, pseudonymisation is related to the existence of an association between personal identifiers and pseudonyms, whilst in anonymisation such an association should not be availabe by any means“; bei § Nr. 6 BDSG a.F. erfolgt eine Abwägung nach dem Aufwand an Zeit, Kosten und Arbeitsaufwand, die sich hier auf die Anonymisierung bezieht, aber in ähnlicher Form (Kosten, Zeitaufwand, Technologien) auch in der DSGVO bzgl. pseudonymisierter Daten zu finden ist, vgl. ErwG 26 DSGVO; ferner GMDS: Arbeitshilfe, S. 9; zur Verhältnismäßigkeitsprüfung Schwartmann/Mühlenbeck, in: Schwartmann/Jaspers/Thüsing, DSGVO/BDSG, Art. 4, Rn. 74.

24 Vgl. auch Gola, in: Gola DSGVO, Art. 4, Rn. 39–41.

fungieren,[25] sofern sie denn eine Zuordnung tatsächlich erschweren.[26] Da es sich auch bei Pseudonymen um ein Attribut (Einzelangabe) eines Datensatzes unter anderen handelt, kann jedes nur einem Datensatz zugeordnete Attribut, auch die Signatur oder ID einer Personalakte im Archivfachinformationssystem, wie ein Pseudonym eingesetzt werden. Die Auslassung einer identifizierenden Information führt daher häufig nicht zu einer Anonymisierung, sondern zu einer Pseudonymisierung.[27]

II.2 Vollständige Auflösung des Personenbezugs

Für die Definition nicht eindeutig abzuleiten ist der Stellenwert einer Beziehbarkeit der Datensätze untereinander. So ist etwa nach dem obigen Beispiel die Verarbeitung mehrerer Daten eines Datensatzes möglich, der sich auf eine pseudonymisierte, aber grundsätzlich noch identifizierbare Person X bezieht; im Falle einer Strafakte etwa Beruf, Rechtsbetreff und Urteil.[28] Dennoch bleibt für den Verarbeiter dabei sichtbar, dass sich Beruf, Rechtsbetreff und Urteil alle auf eine einzige, pseudonymisierte und dadurch nicht identifizierte Person X beziehen. Über die Zuordnung bestimmter Eigenschaften zu einer Person ist so etwa „Profiling“ möglich.[29] Dagegen besteht ebenso die Möglichkeit, die Daten etwa für statistische Forschungen völlig ohne Bezug zueinander verarbeiten zu lassen. Im Fall der Strafakten wäre dies etwa der Fall, wenn bei einer Menge an Angaben von Berufen, Rechtsbetreffen und Urteilen nicht klar wäre, welche der Angaben überhaupt zueinander oder gar den Personen X, Y, Z etc. zuzuordnen wären. Solche aggregierten Daten (ErwG 162 DSGVO), die sich nur daraus geformten Gruppen, aber keinen Individuen zuordnen lassen, gelten nicht als personenbezogene Daten.[30]

---

[25] Die Grenzen zwischen Pseudonym und Identifikator (mithin also dem genauen Gegenteil) können fließend sein, vgl. zur Aufzählung Arning/Rothkegel, in: Taeger: DSGVO, Art. 4, Rn. 116; dagegen etwa Gola, in: Gola DSGVO, Art. 4, Rn. 37, der „keine andere Aussage als § 3 Abs. 6a BDSG aF“ erkennt; ferner aus technischer Sicht Pfitzmann/Hansen: A terminology v0.34, S. 21: „A pseudonym is an identifier of a subject other than one of the subject’s real names“, S. 22, Anm. 64: „Anonymous says something about a subject with respect to identifiability, pseudonymous only says something about employing a mechanism, i.e., using pseudonyms“, auch ENISA: Recommendations, S. 9f.

[26] Die These ist umstritten, vgl. nur Knopp: Pseudonym - Grauzone, S. 528.

[27] Umgekehrt reicht die Nennung des Namens allein oft nicht aus, um ihn einem Individuum zuzuordnen, vgl. The National Archives: Guide, S. 30.

[28] Vgl. für dieses Beispiel die Tabelle 3 bei Schumacher: Vorschläge, S. 57.

[29] Vgl. Art. 4 Nr. 4 DSGVO.

[30] Vgl. GMDS: Arbeitshilfe, S. 36; Richter, in: Roßnagel EU DSGVO, S. 247, Rn. 103; Kühling/Seidel/Sivridis: Datenschutzrecht, S. 101, Rn. 216, S. 102, Rn. 219.

Während es sich im ersten Fall eindeutig um eine Pseudonymisierung handelt, sollte es sich im zweiten Fall um eine Anonymisierung handeln, da sich der Rückschluss auf eine Person durch das Fehlen der Verkettung der übrigen Daten nicht unmittelbar ergibt, der Personenbezug somit aufgehoben ist. Es kommt jedoch darauf an, ob es angesichts der Beschaffenheit des Datensatzes (z. B. Größe, Individualität der Daten) mit Art. 4 Abs. 1 DSGVO generell möglich bleibt, mit Hilfe von Faktoren wie Zeit, Kosten oder Technologie (vgl. ErwG 26 DSGVO) einen Personenbezug wiederherzustellen. Dabei kann es je nach Auslegung der Relativität des Personenbezugs ein Kriterium sein, dass die datenführende Stelle, die die Anonymisierung durchführt, selbst nicht mehr in der Lage sein sollte, im Anschluss den Personenbezug wiederherzustellen.[31]

II.3 Relativität des Personenbezugs

Um Schlussfolgerungen über die Rechtsfolgen zu ziehen, ist zudem wichtig, die Relativität des Personenbezugs, also die Rollenverteilung der Akteure zu beachten: Wer führt die Pseudonymisierung durch? Wer verwahrt die Zuordnungsregel? Wer verarbeitet die pseudonymen Daten?[32] Denn die Grenzen zwischen Pseudonymisierung und Anonymisierung sind fließend. So ist etwa für denjenigen, der pseudonyme Daten ohne Zugänglichkeit zur Zuordnungsregel verarbeitet, von einer *anonymisierenden Wirkung der Pseudonymisierung* auszugehen[33]: Es macht für ihn keinen Unterschied, ob für jemand anderen eine theoretische Zuordnungsmöglichkeit besteht oder nicht; es wirkt auf ihn so, als sei der Personenbezug generell gelöscht. Dies wird etwa dann der Fall sein, wenn ein Archiv, das in Besitz der Zuordnungsregel ist, pseudonymisierte Daten zur Nutzung vorlegt. Dagegen kann nur von einer *risikomindernden Wirkung der Pseudonymisierung* die Rede sein, wenn die datenführende Stelle die Zuordnung der Daten durch die Trennung der identifizierenden Informationen für den Verarbeitungsprozess zwar aufhebt, aber eine Zuordnung nicht „ausreichend verlässlich ausgeschlossen ist“,[34] etwa weil die getrennte Verwahrung

---

[31] Vgl. Knopp: Pseudonym - Grauzone, S. 529; GMDS: Arbeitshilfe, S. 36, und ENISA: Recommendations, S. 13, mit Verweis auf ISO/TS 25237:2017 „Medizinische Informatik – Pseudonymisierung“.

[32] Vgl. Roßnagel: Pseudonymisierung, S. 243f; Marnau: Anonymisierung, S. 429f.

[33] Vgl. Roßnagel: Pseudonymisierung, S. 245; Kühling/Seidel/Sivridis: Datenschutzrecht, S. 107, Rn. 228; bei Haimberger/Geuer: Anonymisierende Wirkung, S. 58 als „relative Anonymisierung“.

[34] Roßnagel: Pseudonymisierung, S. 245.

durch technisch-organisatorische Maßnahmen bei ein und derselben Stelle erfolgt, z. B. als vorsorgliche Maßnahme gegen Datendiebstahl.[35]

Die gleiche Relativität des Personenbezugs führt auch bei Verbindung mit der Anonymisierung zu unterschiedlichen Haltungen.[36] Die oben bereits skizzierte Meinung bezeichnet nur die *absolute Anonymisierung* als Anonymisierung: Niemand, nicht einmal die anonymisierende Stelle, kann im Anschluss einen Personenbezug herstellen.[37] Sollte dies dennoch der Fall sein, müsste es sich um eine Pseudonymisierung, nicht um eine Anonymisierung handeln. Daneben versteht sich die *faktische* bzw. *relative Anonymisierung* als Ergebnis einer ausreichenden Entfernung der Identifizierungsmerkmale für eine Stelle, während für eine andere noch die Möglichkeit des Personenbezugs besteht.[38] Die *relative Anonymisierung* und die *anonymisierende Wirkung der Pseudonymisierung* teilen damit die Eigenschaft, für einen Verarbeiter dieser Daten einen Personenbezug zu verunmöglichen. Die DSGVO bleibt in dieser Auslegungsfrage uneindeutig, tendiert aber mit ErwG 26 DSGVO zu einem relativen Begriff, da Zusatzwissen nur dann für die Bewertung des Personenbezugs beachtet werden soll, wenn es nach „allgemeinem Ermessen wahrscheinlich“ benutzt wird.[39] Die Pseudonymisierung kann somit eine Stellung zwischen der Verarbeitung von Klardaten der betroffenen Personen einerseits und deren (absoluten) Anonymisierung andererseits einnehmen und Nachteile beider Varianten ausgleichen.

---

[35] Für Ernst, in: Paal/Pauly: DSGVO BDSG, Art. 4, Rn. 42, liegt angesichts der Relativität des Personenbezugs in diesem Fall überhaupt keine Pseudonymisierung, sondern ein unmittelbarer Personenbezug vor.

[36] Diese Frage ist seit Jahren Streitpunkt in der Auslegung des BDSG, vgl. Marnau: Anonymisierung, S. 429; für die folgenden Ausführungen bes. Haimberger/Geuer: Anonymisierende Wirkung, S. 58; Kühling/Seidel/Sivridis: Datenschutzrecht, S. 104–106, Rn. 226f, aber dagegen ebd., S. 108, Rn. 229 (Abb. 9).

[37] Eine „irreversible Pseudonymisierung“ ist dann nicht möglich, so Knopp: Pseudonym - Grauzone, S. 529, ebenso wenig eine „De-Anonymisierung“, vgl. Arning/Rothkegel, in: Taeger: DSGVO, Art. 4, Rn. 120.

[38] Vgl. Haimberger/Geuer: Anonymisierende Wirkung, S. 58; Manegold: Archivrecht, S. 110f.

[39] Haimberger/Geuer: Anonymisierende Wirkung, S. 58f; in diese Richtung auch Roßnagel: Pseudonymisierung, S. 247.

II.4 Pseudonymisierung – Verschlüsselung

Aufgrund einiger Gemeinsamkeiten bestehen häufig Unklarheiten in den Beziehungen zwischen Pseudonymisierung und Verschlüsselung.[40] Das könnte daran liegen, dass mitunter kryptographische Verfahren zur Pseudonymisierung verwendet werden.[41] Pseudonymisierung schützt die Betroffenen vor der Aufdeckung ihrer Identität, dagegen geht es bei der Verschlüsselung um eine Lesbarkeitsbeschränkung eines Teils oder der ganzen jeweiligen Datei und schützt so vor unautorisierten Auswertungen Dritter. Im Gegensatz zu einer Pseudonymisierung, die ein „single input" (Datensatz) zu einem „dual output" (pseudonymisierter Datensatz und Zuordnungsregel) verarbeitet, bleibt die Verschlüsselung bei einem „single output", zu öffnen mit einem Schlüssel.[42]

III. Gesetzliche Bestimmungen

III.1 DSGVO

Die Pseudonymisierung taucht an vielen Stellen der DSGVO auf, um die Rechte Betroffener sicherzustellen.[43] In ErwG 28 DSGVO verweist der Gesetzgeber auf eine „ausdrückliche Einführung der ‚Pseudonymisierung'" in das Datenschutzrecht, ohne „andere Datenschutzmaßnahmen auszuschließen" zu wollen. Für das öffentliche Archivwesen ist dabei ihre Erwähnung in Art. 89 Abs. 1 entscheidend: Hier wird eine Verarbeitung zu „im öffentlichen Interesse liegende[n] Archivzwecken" (neben „wissenschaftlichen oder historischen Forschungszwecken" sowie „statistischen Zwecken") dadurch eingeschränkt, dass die „Rechte und Freiheiten" Betroffener gewahrt werden müssen, und zwar mit „geeigneten Garantien" technischer und organisatorischer Maßnahmen (TOMs), unter besonderer Einhaltung des Grundsatzes der Datenminimierung. „Zu diesen Maßnahmen", so Art. 89 Abs. 1 S. 3 DSGVO, „kann die Pseudonymisierung gehören, sofern es möglich ist, diese Zwecke auf diese Weise zu erfüllen". Wo allerdings eine „Identifizierung von

---

[40] Vgl. ENISA: Recommendations, S. 17. Knopp: Pseudonym - Grauzone, S. 529 (wo nur Identifizierungsmerkmale verschlüsselt sind, ist Verschlüsselung eine Form der Pseudonymisierung).

[41] Vgl. Whitepaper, S. 17; unten Abschnitt V.2.

[42] Vgl. ENISA: Recommendations, S. 17f.

[43] Vgl. die Aufzählung bei Roßnagel: Pseudonymisierung, S. 243; ENISA: Recommendations, S. 16, zählt einschließlich der Erwägungsgründe insgesamt 15 Verweise.

betroffenen Personen nicht oder nicht mehr möglich ist“, also eine Anonymisierung vorliegt, ist konsequenterweise keine Maßnahme nötig.

Die Wichtigkeit dieser Bestimmung zeigt sich in Art. 89 Abs. 3, der für im öffentlichen Interesse liegende Archivzwecke den Mitgliedsstaaten eine Derogation der Betroffenenrechte in den Art. 15, 16, 18, 19, 20 und 21 ermöglicht, aber nur „vorbehaltlich der Bedingungen und Garantien gemäß Absatz 1“. Es ist somit nicht möglich, sich durch eine nationalstaatliche Derogation, etwa in den Archivgesetzen, der Umsetzung solcher „geeigneter Garantien“, insbesondere also der in Abs. 1 genannten Pseudonymisierung (dort, wo sie angebracht ist) zu entziehen.[44] Vielmehr schwebt dem Gesetzgeber laut ErwG 156 S. 3 DSGVO vor, eine Archivierung (oder wissenschaftliche bzw. statistische Auswertung) nur dann erfolgen zu lassen, „wenn der Verantwortliche geprüft hat, ob es möglich ist, diese Zwecke durch die Verarbeitung von personenbezogenen Daten, bei der die Identifizierung von betroffenen Personen nicht oder nicht mehr möglich ist, zu erfüllen, sofern geeignete Garantien bestehen (wie z. B. die Pseudonymisierung von personenbezogenen Daten)“.

Was ist nun unter diesen „geeigneten Garantien“ technischer und organisatorischer Maßnahmen im Sinne der DSGVO zu verstehen? Die Datenminimierung, d. h. die Beschränkung der Verarbeitung auf das für die jeweiligen Zwecke notwendige Maß, ist in Art. 5 Abs. 1 lit. c DSGVO als ein Grundsatz der Verarbeitung definiert. Die Pseudonymisierung gilt dabei laut Art. 25 Abs. 1 insbesondere als Maßnahme der Datenminimierung durch Technikgestaltung bei der Datenerhebung („data protection by design“)[45] wie auch laut Art. 32 Abs. 1 lit. a DSGVO bei der Verarbeitung als eine „geeignete technische und organisatorische Maßnahme“ (gemeinsam mit der Verschlüsselung), um ein „angemessenes Schutzniveau“ der Betroffenenrechte zu erreichen.[46] Über ihren Einsatz wird im Zuge einer Datenschutzfolgenabschätzung (DSFA) nach Art. 35 DSGVO entschieden, die ein dazu eingesetzter Verantwortlicher nach Art. 24 Abs. DSGVO „unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung“ durchzuführen hat, wenn ein wahrscheinlich hohes Risiko für die Rechte und Freiheiten der

[44] Vgl. nur Berger: Öffentliche Archive, S. 108–109.
[45] Vgl. EAG: Guidance, S. 23.
[46] Vgl. auch ErwGG 29, 78 DSGVO, zu Risiken für Rechte und Freiheiten der Person ErwG 75 und zu den Folgen einer Verletzung des Datenschutzes ErwG 85 DSGVO, wenn die Pseudonymisierung aufgedeckt wird.

betroffenen Personen besteht.[47] Auch Art. 6 (Erlaubnistatbestände) Abs. 4 DSGVO führt einige Punkte auf, die ein Verantwortlicher bei einer vom Ursprungszweck abweichenden Verarbeitung zu beachten hat,[48] und nennt ebenfalls explizit die Pseudonymisierung (wieder neben der Verschlüsselung) als geeignete Garantie für Betroffene (ebd. lit. e). Ferner wird die Pseudonymisierung auch einer genaueren Ausarbeitung in Verhaltensrichtlinien anempfohlen, die Verbände und Vereinigungen im privat(wirtschaftlich)en Bereich, aber auch Archivverbände zur Anwendung der DSGVO entwerfen können (Art. 40 Abs. 2 lit. d DSGVO).[49]

Damit ist zunächst festzuhalten: Die Pseudonymisierung gilt als technische oder organisatorische Maßnahme, die den Grundsatz der Datenminimierung bei der Datenerhebung wie auch bei der Datenverarbeitung umsetzen kann. Aus archivischer Sicht betrifft dies zum einen die Bestandsbildner nach Art. 25 und 32 DSGVO. Sie müssen gegebenenfalls eine DSFA durchführen und kommen möglicherweise zu dem Schluss, dass die Pseudonymisierung personenbezogener Daten für ihre Verarbeitung möglich und geeignet ist. Dies hat zum anderen unmittelbare Folgen für die Überlieferungsbildung, angefangen mit dem Records Management der Bestandsbildner und in der Folge auch in der Bewertung und Übernahme.

Letztere berühren als archivische Bearbeitungen bereits Art. 89 DSGVO, der zudem die Erschließung und Bestandserhaltung bis hin zur allgemeinen Nutzung geeigneten Garantien für betroffene Personen unterwirft. Damit überträgt sich auch die Verantwortung für die Maßnahmen auf die Archive. Wenngleich der Gesetzgeber einen besonderen Akzent auf die Pseudonymisierung legt, stellt er sie ausdrücklich nicht als einzige Maßnahme dar und gibt sie häufig als eine unter anderen Möglichkeiten der Gewährung geeigneter Garantien an.[50]

In Art. 89 DSGVO führt der Gesetzgeber die Pseudonymisierung nicht nur für im öffentlichen Interesse liegende Archivzwecke, sondern auch für wissenschaftliche oder

---

47 Vgl. auch ErwGG 71, 75 DSGVO.

48 Vgl. Schwartmann/Weiß: Whitepaper, S. 11; im öffentlichen Interesse liegende Archivzwecke gelten laut Art. 5 Abs. 1 lit. b DSGVO dagegen „nicht als unvereinbar mit den ursprünglichen Zwecken“ und unterliegen nicht der Prüfung nach Art. 6 DSGVO.

49 Auf Art. 40 DSGVO verweist auch Hänger: Europäische Datenschutzgrundverordnung, S. 52, mit Nennung der EAG Guidance als Schritt in diese Richtung, vgl. für das Vereinigte Königreich auch The National Archives: Guide.

50 Ob sie durch ihre Nennung zu einer Vorschrift wird, die „nur in Ausnahmefällen nicht obligatorisch ist“, darf bezweifelt werden, vgl. Schlagk: Die datenschutzrechtliche Privilegierung, S. 23f.

historische Forschungszwecke sowie statistische Zwecke in einem Zug an. Es ist daher fraglich, inwieweit Abs. 1 S. 3 zur Pseudonymisierung die Archive mit einbeziehen soll, denn die angeführten Zwecke sind zwar miteinander verbunden, aber doch unterschiedlich: Aus einer Forschungsfrage leitet sich direkt ein Verarbeitungszweck ab, während die Archivierung möglichst offen für verschiedene Zwecke sein soll.[51] Entsprechend dürfte auch mit Unterschieden in der konkreten Umsetzung der geforderten Garantien zu rechnen sein[52]. Gerade im Fall der Verarbeitung medizinischer Daten zu Forschungszwecken bei Langzeitprojekten ist die Pseudonymisierung aufgrund ihrer anonymisierenden Wirkung angemessen und etabliert.[53] Archive verwahren solche Daten aber auch für berechtigte Belange der (lebenden) betroffenen Personen – auf Grundlage der Integrität und Authentizität der Unterlagen gelang es etwa Opfern von Zwangssterilisierungen ihre Rechte geltend zu machen.[54] Um es vorweg zu nehmen: Eine Störung der Integrität, Authentizität und Verfügbarkeit vergleichbarer Unterlagen zugunsten einer hier risikomindernden Pseudonymisierung bei der Übernahme wäre in solchen Fällen kein angemessenes Mittel,[55] sofern Archive auch ihrer gesellschaftlichen Aufgabe nach Art. 6 Abs. 1 lit e DSGVO nachkommen sollen. In Einklang mit ErwG 156 DSGVO ist also zu prüfen, ob eine Pseudonymisierung eine geeignete Garantie darstellen könnte, oder ob für diese Zwecke andere Garantien greifen müssen. Daneben ist ebenfalls abzuwägen, ob Umfang, Kontext und relevante Risiken der Betroffenen eine solche Maßnahme rechtfertigen könnten.[56]

III.2 Datenschutzgesetze

In der Folge ihrer Verabschiedung 2016 wurden in Bund und Ländern die Datenschutzgesetze an die DSGVO angepasst. Obwohl den Archivgesetzen nachgeordnet, wirken sie sich über die Unterlagenentstehung bei den Bestandsbildnern aus. Sie sind auch als

---

[51] Vgl. Hillegeist: Rechtliche, S. 158: Im Rahmen von Forschung und Wissenschaft hält er eine (Forschungsdaten-)Archivierung personenbezogener Daten für nicht notwendig.

[52] Vgl. EAG: Guidance, S. 12.

[53] Vgl. die Erarbeitung der GMDS: Arbeitshilfe zu diesem Zweck; Hillegeist: Rechtliche, S. 154, S. 166; Datenschutzgruppe nach Artikel 29: Leitlinien DSFA, S. 14; Dickmann/Rienhoff: Medizin, S. 248–251. Ähnlich verhält es sich mit der Kriminalstatistik (für den Hinweis danke ich Dr. Kai Naumann, Stuttgart).

[54] Vgl. EAG: Guidance, S. 12; Becker: Bewertungshoheit, S. 66f; auch unten Anm. 103.

[55] Vgl. EAG: Guidance, S. 12; auch die anderen Grundsätze des Art. 5 DSGVO sollen erfüllt werden, vgl. auch die bereits bewährten Gewährleistungsziele in AK Technik der DSK: Standard-Datenschutzmodell, S. 9–11, 24–28; ferner Schlagk: Die datenschutzrechtliche Privilegierung, S. 24.

[56] Vgl. ENISA: Recommendations, S. 16.

„Auffanggesetze“ von Bedeutung, die immer dann zur Anwendung kommen, wenn die Daten nicht anderen datenschutzrechtlichen Spezialgesetzen unterworfen sind.[57] Bezüglich der DSGVO ist zu beachten, dass sie zwischen öffentlichen und nichtöffentlichen Stellen unterscheiden, bezüglich der Archivgesetze aber, dass es sich um Verbotsgesetze mit Erlaubnisvorbehalt handelt.[58]

Wenn in den Datenschutzgesetzen die Pseudonymisierung definiert wird, dann in jenen Gesetzen, die eine Umsetzung der JI-Richtlinie enthalten und in diesem Zuge eine zur DSGVO wortgleiche Definition vorschalten.[59] Eine Ausnahme stellt das DSG LSA dar, das bereits im § 1 die Pseudonymisierung als Maßnahme (soweit zweckmäßig) nennt und in § 2 ohne den Kontext der JI-Richtlinie definiert.[60] Jenseits des engeren archivischen Kontextes wird sie regelmäßig als Maßnahme bei der Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO angeführt,[61] obwohl es in den Artikeln der DSGVO eine spezielle Bestimmung zur Pseudonymisierung in diesen Kategorien nicht gibt.[62] Das Datenschutzgesetz Baden-Württemberg erwähnt sie unter den Maßnahmen zur Sicherstellung des Datenschutzes, also in risikomindernder Wirkung.[63] Darüber hinaus findet sich ihre Erwähnung vor allem unter den einführenden Regelungen der JI-Richtlinie, so ebenfalls im Kontext der besonderen Kategorien personenbezogener Daten[64], der Sicherheit der Datenverarbeitung[65] und der Bestimmungen zu „data protection by design/default“.[66]

---

57 BfDI: DSGVO - BDSG, S. 13; laut BMI: Organisationskonzept, S. 10, sind dies etwa das Sozialgesetzbuch, Verfassungsschutz- und Polizeigesetze des Bundes und der Länder, Telekommunikationsgesetz, Telemediengesetz, IT-Sicherheitsgesetz und andere.

58 Vgl. BMI: Organisationskonzept, S. 11.

59 Vgl. § 46 Nr. 5 BDSG; § 31 Nr. 5 BlnDSG; § 41 Nr. 5 HDSIG; § 24 Nr. 5 NDSG; § 36 Nr. 5 DSG NRW; § 27 Nr. 5 LDSG RP; § 21 Nr. 5 LDSG SH; § 32 Nr. 5 ThürDSG. Die Definition ist wenig überraschend gleichlautend mit Art. 3 Nr. 5 EU-Richtlinie 2016/680.

60 Vgl. § 1 Abs. 2 und § 2 Abs. 7a DSG LSA.

61 Vgl. § 22 Abs. 2 Nr. 6 BDSG; § 24 Nr. 5 BbgDSG; § 11 Abs. 2 Nr. 5 BremDSGVOAG; § 22 Abs. 2 Nr. 6 HDSIG; § 15 Nr. 5 DSG NRW; § 8 Nr. 5 DSG M-V; § 8 Abs. 2 Nr. 5 SDSG; § 12 Abs. 3 LDSG SH. Keine näheren Bestimmungen zu besonderen Kategorien personenbezogener Daten haben SächsDSDG (nur Erwähnung in § 4 Abs. 2 zu zweckändernder Verarbeitung) und Art. 8 BayDSG (hier jedoch Verweis auf Maßnahmen nach Art. 30 DSGVO).

62 Vgl. Art. 6 Abs. 4 lit. e DSGVO bezieht sich auf eine Weiterverarbeitung jeder Art personenbezogener Daten.

63 Vgl. § 3 Abs. 1 Nr. 5 LDSG BW.

64 Vgl. § 48 Abs. 2 Nr. 6 BDSG; § 33 Abs. 2 Nr. 6 BlnDSG; § 43 Abs. 2 Nr. 6 HDSIG; § 29 Abs. 2 Nr. 6 LDSG RP; § 37 Abs. 2 Nr. 6 ThürDSG.

65 Vgl. § 50 BlnDSG; § 59 Abs. 2 HDSIG; § 34 NDSG; § 58 Abs. 2 DSG NRW; § 53 Abs. 2 LDSG RP; § 54 Abs. 2 ThürDSG.

66 Vgl. § 64 BDSG; § 57 Abs. 1 BlnDSG; § 66 Abs. 1 HDSIG; § 59 Abs. 1 LDSG RP; § 47 Abs. 1 LDSG SH.

Bei der Suche nach einer Rezeption von Art. 89 DSGVO fällt auf, dass einige Gesetze die wissenschaftlichen, historischen und/oder statistischen Zwecke von den Archivzwecken durch eine Teilung in zwei Paragraphen bzw. Artikel trennen.[67] Dies bildet die Zweiteilung der Derogationsmöglichkeit in Art. 89 Abs. 2 für die Forschung und Art. 89 Abs. 3 DSGVO für die Archivzwecke ab, die auch in diesen Datenschutzgesetzen getrennt voneinander verwirklicht ist.[68] Das Berliner Datenschutzgesetz verhandelt alle diese Zwecke in einem Paragraphen.[69] Die Mehrheit der Gesetze verzichtet jedoch auf eine Erwähnung der Archivzwecke unter den besonderen Verarbeitungssituationen und verhandelt unter unterschiedlichen Bezeichnungen nur die wissenschaftlichen, historischen oder statistischen Zwecke.[70] Die Derogationen für das Archivwesen sollten dann in den Archivgesetzen umgesetzt werden.

In aller Regel findet sich unter den wissenschaftlichen, historischen und/oder statistischen Zwecken dabei auch ein Anonymisierungsgebot, das eine anonymisierte Nutzung der Daten vorschreibt, wenn die Zwecke damit erfüllt werden können. Solange eine Anonymisierung nicht möglich ist, verlangen sie eine „gesonderte Speicherung“ der identifizierenden Merkmale bzw. eine Pseudonymisierung bis zu einem möglichen Löschzeitpunkt.[71] Dagegen sind in den Landesdatenschutzgesetzen, die außerdem die Archivzwecke aufgenommen haben, nur die Derogationen der Betroffenenrechte oder auch die Archivierung als Löschungssurrogat ausgeführt. Art. 26 Abs. 1 BayDSG hat durch die

---

67 Vgl. § 27/28 BDSG (§ 28 nur Archivzwecke in Bezug auf besondere Kategorien personenbezogener Daten); Art. 15/16 BayDSG; § 13/14 LDSG BW; § 24/25 HDSIG (in § 25 nur Archivzwecke in Bezug auf besondere Kategorien personenbezogener Daten); § 23/24 SDSG.

68 Die Spiegelung ergibt sich auch dann, wenn die getrennte Behandlung bereits auf die vorherigen Datenschutzgesetze zurückzuführen ist und nicht auf die DSGVO.

69 Vgl. § 35 BlnDSG.

70 Vgl. § 25 BbgDSG (Datenverarbeitung für wissenschaftliche und historische Forschungszwecke); § 9 DSG M-V (Datenverarbeitung für wissenschaftliche oder historische Zwecke); § 13 NDSG (Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken); § 17 DSG NRW (Datenverarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken); § 22 DSG Rheinland Pfalz (Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken); § 12 SächsDSDG (Verarbeitung personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken); § 27 DSG LSA (Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen); § 13 LDSG SH (Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken); § 28 ThürDSG (Verarbeitung personenbezogener Daten durch Forschungseinrichtungen); § 11 HmbDSG (Datenverarbeitung zum Zwecke wissenschaftlicher und historischer Forschung sowie Statistik); § 13 BremDSGVOAG (Verarbeitung besonderer Kategorien personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken).

71 § 12 Abs. 2 SächsDSDG hat ein implizites Anonymisierungsgebot, da getrennt zu speichernde identifizierende Merkmale sobald als möglich zu löschen sind.

Nennung der „geeigneten Garantien“ einen zumindest indirekten Verweis auf die Pseudonymisierung als TOM.[72] Das BDSG verweist auf die Maßnahmen zur Verarbeitung besonderer Kategorien personenbezogener Daten, die auch die Pseudonymisierung nennt.[73]

Obwohl also die Datenschutzgesetze sich an die DSGVO angleichen, sind Bestimmungen zur Pseudonymisierung weit zurückhaltender ausgeführt als in der DSGVO, gilt sie hier doch zumeist nur als Zwischenstufe auf dem Weg zur Anonymisierung. Auch weist die Aufteilung in unterschiedliche Paragraphen auf eine Rezeption der Pseudonymisierung hin, die sich weniger auf die Archivzwecke als auf die anderen in Art. 89 DSGVO genannten Zwecke bezieht. Über die Bestandsbildner, die insbesondere im Bereich der besonderen Kategorien personenbezogener Daten sowie über die JI-Richtlinie die Pseudonymisierung als Sicherheitsmaßnahme einbeziehen müssen, und über die Uneindeutigkeit des vorrangig geltenden Art. 89 DSGVO bleibt sie für die Tätigkeit von Archiven relevant.

III.3 Archivgesetze

Bei der Suche nach Auswirkungen auf Pseudonymisierungsbestimmungen in den 17 deutschen Archivgesetzen ist zunächst festzustellen, dass erst knapp mehr als die Hälfte die DSGVO in ihren aktuellen Fassungen berücksichtigen, die übrigen dennoch in puncto Datenschutz im Licht der vorrangigen DSGVO interpretiert werden müssen.[74] Übliche Anpassungen betreffen etwa die Begrifflichkeit („Betroffener“ wird „betroffene Person“) oder die Derogationen der Rechte betroffener Personen nach Art. 89 Abs. 3 DSGVO.[75]

In keinem Gesetz wird die Pseudonymisierung wörtlich erwähnt. Es finden sich jedoch einige Bestimmungen, in denen die Archivgesetze eine anonymisierte Vorlage von personenbezogenen Unterlagen bzw. Archivgut für die Nutzung vorsehen. Dies geschieht häufig mit einem Verweis auf Unterlagen, die mit Absätzen aus § 203 StGB (Verletzung von

---

[72] Vgl. auch § 28 Abs. 1 iVm § 22, Abs. 2 Nr. 6 BDSG.

[73] Vgl. § 22 Abs. 2 Nr. 6 BDSG, auch Hänger: Europäische Datenschutzgrundverordnung, S. 54-55.

[74] Dies ist der Fall für BremArchivG, LArchG M-V, SArchG, NArchG, LArchG SH, ThürArchivG, BbgArchivG, BArchG, SächsArchivG; noch ohne DSGVO LArchG BW, BayArchivG, ArchGB, HmbArchG, ArchG LSA, LArchG RP, ArchivG NRW, HArchivG; vgl. auch Berger: Öffentliche Archive, S. 314.

[75] Vgl. nur Birk: Anpassung; Heilmann: Anpassung; Landesarchiv Thüringen: Neues Thüringer Archivgesetz; auch Steinert: Datenschutz.

Privatgeheimnissen) in Verbindung gebracht werden können.[76] Die Anonymisierung findet sich jedoch auch als ausdrückliche Maßnahme bei einer Schutzfristenverkürzung, um schutzwürdige Belange Betroffener zu schützen.[77] Da nicht davon auszugehen ist, dass in diesen Fällen ein Personenbezug auch für das Archiv unwiderruflich aufgehoben wird, ist diese Form als *relative Anonymisierung* anzusehen. Mit der Verschiebung der Definition von der konkreten Methode zur Wirkung kann sie daher im Sinne der oben erläuterten Definition auch als *Pseudonymisierung* verstanden werden, die auf eine *anonymisierende Wirkung* abhebt, da eine Beziehbarkeit der Personen über die nicht vorgelegten Daten im Archiv erhalten bleibt. Tatsächlich stellt sich die Frage, wie oft in der Praxis die Beziehbarkeit der Daten eines Datensatzes untereinander durch den Erhalt einer Einzelangabe pro Datensatz oder durch Vergabe einer Kennung erhalten bleibt und somit de facto eine Pseudonymisierung statt einer Anonymisierung vorliegt. Es ist jedenfalls deutlich, dass ein Archiv in diesem Fall die Maßnahme durchführt und so Dritten die Verwendung für wissenschaftliche und historische Zwecke oder Statistikzwecke getreu Art. 89 Abs. 1 DSGVO ermöglicht.

Bisweilen ist mit Bezug auf § 203 Abs. 1 StGB auch eine anonymisierte Übernahme gefordert.[78] Im Archivgesetz des Saarlandes ist zudem vorgesehen, dass, wenn entgegengesetzte „schutzwürdige Belange Betroffener" auch durch eine Verlängerung der Schutzfrist nicht ausreichend geschützt sind, die Unterlagen anonymisiert werden müssen, oder, wenn auch das keine Abhilfe schafft, eine Übernahme sogar unterbleiben muss.[79] In diesen Fällen wird dagegen auf eine relative Anonymisierung zur Datenminimierung abgehoben, die bei Kassation der zunächst noch erhaltenden Klardaten in eine *absolute Anonymisierung* mündet.

Ferner behandeln die Archivgesetze auch „Maßnahmen", die entweder ausdrücklich oder implizit als TOMs gelten müssen und zu denen die Pseudonymisierung gezählt werden kann. Zu nennen ist etwa der für die Anonymisierung bereits angesprochene Kontext

---

[76] Vgl. § 7 Abs. 6 BremArchivG, § 6 Abs. 2 LArchG M-V, § 8 Abs. 2 SArchG, § 11 Abs. 2 BbgArchivG; in § 3 Abs. 1 LArchG BW nicht bei der Nutzung, sondern bei der Übernahme.

[77] Vgl. § 12 Abs. 2 Nr. 2 BArchG, § 6 Abs. 4 LArchG BW.

[78] Das betrifft insbesondere die Unterlagen aus Beratungsstellen, vgl. § 4 Abs. 2 Nr. 3 BbgArchivG (mit Bezug auf § 203 Abs. 1 Nr. 1, 4, 4a/5 StGB), § 6 Abs. 2 LArchG M-V (Abs. 1 gesamt), § 4 Abs. 2 Nr. 2 ArchivG NRW (Nr. 1, 2, 4, 4a/5), § 3 Abs. 1 LArchG BW (Nr. 1, 4, 4a/5).

[79] Vgl. § 9 Abs. 6 SArchG.

der Schutzfristenverkürzungen im Bereich der Nutzung.[80] Daneben werden solche Maßnahmen aber auch im Kontext der „Speicherung", „Sicherung", des „Datenschutz[es]" oder ähnlichem genannt, die sich entweder auf das Archivgut insgesamt oder auch spezieller auf personenbezogene Daten bzw. Unterlagen beziehen.[81] Dabei geht das Archivgesetz Thüringens sogar ausdrücklich auf die TOMs nach Art. 32 DSGVO ein.[82] Sofern also die Pseudonymisierung sich (von Fall zu Fall) als eine geeignete Maßnahme erweist, kommt hier ihre *risikomindernde Wirkung* zum Tragen. In Rheinland-Pfalz ist außerdem ein Passus zur Übernahme von Archivgut angeführt, der bestimmt, dass „bei Unterlagen mit personenbezogenen Daten die Vorschriften über die Verarbeitung und Sicherung dieser Unterlagen zu beachten [sind], die für die abgebende Stelle gelten"[83]: Ist hier eine risikomindernde Pseudonymisierung als Vorschrift vorgesehen, muss auch das Archiv diese Maßnahme umsetzen. Im Bereich (digitaler) Zwischenarchive kann die Verantwortung für TOMs an die jeweiligen Archive fallen,[84] wenngleich die abgebende Stelle die eigentlich verarbeitende Stelle bleibt.

IV. Auswirkungen im Archivwesen

Bei vergleichender Betrachtung der DSGVO, der Datenschutzgesetze und der Archivgesetze zeigt sich, dass Maßnahmen zur Pseudonymisierung stets zu unterscheiden sind nach ihrer anonymisierenden oder ihrer risikomindernden Wirkung. Für die Archive ergeben sich eine Reihe von Fragen, die sämtliche Arbeitsbereiche der Archive von Behördenberatung und Records Management bis hin zur Nutzung betreffen. Im Folgenden können aber als Schwerpunkt nur Elemente aus der Überlieferungsbildung und der digitalen Archivierung behandelt werden.

---

80 Vgl. § 5 Abs. 4 HmbArchG; § 10 Abs. 4 Nr. 3 LArchG M-V; § 9 Abs. 4 ArchGB; § 5 Abs. 5 Nr. 2 NArchG; § 9 Abs. 6 Nr. 2 LArchG SH; § 12 Abs. 2 Nr. 2 BArchG; § 13 Abs. 5 Nr. 3 HArchivG, § 10 Abs. 4 Nr. 2 lit. b ArchG LSA.

81 Auch zu personenbezogenen Unterlagen § 5 Abs. 2 ArchivG NRW, § 6 Abs. 3 BbgArchivG; zu Archivgut insgesamt § 9 Abs. 2 LArchG RP, § 8 Abs. 1 LArchG SH, Art. 9 Abs. 1 BayArchivG, § 11 Abs. 1 HArchivG und § 9 Abs. 4 ArchGB.

82 Vgl. § 15 Abs. 1 ThürArchivG, siehe Berger: Öffentliche Archive, S. 335–337.

83 Vgl. § 9 Abs. 3 LArchG RP.

84 Vgl. § 5 Abs. 5 BbgArchivG, § 8 Abs. 2 BArchG.

IV.1 Überlieferungsbildung

IV.1.1 Pseudonymisierung bei datenführenden Stellen

Angesichts der Anwendbarkeit der DSGVO auf die Bestandsbildner stellt sich zunächst die Frage, welche abgabepflichtigen Behörden und Einrichtungen von den Bestimmungen zur Pseudonymisierung betroffen sein könnten. Da die DSGVO neben nichtöffentlichen Stellen generell fast alle öffentliche Stellen betrifft, kommen zunächst alle öffentlichen Stellen des Bundes und der Länder, der Kommunen und anderer öffentlicher Stellen in Frage, die nicht Tätigkeiten außerhalb des Anwendungsbereichs des Unionsrechts und der Sicherheits- und Außenpolitik entsprechen.[85] Die von der JI-Richtlinie erfassten Bereiche wie „Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten“ betreffen einen beträchtlichen Teil personenbezogener Unterlagen der Justiz und der Polizei, so etwa Kriminalämter, Zoll oder Behörden, die Ordnungswidrigkeitenrecht umsetzen,[86] fallen aber erst bei einer Archivierung wieder unter die Bestimmungen der DSGVO.[87]

Personenbezogene Daten werden in so vielen Behörden verarbeitet, dass eine abschließende Auflistung an dieser Stelle weder sinnvoll noch zweckmäßig wäre. Eine Liste möglicher Verarbeitungstätigkeiten findet sich in den Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO der Datenschutzkonferenz, darunter Personalaktenführung, Lohn, Gehalt, Bezüge, Schülerverwaltung, Finanzbuchhaltung, Antragsbearbeitung, Rats- und Bürgerinformationssysteme, Melderegister, Fahrzeugregister, Wählerverzeichnisse oder Untersuchungen beim Amtsarzt.[88] Darüber hinaus finden sie sich auch in Personalverwaltungssystemen (PLUS), Volkszählungen, Geburten- oder Eheschließungsstatistiken oder in Katastern.[89] Regelmäßig sind sie also massenhaft gleichförmig und in der (heute meist elektronischen) Verwaltung physischer Akten, in von Fachverfahren verwalteten Datenbankstrukturen oder (E-)Akten aufzufinden, wo eine

---

85 Siehe oben Anm. 4.
86 Vgl. BfDI: DSGVO - BDSG, S. 17.
87 Vgl. Anm. 7.
88 Vgl. Datenschutzkonferenz: Hinweise, S. 5.
89 Vgl. Keitel: Digitale personenbezogene Unterlagen, S. 50; zur Schutzwürdigkeit von Daten in Personenstandsunterlagen vgl. Baumann: Schutzwürdigkeit, bes. S. 147–149; im Bestand des Landesamts für Geoinformation und Landentwicklung Baden-Württemberg im Staatsarchiv Ludwigsburg (StAL EL 68 V) wurden personenbezogene Teile sogar separat abgelegt (für die Auskunft danke ich Dr. Kai Naumann, Stuttgart).

Pseudonymisierung zumindest technisch machbar wäre. Dabei ist denkbar, dass die Zuordnungsregel als ein „Bestandteil außerhalb des Systems“ auftreten könnte, der es nachzugehen gilt.[90]

In vielen Fällen ist es im Bereich der öffentlichen Leistungsverwaltung weder notwendig noch zweckmäßig, Daten pseudonymisiert zu verarbeiten: Es kann die Arbeit des Bestandsbildners unverhältnismäßig erschweren. Ausschlaggebend für die Maßnahme einer Pseudonymisierung im Zuge des Verarbeitungsprozesses sind, wie ausgeführt, bei den Bestandsbildern immer die Abwägung nach dem Risiko für die Freiheiten und Rechte der Betroffenen in Relation zu Arten, Umfang, Umständen und Zwecken der Verarbeitung.[91] Diese Abwägung findet im Zuge einer DSFA statt.

Ein „hohes Risiko“ besteht, wenn Verarbeitungsvorgänge ein Profiling für Entscheidungen über Rechtswirkungen gegen eine Person, besondere Kategorien personenbezogener Daten oder Überwachung öffentlich zugänglicher Bereiche zum Gegenstand haben.[92] Die Artikel-29-Datenschutzgruppe der EU-Kommission führt in ihren Leitlinien neun Kriterien aus Verarbeitungen und Datentypen auf, von denen zwei erfüllt sein müssen, um in der Regel eine DSFA erforderlich zu machen. Dazu zählen etwa

- die Verarbeitung vertraulicher oder höchst persönlicher Daten nach Art. 9 und 10 DSGVO wie medizinische oder genetische Daten, Daten zur politischen oder religiösen Weltanschauung und sexueller Identität, zur strafrechtlichen Verfolgung oder zum privaten Lebensbereich,
- ein besonders großer Umfang der Datenverarbeitung,
- Abgleich oder Zusammenführung von Datensätzen oder
- Daten schutzbedürftiger Betroffener wie Kinder, Kranke, Senioren oder auch Arbeitnehmer.[93]

---

[90] Vgl. nestor-Arbeitsgruppe E-Akte: E-Akte, S. 13.

[91] Vgl. Datenschutzgruppe nach Artikel 29: Leitlinien DSFA, S. 5–7, nach Art. 35 Abs. 1 DSGVO; Schwartmann/Weiß: Entwurf Code of Conduct, S. 10f.

[92] Vgl. Art. 35 Abs. 3 DSGVO; ErwG 75 DSGVO; Datenschutzgruppe nach Artikel 29: Leitlinien DSFA, S. 9; BMI: Organisationskonzept, S. 22–25; zur Schwellwert-Analyse siehe AK Technik der DSK: Standard-Datenschutzmodell, S. 42–46; zur Risikoanalyse auf Basis des IT-Grundschutzes des BSI vgl. BSI: BSI-Standard 200-3.

[93] Vgl. Datenschutzgruppe nach Artikel 29: Leitlinien DSFA, S. 10f, weitere: 1. Bewerten und Einstufen nach Arbeitsleistung, Gesundheit oder anderen Aspekten, 2. Automatisierte Entscheidungsfindung, 3. systematische Überwachung, 5. Datenverarbeitung im großen Umfang, 8. Neue Technologien oder innovative Nutzung bestehender Technik, 9. Hinderung an Dienstleistung oder Vertragsschluss (z. B. Schufa).

Damit geraten besonders Daten, die traditionell in Patienten-, Justiz-, Sozial- und Personalakten zu finden sind, und ihre Produzenten in den Fokus.[94] Es kommt jedoch ebenso auf die Arten der Verarbeitung, die Betroffenen und deren Anzahl an.[95] Umgekehrt gibt es Fälle, in denen keine DSFA notwendig ist: Das gilt nicht nur bei geringem Risiko, sondern unter anderem auch dann, wenn die Verarbeitung im öffentlichen Interesse liegt oder in der Ausübung öffentlicher Gewalt erfolgt bzw. bei Schaffung der Rechtsgrundlage eine DSFA erfolgte.[96] Hier bleibt es eine Ermessensentscheidung, ob eine DSFA durchgeführt wird oder nicht. So erstellt etwa der LfDI Baden-Württembergs eine DSFA für die E-Akte BW, die als Muster für die behördenspezifischen Verarbeitungen genutzt werden soll.[97]

Welche Behörden bei welchen Verarbeitungsprozessen welcher Daten sich der Pseudonymisierung als TOM zur Wahrung der Rechte betroffener Personen bedienen, lässt sich also nur im Einzelfall und in direktem Behördenkontakt feststellen. Überall dort, wo Verarbeitungsform und Daten auf eine DSFA hindeuten, ist die Möglichkeit ihres Einsatzes zumindest zu bedenken. Eine Hilfestellung bietet das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO, das die bisherigen Dokumentationspflichten ersetzt.[98] Dieses Verzeichnis muss von allen Verantwortlichen und Auftragsverarbeitern geführt werden und enthält auch einen Nachweis über die eingerichteten TOMs.[99] Auch das Ergebnis der DSFA ist zu dokumentieren und kann so Hinweise auf den Einsatz einer Pseudonymisierung im konkreten Fall geben.[100] Es gilt zu beobachten, in welchen Bereichen

---

94 Vgl. auch Schumacher: Vorschläge, S. 5; die Verarbeitung besonderer Kategorien personenbezogener Daten führt „automatisch“ zu einem erhöhten Schutzbedarf, vgl. BMI: Organisationskonzept, S. 80f.

95 Schwartmann/Weiß: Entwurf Code of Conduct, S. 11.

96 Datenschutzgruppe nach Artikel 29: Leitlinien DSFA, S. 15, nach Art. 35 Abs. 10 iVm Art. 6 Abs. 1 lit. e DSGVO.

97 LfDI BW: 35. Datenschutz-Tätigkeitsbericht 2019, S. 34f.; ein Muster zur DSFA bei der Einführung der elektronischen Personalakte ist zu finden bei BMI: Organisationskonzept, S. 98–101.

98 Vgl. Datenschutzkonferenz: Hinweise, S. 1.

99 Vgl. Datenschutzkonferenz: Hinweise, S. 2; ausgenommen von der Pflicht der Führung eines solchen Verzeichnisses sind datenführende Stellen unter 250 Beschäftigten, nicht jedoch, wenn sie besondere Kategorien personenbezogener Daten verarbeiten, ein Risiko für Rechte und Freiheiten besteht oder sie regelmäßig erfolgen, sodass diese Ausnahmen kaum vorkommen, vgl. ebd., S. 3f; eine Übersicht über die TOMs mit Beispielen ebd., S. 8–12; ferner Kaufmann: Handlungsbedarf, S. 243; zur Bestimmung der TOMs nach dem Risiko AK Technik der DSK: Standard-Datenschutzmodell, S. 46f.

100 Vgl. Art. 35 Abs. 7 DSGVO, Datenschutzkonferenz: Hinweise, S. 1; für besondere Kategorien personenbezogener Daten wird auch nach § 22 Abs. 1, 2 BDSG ausdrücklich die Pseudonymisierung genannt, vgl. Arning/Rothkegel, in: Taeger: DSGVO, Art. 4, Rn. 122.

sich die bestandsbildenden Stellen nach einer DSFA für die Pseudonymisierung entscheiden werden.

IV.1.2. Anbietung und Bewertung

Durch die Maßnahmen einer Pseudonymisierung ändert sich nichts an den Anbietungspflichten der Bestandsbildner. Bei Vorliegen einer risikomindernden Pseudonymisierung ist eine Anbietung der Daten wie auch der Zuordnungsregel vom gleichen Bestandsbildner rechtens. Hier gilt es, auf tatsächliche Anbietung und Übernahme der Zuordnungsregel sowie ihre Nutzbarkeit sorgfältig zu achten.[101] Wo gesetzlich eine anonymisierte Übernahme gefordert ist,[102] muss sie weiterhin anonymisiert, also unter Aufgabe des Personenbezugs, erfolgen. Es wäre jedoch denkbar, angesichts der Schutzwirkung der Pseudonymisierung eine Änderung dieser Normen zugunsten einer Rechtswahrung der betroffenen Personen in Erwägung zu ziehen,[103] geeignete TOMs für die Sicherung der Zuordnungsregel bis zum Ablauf der Schutzfristen vorausgesetzt.

Da man es aus den genannten Gründen häufig mit personenbezogenen Daten besonderer Kategorien zu tun haben dürfte, erwächst den Archiven nach Art. 9 Abs. 2 lit. j DSGVO womöglich eine neue Herausforderung: Die weitere Verarbeitung solcher Daten ist laut dieser Öffnungsklausel nur erlaubt, wenn sie „für im öffentlichen Interesse liegende Archivzwecke…erforderlich“ ist.[104] Daraus lässt sich unter Umständen die Pflicht zu einer „Erforderlichkeits- bzw. Verhältnismäßigkeitsprüfung“ ableiten, nach der die Ziele vielleicht auch auf andere Weise erreicht werden könnten.[105] Hier besteht ein Zusammenhang zu ErwG 156 S. 3 DSGVO, der, wie oben erläutert, die Prüfung „des Verantwortlichen“ voraussetzt, ob die Zwecke des Art. 89 DSGVO nicht auch anonymisiert

---

[101] Vgl. The National Archives: Guide, S. 11: „There is a risk that over-cautious or inaccurate interpretation may lead to the weeding, anonymising or destruction of files containing personal data that would otherwise be passed to the archive service with managed access over time.“ Erfolgt die Pseudonymisierung durch eine Softwarelösung (innerhalb oder zusätzlich zu einem DMS), muss sichergestellt sein, dass ihre Funktionalität zur Depseudonymisierung erhalten wird oder simuliert werden kann.

[102] Vgl. oben Anm. 78.

[103] Es ist möglicherweise im Sinne der betroffenen Personen, für eine Rechtswahrung den Personenbezug zu erhalten, vgl. Becker: Bewertungshoheit, S. 66f; zur Problematik auch Manegold: Archivrecht, S. 158–160; für diese Anregung danke ich Dr. Jakob Wührer, Linz.

[104] Die Abhängigkeit von einer Erforderlichkeit betrifft auch weitere Verarbeitung in Art. 9 Abs. 2 DSGVO. Sie wird auch in Datenschutzgesetzen wiederholt, z. B. § 14 LDSG BW.

[105] Vgl. Berger: Öffentliche Archive, S. 316, und dort angegebene Kommentare; ohne Verweis auf eine solche Prüfung Jaspers/Schwartmann/Mühlenbeck, in: Schwartmann/Jaspers/Thüsing, DSGVO/BDSG, Art. 9, vgl. ferner das dreistufige Verfahren bei Schlagk: Die datenschutzrechtliche Privilegierung, S. 23f.

(„Identifizierung von Personen nicht oder nicht mehr möglich“) erfüllt werden können. Da jedoch auch hier die Pseudonymisierung als geeignete Garantie genannt wird, spielt der Gesetzgeber wohl auf deren anonymisierende Wirkung unter Erhalt der Zuordnungsregel an – die im Fall der Archivzwecke nur durch ihre Überlieferung im Archiv gewährleistet bleibt.[106] Keinesfalls sollte eine solche Prüfung also durch die bestandsbildende Behörde und noch vor der Anbietung stattfinden.[107]

Im Kontext pseudonymisierter Daten kann dies darauf hinauslaufen, die Bewertung der Zuordnungsregel als archivwürdig anhand von Nutzungszwecken begründen zu müssen, um in der Folge eine absolute Anonymisierung abzuwenden.[108] Bei Zielen zur Rechtswahrung scheint dies ohne weiteres möglich, bei Zielen quantitativer statistischer Auswertungen dagegen nicht. Für den Erhalt methodisch qualitativer Auswertung, beispielsweise für exemplarische Fälle oder für Personen der Zeitgeschichte, wird es auf die technischen Umstände ankommen, um etwa Teile der Zuordnungsregel zu erhalten. Jenseits der bereits in den Archivgesetzen geforderten anonymisierten Übernahmen wird es künftig also zusätzlich nötig sein, im Licht künftiger Auswertungsmöglichkeiten die Notwendigkeit des Erhalts einer Personenbeziehbarkeit aus dem Einzelfall zu begründen und zu dokumentieren, auch wenn es den Zielen einer auswertungsoffenen Überlieferungsbildung widerspricht.

IV.2 Digitale Langzeitarchivierung

Sobald die Unterlagen in den Verantwortungsbereich des Archivs gelangen, stellen sich nach Art. 89 DSGVO neue Fragen zur Pseudonymisierung: Dürfen Archive pseudonymisierte Daten depseudonymisieren? Oder sollen Archive bereits vorhandene digitale Bestände, die unter die DSGVO fallen, sogar im Nachhinein pseudonymisieren?

---

[106] Beim Bestandsbildner löst der Abschluss einer archivischen Übernahme gerade bei personenbezogenen Daten eine Löschpflicht des kassablen Rests nach Art. 5 Abs. 1 lit. e bzw. Art. 17 Abs. 1 lit. a und e DSGVO aus; vgl. ferner auch Keitel: Aussonderung, S. 74.

[107] So aber Berger: Öffentliche Archive, S. 317f, mit Verweis insbesondere auf § 11 Abs. 3 S. 2 ThürArchivG und § 6 Abs. 2 LArchG SH; dagegen Becker: Bewertungshoheit, S. 67; Johannes: § 4 V. Archivierung, Rn. 141f.

[108] Vgl. Hänger: Europäische Datenschutzgrundverordnung, S. 54; auch Berger: Öffentliche Archive, S. 500: „Würde man unter im öffentlichen Interesse liegenden Archivzwecken jede wissenschaftliche oder historische Methode zu beliebig neuen Zwecken verstehen, dann würde man damit den Grundsatz der Zweckbindung systemwidrig umgehen.“ Zur Problematik der Antizipation von Nutzerinteressen vgl. nur Keitel: Zwölf Wege, S. 227-230, Bischoff: Bewertung, S. 50. Umgekehrt kann das Risiko durch eine „Verrumpfung“, also Ausdünnung des Datensatzes auf positiv bewertete Teile, begrenzt werden (für den Hinweis danke ich Dr. Kai Naumann, Stuttgart).

IV.2.1 Übernahme und Ingest

Grundsätzlich gelten in Sachen Datensicherheit, Schutz von Persönlichkeitsrechten, Geheimhaltungsvorschriften „die gleichen Regeln und Qualitätsstandards“ wie bei den Bestandsbildnern.[109] Auch die Übertragung der pseudonymisierten Daten sollte von gleicher Sicherheitsqualität sein wie jene nichtpseudonymisierter Daten.[110] Aufgrund der geringen Erhaltungszeiträume digitaler Unterlagen und ihrer frühen Anbietung kann nicht davon ausgegangen werden, dass Archivzwecke sich in der Regel auf die Daten nicht mehr lebender Personen beziehen.[111] Als nun verantwortliche Stelle ist das Archiv zwar nicht weniger als der Bestandsbildner berechtigt, Depseudonymisierungen vorzunehmen.[112] Es sollte dennoch regelmäßig dann, wenn pseudonymisierte personenbezogene Daten übernommen werden, die getrennte Verwahrung von Daten und Zuordnungsregel erhalten bleiben. Dies gebietet auch der Erhalt der Integrität und Authentizität zum Beweiswert der Unterlagen,[113] der für die gesetzliche Aufgabenerfüllung eines Archivs essenziell ist. Voraussetzung ist, beim Ingest eine separate Speicherung der Zuordnungsregel bei der Formierung der AIPs nach dem OAIS-Modell sicherzustellen und gegebenenfalls den Zugriff durch ein Rechtekonzept einzugrenzen, um anlassbezogene Reidentifizierungen zu ermöglichen. Ferner ist bei kryptographischen Pseudonymisierungen über Softwarelösungen darauf zu achten, die Entschlüsselungsalgorithmen und ihre Funktionalität zu erhalten oder entschlüsselte Versionen gesondert abzulegen.

Zusätzlich kann eine Befreiung von datenschutzrechtlichen Pflichten zur Erfüllung der Betroffenenrechte vorliegen, nämlich dort, wo unter der Derogation des Auskunftsrechts nach Art. 15 DSGVO für Archivzwecke eine Nennung des Namens die Voraussetzung dieser Pflichterfüllung ist und eine Depseudonymisierung aufgrund ihrer TOMs nur aufwendig erfolgen kann.[114]

---

[109] LVR-AFZ: Handreichung, S. 11.

[110] Vgl. zur Übertragungssicherheit Keitel: Aussonderung, S. 81.

[111] Vgl. dagegen Pötters, in: Gola DSGVO, Art. 89, Rn. 22.

[112] Das gilt insbesondere bei Pseudonymisierungen „als reine Schutzmaßnahme“, also zur risikomindernden Wirkung, vgl. Schwartmann/Weiß: Entwurf Code of Conduct, S.17. Im Fall (digitaler) Zwischenarchive ist dringend darauf zu achten und festzulegen, wer zur Reidentifizierung berechtigt ist.

[113] EAG: Guidance, S. 24f.

[114] Vgl. Schwartmann/Weiß: Whitepaper, S. 17; Arning/Rothkegel, in: Taeger: DSGVO, Art. 4, Rn. 122 in Bezug auf Art. 11 DSGVO; für Datenschutzgesetze § 14 Abs. 2 LDSG BW; Art. 26 Abs. 3 BayDSG; § 28 Abs. 2 BDSG; § 25 Abs. 2 HDSIG; § 24 Abs. 3 SDSG; für Archivgesetze § 11 Abs. 1 ArchG

IV.2.2 Im Digitalen Magazin

Eine nachträgliche Pseudonymisierung von personenbezogenem Archivgut zur Risikominimierung ist ebenfalls schwer mit dem gesetzlichen Auftrag ins Reine zu bringen und generell nicht zweckmäßig. Laut den Richtlinien der EAG können Archive sie anwenden, wenn die Maßnahme vollständig reversibel ist und auf eine Weise geschieht, die den Beweiswert nicht gefährdet.[115] Es müsste auch im Rahmen einer DSFA beachtet werden, dass bei hohem Risiko durch besonders sensible Daten die Verarbeitungsprozesse in einem Archiv gegenüber jenen beim Bestandsbildner verschieden sind, sich somit Kontext und Risiken unterscheiden können: Die Anzahl der Personen, die im Archiv arbeiten, Zugriff haben und tatsächlich zugreifen, ist meist ohnehin nicht besonders hoch. Bei der Abwägung der Faktoren Stand der Technik, Kosten einer Implementierung, Umfang, Verarbeitungszwecke und vor allem auch der Eintrittswahrscheinlichkeiten eines Missbrauchs gilt es zu bedenken, welche anderen TOMs einen Datendiebstahl aus digitalen Magazinen verhindern, etwa die ebenfalls in der DSGVO angeführte Verschlüsselung.[116]

Auf der Basis einer Erschließung durch Metadaten-Import sind ohne Hinzuziehung der Zuordnungsregel pseudonymisiert übernommene Daten auch in der Erschließungssoftware zunächst pseudonymisiert. Auch notwendige Ergänzungen lassen sich ohne Auflösung der Pseudonymisierung durchführen. Recherchen zu vielen Forschungszwecken dürften bereits mit diesen Informationen möglich sein.[117] Anders als bei einer Erschließung analoger Unterlagen ist eine maschinelle Depseudonymisierung der Erschließungsdaten digitaler Unterlagen bei Vorliegen einer digitalen Zuordnungsregel, wenn die Schutzfristen abgelaufen sind, ein eher überschaubarer Arbeitsaufwand.[118] Über diesen Weg wäre auch die Pseudonymisierung des DIP faktisch aufgehoben, ohne die Integrität

---

Mecklenburg-Vorpommern; § 5 Abs. 1 und 2 BremArchivG; § 8 Abs. 1 BbgArchivG; § 14 Abs. 1 BArchG; § 6 Abs. 1 SächsArchivG.

[115] EAG: Guidance, S. 13: „In case of personal data preserved for archiving purposes in the public interest, archive services should store unaltered original data in a protected storage facility."

[116] Vgl. zur Aufzählung Berger: Öffentliche Archive, S. 335; Gutachten der Datenschutzbehörden könnten Sicherheit darüber schaffen, ob die TOMs in den Archiven im Sinne der DSGVO ausreichend sind, vgl. van Honacker: EU, S. 28.

[117] Vgl. Schumacher: Vorschläge, S. 16–18.

[118] Zur effizienten Erschließung analoger Akten vgl. Schumacher: Vorschläge, S. 16f.

und Authentizität der originär übernommenen pseudonymen Daten des AIP zu beeinflussen.[119]

IV.2.3 Nutzung

Gleichwohl ist das Herstellen einer pseudonymisierten Kopie als DIP zu Nutzungszwecken in anonymisierender Wirkung eine sinnvolle Maßnahme, um wissenschaftliche Auswertungen vor Ablauf der Schutzfristen zu ermöglichen;[120] stets vorausgesetzt, dass mit ErwG 156 S. 3 DSGVO eine Identifizierung der betroffenen Personen weitgehend ausgeschlossen werden kann. Wurde das Archivgut bereits durch den Bestandsbildner pseudonymisiert, ist zu prüfen, ob die ursprünglich risikomindernde Pseudonymisierung bei einer Vorlage ihrer anonymisierenden Wirkung ausreichend gerecht wird, da sich nun auch die Verarbeitung der Daten ändert und möglicherweise in neue Kontexte gestellt wird.[121] Dies gilt insbesondere bei Big-Data-Auswertungen im Rahmen von wissenschaftlichen und (zeit)historischen Forschungszwecken.[122] Ferner besteht auch nach Ablauf einer Schutzfrist kein Automatismus, der eine Herstellung des Personenbezugs auch nur in den Erschließungsdaten ungeprüft rechtfertigen würde. Das ideelle postmortale Persönlichkeitsrecht kann über die Schutzfristen hinaus noch nicht verblasst sein.[123]

V. Methoden

Die Kenntnis der Pseudonymisierungsmethoden, insbesondere bei den Bestandsbildnern, ist für die bereits ausgeführte archivische Aufgabenerfüllung essenziell. Zu den Basisanforderungen der Pseudonymisierung gehört, dass zusätzliche Informationen zur

---

[119] Vgl. zur faktischen Aufhebung auch Schwartmann/Weiß: Whitepaper, S. 11; Ernst, in: Paal/Pauly: DSGVO BDSG, Art. 4, Rn. 42; Arning/Rothkegel, in: Taeger: DSGVO, Art. 4, Rn. 126.

[120] Vgl. EAG: Guidance, S. 13; The National Archives: Guide, S. 30; Zur Datenminimierung bei Findbuchinformationen insbesondere Schumacher: Vorschläge. Sehr wahrscheinlich können aufgrund der anonymisierenden Wirkung der Pseudonymisierung (relative Anonymisierung) solche Daten für den Nutzer auch als Forschungsdaten an Dritte weitergegeben werden, vgl. Haimberger/Geuer: Anonymisierende Wirkung, S. 58f.

[121] Vgl. Schwartmann/Weiß: Entwurf Code of Conduct, S. 17.

[122] Vgl. Berger: Öffentliche Archive, S. 498–500; Roßnagel: Pseudonymisierung, S. 247; zum Problem der Verknüpfung auch Brinkhus: Erschließung, S. 120f.

[123] Vgl. Schumacher: Vorschläge, S. 7f; Manegold: Archivrecht, S. 117–123, dabei kommt es darauf an, ob die Daten tatsächlich die Menschwürde des Verstorbenen tangieren, vgl. ebd., S. 119.

Herstellung des Personenbezugs notwendig sind, diese getrennt aufbewahrt und passende TOMs erfüllt werden.[124] Letztere werden hier genauer vorgestellt.

Es gibt verschiedene Wege, Pseudonyme zu unterscheiden: Nach dem Inhaber der Zuordnungsregel (Betroffener/Verarbeiter/Dritter), der Erzeugung (aus Identitätsdaten/ willkürlich/zufällig), sowie in gesellschaftlicher Verwendung als Personenpseudonym (öffentlich/nichtöffentlich/anonym) oder Rollenpseudonym (Geschäftsbeziehung/Transaktion).[125] Die Anwendung der Methode ist hochgradig abhängig vom Einzelfall, eine „One size fits all"-Lösung ist nicht greifbar.[126] Je nach der zu wählenden Methode der Pseudonymisierung und auch der Art der elektronischer Unterlagen (E-Akte, Fachverfahren, Datenbanken…) dürfte sich der konkrete Workflow der Übernahme pseudonymisierter Daten und ihrer Zuordnungsregel erheblich unterscheiden.[127]

V.1 Organisatorische Maßnahmen

Entsprechend Art. 40 Abs. 2 lit. d DSGVO entwickelte die Fokusgruppe Datenschutz der Plattform „Sicherheit, Schutz und Vertrauen für die Gesellschaft und Wirtschaft" den Entwurf eines „Code of Conduct" als Leitlinien für die Anwendung der Pseudonymisierung.[128] Wichtigste Maßnahme: Es wird ein eigener Fachverantwortlicher für Pseudonymisierung (FvfP) zu Organisation der Pseudonymisierung ernannt, dessen Aufgabe auch eine ganze Abteilung übernehmen kann, der auf jeden Fall aber das nötige Fachwissen vorzuweisen hat.[129] Der FvfP bestimmt die Risikoklasse anhand der Kategorie der personenbezogenen Daten sowie der Verarbeitungen, Betroffenenkategorien und Anzahl,[130] dokumentiert die Verarbeitungszwecke und den rechtlichen Kontext (anonymisierende oder risikomindernde Wirkung der Pseudonymisierung) sowie die Anzahl der so verarbeiteten Datensätze. Er entscheidet ebenfalls über die Pseudonymisierungsart und

[124] Vgl. Schwartmann/Weiß: Whitepaper, S. 10–11; Arning/Rothkegel, in: Taeger: DSGVO, Art. 4, Rn. 124. Die Literatur folgt dabei oft der technischen Terminologie nach dem Verfahren (Pseudonymisierung als eine Ersetzung durch Kennung; Anonymisierung als Weglassen identifizierender Daten), nicht wie die DSGVO nach dem Ergebnis (Wiederherstellbarkeit des Personenbezugs).

[125] Vgl. GMDS: Arbeitshilfe, S. 20.

[126] Vgl. LfD SH (Hg.): 38. Tätigkeitsbericht 2020, S. 127f.

[127] Die medizinische Informatik hat einen eigenen Standard zur Pseudonymisierung, DIN ISO 25237, vgl. GMDS: Arbeitshilfe, S. 30, Anm. 21.

[128] Vgl. Schwartmann/Weiß: Entwurf Code of Conduct, S. 8.

[129] Dieser darf nicht zugleich der Datenschutzbeauftragte des Verantwortlichen sein, weil jener nach Art. 39 DSGVO nur für Beratung und Kontrolle zuständig sein soll, vgl. Schwartmann/Weiß: Entwurf Code of Conduct, S. 10.

[130] Vgl. dazu auch Abschnitt IV.1.1.; Schwartmann/Weiß: Entwurf Code of Conduct, S. 10f.

Pseudonymisierungsmethode und dokumentiert den Weg zu seinen Entscheidungen.[131] Er macht sich ferner Gedanken darüber, unter welchen Bedingungen die pseudonymisierten Daten weitergegeben werden können, was bei einer Verarbeitung in einem Staat außerhalb der DSGVO-Geltung zu beachten ist und wie oft und aus welchen Anlässen eine Depseudonymisierung stattfinden soll.[132] Für den Fall einer unbeabsichtigten oder unrechtmäßigen Depseudonymisierung entwirft er einen Reaktionsplan und überprüft alle zwei Jahre die Erforderlichkeit der Verarbeitung.[133]

Kernstück für die Schutzfunktion organisatorischer Maßnahmen ist ein geeignetes Rechte- und Rollenkonzept.[134] Im Groben unterscheidet man drei Modelle:[135]

- „Alles-in-einer-Hand-Modell“: Die Möglichkeit der Depseudonymisierung liegt beim Verantwortlichen selbst, möglicherweise eingeschränkt auf eine Abteilung oder Person.[136] Wenigstens die Anlässe und Dokumentationspflichten sollten im Vorfeld geklärt werden.
- Treuhändermodell: Eine zusätzliche juristische Person verwaltet die Schlüssel zu Depseudonymisierung „von außen“.[137]
- Mischmodelle: Das Treuhändermodell wird innerhalb einer datenführenden Stelle auf mehreren Hierarchie-Ebenen oder Abteilungen durchgeführt oder eine eigene „dritte Partei“ dafür konstruiert.

Archive müssen diese Rechte- und Rollenkonzepte bei den Bestandsbildnern kennen, um einen Verlust der Zugänglichkeit zu der Zuordnungsregel zu verhindern. Insbesondere die Dokumentationen des FvfP sollten eingesehen und übernommen werden. Für pseudonymisierte Daten und deren Weiterverarbeitung für Forschungszwecke wäre es auch in

---

131 Vgl. Schwartmann/Weiß: Entwurf Code of Conduct, S. 11f.

132 Vgl. Schwartmann/Weiß: Entwurf Code of Conduct, S. 13–15, S. 17; vgl. auch Datenschutzkonferenz: Hinweise, S. 9. Zu diesem Zweck sind passwortgeschützte privilegierte Zugänge, auch chipkartenbasiert oder biometrisch denkbar, vgl. Spindler/Hillegeist: Langzeitarchivierung, Kap. 16:22.

133 Vgl. Schwartmann/Weiß: Entwurf Code of Conduct, S. 18; Arning/Rothkegel, in: Taeger: DSGVO, Art. 4, Rn. 133.

134 Vgl. auch Roßnagel: Pseudonymisierung, S. 243f; Ernst, in: Paal/Pauly: DSGVO BDSG, Art. 4, Rn. 47.

135 Vgl. Schwartmann/Weiß: Entwurf Code of Conduct, S. 16f; ENISA: Pseudonymisation, S. 12f, kennt auch die Pseudonymisierung mit, für und durch einen Datenverarbeiter sowie (S. 14) die Pseudonymisierung durch die Betroffenen selbst, sofern die Verarbeitung es zulässt.

136 Vgl. ENISA: Pseudonymisation, S. 11. Die Personen mit Zugriff auf diese Informationen sollten benannt sein, vgl. Arning/Rothkegel, in: Taeger: DSGVO, Art. 4, Rn. 132 mit Verweis auf ErwG 29 S. 2 DSGVO.

137 Vgl. dazu auch ENISA: Pseudonymisation, S. 14; Arning/Rothkegel, in: Taeger: DSGVO, Art. 4, Rn. 127f.

größeren Archiven mit besonders einschlägigen Beständen ratsam, einen FvfP zu bestimmen. Für den Erhalt einer risikomindernden Wirkung der Pseudonymisierung könnte ein spezielles Rechtekonzept für das Archiv entworfen werden, das Bestimmungen enthält, wer Zugriff auf welche Zuordnungsregeln erhält.

V.2 Technische Maßnahmen

Es gibt eine Reihe von technischen Möglichkeiten zur Durchführung einer Pseudonymisierung, über deren Einsatz je nach Einzelfall zu entscheiden ist. Dabei sind die Methoden jener der Anonymisierung oft verwandt und beziehen auch kryptographische Verschlüsselungsverfahren mit ein. Um überhaupt geeignete Methoden auszuwählen, ist eine Risikoanalyse im Vorfeld unumgänglich.[138] Die Effektivität des Schutzes einerseits und der Handhabbarkeit andererseits sind gegeneinander abzuwägen.[139] Die folgenden Methoden stammen im Wesentlichen aus der Arbeitshilfe zur Pseudonymisierung/Anonymisierung der GMDS und sind mit weiteren Empfehlungen und Richtlinien abgeglichen. Zu unterscheiden sind nichtkryptographische und kryptographische Verfahren, bei denen die Depseudonymisierung über eine Zuordnungstabelle oder über kryptographische Schlüssel erfolgt.[140] Auch eine Trennung nach randomisierenden und generalisierenden Verfahren ist möglich, die Einzelwerte durch Zufallsdaten ersetzen oder durch Verallgemeinerung verschleiern.[141]

In aller Regel, insbesondere bei kryptographischen Verfahren, erfolgt die konkrete Umsetzung der Pseudonymisierung also durch Softwareprogramme. Diese könnten zusätzlich oder als Teil des Fachverfahrens oder Dokumentenmanagementsystems (DMS) zum Einsatz kommen.[142] Die Zuordnungsregel besteht dann aus der Kombination von Schlüssel und Algorithmus. Die konkrete Funktionsweise für den Erhalt der Depseudonymisierungsfunktion ist genau zu untersuchen sowie die künftige Entwicklung der Softwarelösungen bei den Bestandsbildern zu beobachten und mitzugestalten, um

---

[138] Vgl. ENISA: Pseudonymisation, S. 42.
[139] Vgl. ENISA: Recommendations, S. 24.
[140] Vgl. Schwartmann/Weiß: Whitepaper, S. 17; Arning/Rothkegel, in: Taeger: DSGVO, Art. 4, Rn. 128.
[141] Vgl. Datenschutzgruppe nach Artikel 29: Stellungnahme 5/2014, S. 13; Winter u. a.: Herausforderungen, S. 490f.
[142] Diverse Dienstleister lassen sich im Internet leicht aufstöbern. Ein DMS wie *enaio* bietet bisher keine Pseudonymisierungsfunktion, vgl. nur Optimal Systems: Systemhandbuch.

entsprechende Vorkehrungen treffen zu können. Dafür ist bereits im Records Management ein enger Austausch mit den einschlägigen Entwicklern zu empfehlen.[143]

V.2.1 Nichtkryptographische Verfahren

Die *Nichtangabe* bzw. Auslassung eines oder mehrerer identifizierender Merkmale muss nicht zwangsläufig, wie oben bereits erläutert, zu einer Anonymisierung, sondern kann auch zu einer Pseudonymisierung führen, sofern individuelle Einzelangaben übrigbleiben. Dies ist etwa beim „device fingerprinting" der Fall, bei der soziale Netzwerke, die sich selbst als anonymisierend bezeichnen, den genutzten Endgeräten eine ID zuweisen und sich so eine Identifizierungsmöglichkeit bewahren.[144] Üblicherweise wird bei diesem Verfahren eine Spalte eines tabellarischen Datensatzes gelöscht bzw. nicht exportiert.[145]

Die *Maskierung* oder *Ersetzung* hat mit der Nichtangabe gemein, dass sie zu einer Anonymisierung führen kann, aber bei weniger gründlicher Ausführung den Status einer Pseudonymisierung nicht überschreitet.[146] Anstatt aber identifizierende Merkmale auszulassen, werden sie hier durch einen anderen String ersetzt oder abgeändert. Die Arbeitshilfe der GMDS nimmt als Beispiel die Festlegung von zwei Strings „Anne Musterfrau" bzw. „Max Mustermann" anstelle der jeweiligen Namen (wobei die Geschlechterzuordnung erhalten bleibt) und die Veränderung der Geburtsdaten zu Tag und Monat auf den „01.01." eines jeden Jahres.[147]

Die *Mischung* (Shuffeling/Vertauschung) ist eine Methode, die die Werte eines Datensatzes durch eine Zufallsverteilung „verwürfelt", sodass die einzelnen Attribute wie Name, Geburtsdatum und Geburtsort nicht mehr zueinander gehören.[148] Passiert diese Verteilung nicht ganz zufällig („pseudozufällig"), ergibt sich aus der Kenntnis dieser Regel die Zuordnung.

Bei der *Varianzmethode* (stochastische Überlagerung) werden Daten innerhalb bestimmter oder zufälliger Streuungsintervalle verändert. Wenn sich etwa alle

---

[143] Vgl. van Honacker: EU, S. 28.
[144] Vgl. ENISA: Recommendations, S. 14; dagegen die Tabelle in GMDS: Arbeitshilfe, S. 25.
[145] Vgl. GMDS: Arbeitshilfe, S. 20f. Übliche zu löschende Daten sind etwa Name, Anschrift, Personenkennzeichen, Kontonummern und ähnliches, vgl. Roßnagel: Pseudonymisierung, S. 247.
[146] Vgl. ENISA: Recommendations, S. 14: „For instance, in some cases it might be a good practice to involve certain anonymisation techniques (e.g. attributes generalisation) in the pseudonymisation process […]."
[147] Vgl. GMDS: Arbeitshilfe, S. 21f; vgl. auch ENISA: Recommendations, S. 29.
[148] Vgl. GMDS: Arbeitshilfe, S. 22f; Datenschutzgruppe nach Artikel 29: Stellungnahme 5/2014, S. 16f.

Geburtstagsdaten nur um wenige Tage verändern, kommen statistische Auswertungsmethoden dennoch zum gleichen Ergebnis wie bei einer Anwendung unveränderter Daten.[149]

V.2.2 Kryptographische Verfahren

Neben ihrem Einsatz als selbstständige Maßnahme nach der DSGVO ist die kryptographische Verschlüsselung auch mit der Pseudonymisierung zu verbinden. Verschiedene Einsatzmöglichkeiten kommen hier in Betracht.

Bei der *Einwegfunktion* wird eine mathematische Funktion verwendet, bei der das zu pseudonymisierende Datum in eine Funktion eingegeben wird und der Funktionswert anschließend das Pseudonym darstellt. Die Funktion ist so gestaltet, dass die Errechnung des Funktionswerts einfach ist, die umgekehrte Errechnung des Eingabewerts aus dem Funktionswert dagegen schwer („praktisch nicht durchführbar").[150]

Die *kryptographische Hashfunktion* ist eine Art gesteigerte Einwegfunktion. Hier wird aus der beliebig langen Eingabe ein stets gleich langer Hashwert gebildet.[151] Wegen dieser Längenunterschiede kommt es zu Kollisionen (gleicher Hashwert bei verschiedenen Eingaben), die sich praktisch nicht berechnen lassen. Ein wichtiges Stichwort für dieses Verfahren ist die Verwendung von SHA-256 für Hashwerte mit einer Länge von 32 Byte.[152]

Eine Steigerung ist der *Message authentication code* (MAC), bei dem die kryptographische Generierung der Hashfunktion zusätzlich mit einem Schlüssel (Code) verbunden ist, ohne den eine Reidentifizierung nicht möglich ist. Dieses Verfahren wird häufig für Internet-Protokolle genutzt und von der ENISA als ein besonders robustes Verfahren zum Datenschutz bezeichnet.[153]

Auch für eine Pseudonymisierung kommen *Verschlüsselungsverfahren* zum Einsatz, die sich in symmetrische (Verschlüsselung und Entschlüsselung mit gleichem Schlüssel) und asymmetrische Verfahren (Verschlüsselung und Entschlüsselung mit öffentlichem und privatem Schlüssel) unterscheiden lassen. In der Regel arbeiten diese Verfahren deterministisch, sodass aus dem gleichen Schlüssel ein stets gleicher String als Pseudonym entsteht, wenn nach einer Entschlüsselung wieder verschlüsselt wird. Es lassen sich

[149] Vgl. GMDS: Arbeitshilfe, S. 23; Datenschutzgruppe nach Artikel 29: Stellungnahme 5/2014, S. 14f.
[150] Vgl. GMDS: Arbeitshilfe, S. 24 („Hash-Funktionen"); Schwartmann/Weiß: Whitepaper, S. 18.
[151] Vgl. GMDS: Arbeitshilfe, S. 24; ENISA: Pseudonymisation, S. 22.
[152] Vgl. Schwartmann/Weiß: Whitepaper, S. 18; sie wird besonders im Code of Conduct empfohlen, vgl. Schwartmann/Weiß: Entwurf Code of Conduct, S. 22.
[153] Vgl. ENISA: Pseudonymisation, S. 22, S. 33f.

jedoch mit einem gleichen Schlüssel auch unterschiedliche Pseudonyme erzeugen, wenn vor einer erneuten Verschlüsselung ein Zusatzwert dem Klardatum beigefügt und nach der Entschlüsselung entfernt wird (probabilistisches Verfahren).[154] In diesem Fall ist darauf zu achten, dass sich die Pseudonyme eines Datensatzes über die Zeit verändert haben können und es zu Unterschieden in der Historie des Datensatzes kommt.

Um die Anforderungen der DSGVO zu erfüllen, müssen die Verschlüsselungsverfahren dem aktuellen Stand der Technik entsprechen, etwa den aktuellen Richtlinien des BSI.[155] Bewegen sich die Klardaten zudem in einem geringen Wertebereich, müssen zur Vermeidung einer Depseudonymisierung durch Aufzählungsangriffe Salt-Werte ermittelt und mit den Klardaten kombiniert werden, da ansonsten die Erstellung einer Zuordnungstabelle droht.[156] Selbstverständlich bedürfen die Salt-Werte wie auch die notwendigen Schlüssel besonderer Vorkehrungen für eine geeignete Verwahrung.[157]

VI. Schlussbetrachtung

Ausgangspunkt der Untersuchung war die Frage, wie sich die Bestimmungen der Pseudonymisierung in der DSGVO auf die Überlieferungsbildung und die digitale Archivierung auswirken könnten. Ein erstes Ergebnis der Arbeit besteht darin, dass die Pseudonymisierung nach der DSGVO mehr bedeutet, als einen Namen wie „James Bond“ durch „007“ zu ersetzen. Ihre Definition ist von der Methode zur Wirkung hin verschoben: Kernpunkt ist, dass pseudonymisierte Daten durch zusätzliche und gesondert aufbewahrte Informationen personenbeziehbar bleiben. Je nach Perspektive des Verarbeiters und seinen Zugriffsmöglichkeiten zur Zuordnungsregel kann eine anonymisierende Wirkung oder eine nur risikomindernde Wirkung der Pseudonymisierung zum Tragen kommen. Sie wird als Maßnahme in der ganzen DSGVO besonders hervorgehoben, soll andere Maßnahmen aber nicht ausschließen, zumal ihr Einsatz einer Prüfung der Zweckmäßigkeit im Einzelfall unterworfen ist.

[154] Vgl. GMDS: Arbeitshilfe, S. 24; Schwartmann/Weiß: Whitepaper, S. 18; ENISA: Pseudonymisation, S. 22f.
[155] Vgl. Schwartmann/Weiß: Whitepaper, S. 22; BSI: IT-Grundschutz.
[156] Vgl. Schwartmann/Weiß: Whitepaper, S. 22.
[157] Vgl. Schwartmann/Weiß: Whitepaper, S. 22; GMDS: Arbeitshilfe, S. 25.

Trotz ihrer Nennung in Art. 89 Abs. 1 S. 3 DSGVO sind die Anwendungsmöglichkeiten auf die übrigen dort genannten wissenschaftlichen und historischen Zwecke sowie Statistikzwecke höher einzuschätzen als auf die Archivzwecke, da es den Archivzwecken nicht nur um Erkenntnis und Veröffentlichung, sondern auch um Rechtswahrung und Erhaltung der Daten geht. Das relativiert die besondere Bedeutung der Pseudonymisierung für das Archivwesen, schafft sie aber nicht aus der Welt. Dieses Bild zeichnen auch die nationalen Datenschutzgesetze, in denen die Archivzwecke meist von den übrigen Zwecken des Art. 89 DSGVO ohne Erwähnung der Pseudonymisierung separiert sind. Bei den übrigen Zwecken gilt die „gesonderte Speicherung" identifizierender Merkmale nur als Übergang zu einer absoluten Anonymisierung.

Ferner zeigte sich, dass die Archivgesetze etliche implizite Bestimmungen zur Pseudonymisierung enthalten, was sich auf die Definition in der DSGVO zurückführen lässt. Besonders im Kontext der Schutzfristenverkürzungen für die Nutzung finden sich Bestimmungen zur Anonymisierung, die vor allem auf eine anonymisierende Wirkung im Lesesaal abzielen und in Anbetracht des grundsätzlichen Erhalts des Personenbezugs im Archiv auch als Pseudonymisierungen im Sinne der DSGVO für wissenschaftliche und historischen Forschungszwecke verstehbar sind. Im Bereich der Überlieferung wird in Bezug auf § 203 Abs. 1 StGB (insbesondere zu Beratungsstellen) mitunter die Übernahme anonymisierter Unterlagen gefordert. Hier könnte eine gesetzliche Einführung der Pseudonymisierung mit einem streng reglementierten Erhalt der Zuordnungsregel künftig neue Optionen schaffen, diese Daten auch zur Rechtswahrung der Betroffenen zu sichern. Über die Nennung von „Maßnahmen" ist die Pseudonymisierung auch in ihrer risikomindernden Wirkung in etlichen Archivgesetzen indirekt berücksichtigt.

Unter den Auswirkungen auf die Überlieferungsbildung zeigte der Blick auf die Bestandsbildner, dass die Pseudonymisierung immer eine Maßnahme nach Ermessen im Einzelfall ist und daher auch nicht ohne Einzeluntersuchungen klar eingegrenzt werden kann, wo mit pseudonymisierten Beständen zu rechnen ist. Besondere Wachsamkeit ist jedoch immer dort angebracht, wo besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO oder schutzwürdige Personen betroffen sind (im Fall der Beratungsstellen trifft beides zu). Informationen zur Wahl der Pseudonymisierungsmethode können über das Verzeichnis von Verarbeitungstätigkeiten und die Dokumentation der DSFA bezogen werden, die der Bestandsbildner vorhalten können muss, sowie (künftig) über die

Dokumentationen des FvfP. Genaues Augenmerk wird auf die Rechtekonzepte und konkrete technische Umsetzung der Pseudonymisierung mittels Softwarelösungen zu legen sein, damit eine Depseudonymisierung unter dem Dach des Archivs in der Zukunft möglich bleibt. Insbesondere bei kryptographischen Pseudonymisierungsmethoden ist die Übernahme der Schlüssel und Algorithmen unverzichtbar. Eventuell ist im Rahmen einer Erforderlichkeitsprüfung der Erhalt der Zuordnungsregel ausdrücklich zu begründen und zu dokumentieren, wenn es für den Erhalt der Rechtswahrung oder exemplarischer Einzelfälle notwendig ist. Künftig wird sich an der Bearbeitung konkreter Einzelfälle zeigen, wie ein Übernahme-Workflow aussehen kann und welches Vorgehen bei welchen Pseudonymisierungsmethoden sowohl Effektivität als auch Effizienz verspricht.

Für die digitale Archivierung ergab sich die Empfehlung, die Entscheidungen der Bestandsbildner für oder gegen eine Pseudonymisierung tendenziell zu übernehmen und die AIPs entsprechend zu formieren. Weder die Datensicherheit noch die Integrität und Authentizität sollten geringeren Standards folgen als bei den Bestandsbildern. Dies bedeutet aber auch, organisatorische Maßnahmen wie Rechts- und Rollenkonzepte im Archiv zu etablieren. Eine Depseudonymisierung zur besseren Handhabung kann, sofern kein Schutzbedarf mehr vorliegt oder die Struktur der Daten es zulässt, auch über die Erschließungs(meta)daten erfolgen. Für die Nutzer können je nach Schutzbedarf aus nicht pseudonymisierten Daten pseudonymisierte DIPs oder aus pseudonymisierten Daten depseudonymisierte DIPs formiert werden.

Aus der Perspektive der Archive ist die Aufhebung des Personenbezugs etwas, das nur zeitweise bestehen muss, nämlich bis zum Ableben der Betroffenen. Die besondere Einführung der Pseudonymisierung durch die DSGVO hält zwar neue Aufgaben, aber auch neue Chancen bereit. Während die vorliegende Arbeit nur einen kleinen Einblick aus theoretischer Perspektive liefern konnte, gilt es, die rechtlichen und technischen Umsetzungen weiter zu verfolgen und im Rahmen des Records Management zu begleiten, damit letztendlich praxisorientierte Lösungen, etwa im Rahmen spezifisch nationaler Verhaltensrichtlinien für Archive nach Art. 40 Abs. 2 DSGVO, zügig Hilfestellungen leisten können.

VII. Anhang

VII.1 Literaturverzeichnis

AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Hrsg.): Das Standard-Datenschutzmodell. Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 2.0a, 2019, URL: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode.pdf [01.04.2010].

Baumann, Carolin: Die Schutzwürdigkeit von Daten in Personenstansunterlagen und ihr Einfluss auf archivische Arbeitsabläufe, in: Baumann, Carolin/Kober, Steffen (Hrsg.): Personenbezogene Unterlagen im Archiv. Beiträge zu Melde- und Personenstandsunterlagen (Veröffentlichungen der Landesfachstelle für Archive und öffentliche Bibliotheken im Brandenburgischen Landeshauptarchiv 10), Potsdam 2013, 115-164.

Becker, Irmgard Christa: Bewertungshoheit - Bewertungskompetenz, in: Becker, Irmgard Christa/Rehm, Clemens (Hrsg.): Archivrecht für die Praxis. Ein Handbuch (Berliner Bibliothek zum Urheberrecht 10), München 2017, S. 58–71.

Berger, Hannes: Öffentliche Archive und staatliches Wissen. Die Modernisierung des deutschen Archivrechts, Baden-Baden 2019.

Birk, Silke: Die Anpassung des Archivgesetzes für den Freistaat Sachsen an die EU-Datenschutz-Grundverordnung, in: Sächsisches Archivblatt 2/2018, S. 11–12.

Bischoff, Frank M.: Bewertung elektronischer Unterlagen und die Auswirkungen archivarischer Eingriffe auf die Typologie zukünftiger Quellen, in: Archivar 1/67 (2014), S. 40–52.

Brinkhus, Jörn: Erschließung und Findmittel, in: Becker, Irmgard Christa/Rehm, Clemens (Hrsg.): Archivrecht für die Praxis. Ein Handbuch (Berliner Bibliothek zum Urheberrecht 10), München 2017, S. 117–131.

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 200-3. Risikoanalyse auf der Basis von IT-Grundschutz, Verion 1.0, 2017, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_3.pdf [01.04.2020].

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutz-Kompendium (Unternehmen und Wirtschaft), Köln 2020, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.pdf [01.04.2020].

Bundesministerium des Innern (Hrsg.): Organisationskonzept elektronische Verwaltungsarbeit. Baustein Datenschutz und Personaldaten, Version 2.0 an die DSGVO und das neue BDSG angepasst sowie erweitert durch Prof. Dr. Mario Martini, 2018, URL:

https://www.uni-speyer.de/files/de/Lehrst%C3%BChle/Martini/PDF%20Dokumente/eigene%20Texte/2018_OrganisationskonzeptelektronischeVerwaltungsarbeit_GutachtenBMI.pdf [01.04.2020].

Datenschutzgruppe nach Artikel 29 (Hrsg.): Stellungnahme 5/2014 zu Anonymisierungstechniken. Angenommen am 10. April 2014, 0829/14/DE, WP216, 2014, URL: http://www.privacy-regulation.eu/privazyplan/materialien/eu-artikel-29-gruppe-workingpaper/wp216%20DE%20Anonymisierungstechniken%202014%2004%2010.pdf [01.04.2020].

Datenschutzgruppe nach Artikel 29 (Hrsg.): Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 "wahrscheinlich ein hohes Risiko mit sich bringt", 17/DE, WP 248 Rev. 01, 2017, URL: https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Guidelines/WP248_LeitlinienZurDatenschutzFolgenabschaetzung.pdf [01.04.2020].

Datenschutzkonferenz (Hrsg.): Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO (Datenschutzkonferenz), Februar 2018, URL: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Hinweise_Verarbeitungstaetigkeiten.pdf [01.04.2020].

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Hrsg.): DSGVO - BDSG. Texte und Erläuterungen, BFDI - Info 1, Juni 2019, URL: https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO1.pdf [01.04.2020].

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS) (Hrsg.): Arbeitshilfe zur Pseudonymisierung/Anonymisierung, 2018, URL: https://www.gesundheitsdatenschutz.org/download/Pseudonymisierung-Anonymisierung.pdf [01.04.2020].

Dickmann, Frank/Rienhoff, Otto: Medizin, in: Neuroth, Heike/Strathmann, Stefan/Oßwald, Achim; Scheffel, Regine; Klump, Jens; Ludwig, Jens (Hrsg.): Langzeitarchivierung von Forschungsdaten. Eine Bestandsaufnahme 2012, URL: http://nbn-resolving.de/urn:nbn:de:0008-2012031401 [01.04.2020], S. 227–256.

Duranti, Luciana: The Right to Be Remembered and the Duty to Memoria. The Role of Archives in an Increasingly Networked Society, in: Wührer, Jakob/Stockinger, Thomas/Schöggl-Ernst, Elisabeth (Hrsg.): Die Zukunft der Vergangenheit in der Gegenwart 2019, S. 31–38.

European Archives Group (Hrsg.): Guidance on Data Protection for Archive Services. EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector, 2018, URL: https://ec.europa.eu/info/files/guidance-data-protection-archive-services_en [01.04.2020].

European Union Agency for Cybersecurity (ENISA) (Hrsg.): Recommendations on shaping technology according to GDPR provisions. An overview on data pseudonymisation, URL: https://doi.org/10.2824/74954 [01.04.2020].

European Union Agency for Cybersecurity (ENISA) (Hrsg.): Pseudonymisation techniques and best practices. Recommendations on shaping technology according to data protection and privacy provisions, 2019, URL: https://doi.org/10.2824/247711 [01.04.2020].

Gola, Peter (Hrsg.): Datenschutz-Grundverordnung. VO (EU) 2016/679, Kommentar, München ^{2}2018, S. 178–215.

Haimberger, Klara/Geuer, Ermano: Anonymisierende Wirkung der Pseudonymisierung, in: Datenschutz Konkret 3/33 (2018), S. 57–59.

Hänger, Andrea: Das Recht auf Vergessenwerden und die Identität einer Gesellschaft - die geplante EU-Datenschutz-Grundverordnung, in: Forum. Das Fachmagazin des Bundesarchivs 2013, S. 34–38.

Hänger, Andrea: Die Europäische Datenschutzgrundverordnung. Ein Werkstattbericht, in: Becker, Irmgard Christa/Rehm, Clemens/Schäfer, Udo (Hrsg.): Nicht nur Archivgesetze…: Archivarinnen und Archivare auf schwankendem rechtlichem Boden? Best Practice - Kollisionen - Perspektiven, Beiträge zum 22. Archivwissenschaftlichen Kolloquium der Archivschule Marburg (Veröffentlichungen der Archivschule Marburg, Hochschule für Archivwissenschaft Nr. 66), Marburg 2019, S. 41–55.

Heilmann, Ute: Die Anpassung des Niedersächsischen Archivgesetzes an die Vorgaben der Datenschutz-Grundverordnung, in: Archiv-Nachrichten Niedersachsen 22 (2018), S. 139–144.

Hillegeist, Tobias: Rechtliche Probleme der elektronischen Langzeitarchivierung wissenschaftlicher Primärdaten, Göttingen 2012.

Johannes, Paul C.: § 4, V. Archivierung, in: Roßnagel, Alexander (Hrsg.): Europäische Datenschutz-Grundverordnung. Vorrang des Unionsrechts - Anwendbarkeit des nationalen Rechts, Baden-Baden 2017, S. 254–263.

Kaufmann, Dörte: Handlungsbedarf für Archive? Ein Arbeitsbericht aus dem Landesarchiv Saarbrücken über die Umsetzung der EU-Datenschutzgrundverordnung, in: Archivar 3/72 (2019), S. 242–245.

Keitel, Christian: Digitale personenbezogene Unterlagen. Konzepte und Erfahrungen des Landesarchivs Baden-Württemberg, in: Tiemann, Katharina (Hrsg.): Bewertung und Übernahme elektronischer Unterlagen - Business as usual? Beiträge des Expertenworkshops in Münster am 11. und 12. Juni 2013 (Texte und Untersuchungen zur Archivpflege 28), Münster 2013, 46-59.

Keitel, Christian: Aussonderung und Übergabe, in: Becker, Irmgard Christa/Rehm, Clemens (Hrsg.): Archivrecht für die Praxis. Ein Handbuch (Berliner Bibliothek zum Urheberrecht 10), München 2017, S. 72–85.

Keitel, Christian: Zwölf Wege ins Archiv. Umrisse einer offenen und praktischen Archivwissenschaft (Archivwissenschaft), Stuttgart 2018.

Knopp, Michael: Pseudonym-Grauzone zwischen Anonymisierung und Personenbezug, in: Datenschutz und Datensicherheit 8/39 (2015), S. 527–530.

Krüger, Sven: Vergesst ihn!, in: Die Zeit 4 (16. Januar 2020), S. 20.

Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios (Hrsg.): Datenschutzrecht (Jura auf den Punkt gebracht), Heidelberg ^{3}2015.

Landesarchiv Thüringen: Neues Thüringer Archivgesetz in Kraft getreten. Zugang erleichtert, kommunale Archive gestärkt, digitale Archivierung geregelt und Datenschutz an EU-Recht angepasst, in: Archive in Thüringen 2018, S. 6–13.

Landesbeauftragte für den Datenschutz Schleswig-Holstein (Hrsg.): Tätigkeitsbericht 2020 des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein. 38. Tätigkeitsbericht der Landesbeauftragten für Datenschutz, 2019, URL: https://www.datenschutzzentrum.de/tb/tb38/uld-38-taetigkeitsbericht-2020.pdf [01.04.2020].

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg (Hrsg.): 35. Datenschutz-Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg, 2019, URL: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/01/35.-T%C3%A4tigkeitsbericht-f%C3%BCr-den-Datenschutz-Web.pdf [01.04.2020].

LVR-Archivberatungs- und Fortbildungszentrum (Hrsg.): Handreichung. Vorüberlegungen zur Implementierung eines Systems zur elektronischen Langzeitarchivierung, 2018, URL: https://afz.lvr.de/media/archive_im_rheinland/archivberatung/digitale_unterlagen/Handreichung_Implementierung.pdf [01.04.2020].

Manegold, Bartholomäus: Archivrecht. Die Archivierungspflicht öffentlicher Stellen und das Archivzugangsrecht des historischen Forschers im Licht der Forschungsfreiheitsverbürgung des Art. 5 Abs. 3 GG (Schriften zum öffentlichen Recht Bd. 874), Berlin 2002.

Marnau, Ninja: Anonymisierung, Pseudonymisierung und Transparenz für Big Data. Technische Herausforderungen und Regelungen in der Datenschutz-Grundverordnung, in: Datenschutz und Datensicherheit 7/2016, S. 428–433.

nestor-Arbeitsgruppe E-Akte (Hrsg.): Die E-Akte in der Praxis. Ein Wegweiser zur Aussonderung (nestor-Arbeitsgruppe E-Akte), 2018, URL: https://nbn-resolving.org/urn:nbn:de:0008-2018020827 [01.04.2020].

Optimal Systems (Hrsg.): Softwaredokumentation enaio Systemhandbuch DMS, Version 9.0, 2019, URL: https://help.optimal-systems.com/enaio/v90/admin/PDF/OS_Systemhandbuch-DMS_de.pdf [01.04.2020].

Pahl, Henning: Archivrecht, Datenschutz und archivische Praxis, in: Aus evangelischen Archiven 58 (2018), S. 31–46.

Pfitzmann/Hansen (Hrsg.): A terminology for talking about privacy by data minimization: Anonymity, Unlikability, Undectectability, Unobservability, Pseudonymity, and Identity Management, Version v0.34 (TU Dresden), 2010, URL: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml [01.04.2020].

Plath, Kai-Uwe (Hrsg.): BDSG/DSGVO. Kommentar, Köln ^{3}2018.

Rehm, Clemens: Europäische Regelungen. EU-Datenschutzgrundverordnung, in: Becker, Irmgard Christa/Rehm, Clemens (Hrsg.): Archivrecht für die Praxis. Ein Handbuch (Berliner Bibliothek zum Urheberrecht 10), München 2017, 37-40.

Rehm, Clemens: Recht auf Erinnerung: Rechtssicherung durch Überlieferungsbildung, in: Kauertz, Claudia (Hrsg.): Archive im Rechtsstaat. Zwischen Rechtssicherung und Verrechtlichung, 51. Rheinischer Archivtag 6.-7. Juli 2017 in Essen, Beiträge (Archivhefte 49), Bonn 2018, S. 43–61.

Roßnagel, Alexander: Pseudonymisierung personenbezogener Daten. Ein zentrales Instrument im Datenschutz nach der DS-GVO, in: Zeitschrift für Datenschutz 6/2018, S. 243–247.

Schlagk, Patricia: Die datenschutzrechtliche Privilegierung von im öffentlichen Interesse liegenden Archivzwecken, Bachelorarbeit Fachhochschule Potsdam, [Potsdam] 2019, URL: https://nbn-resolving.org/urn:nbn:de:kobv:525-24311 [01.04.2020].

Schumacher, Felix: Vorschläge zum Umgang mit personenbezogenen Daten bei der Erschließung mit ScopeArchiv im Landesarchiv Sachsen-Anhalt, Transferarbeit 2019, [Marburg] 2019.

Schwartmann, Rolf/Jaspers, Andreas/Thüsing, Gregor; Kugelmann, Dieter (Hrsg.): Datenschutz-Grundverordnung. Mit Bundesdatenschutzgesetz (Heidelberger Kommentar, Heidelberg 2018.

Schwartmann, Rolf/Weiß, Steffen (Hrsg.): Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2017. Leitlinien für die rechtssichere Nutzung von Pseudonymisierungslösungen unter Berücksichtigung der Datenschutz-Grundverordnung (Gesellschaft für Datenschutz und Datensicherheit e. V.), 2017, URL: https://www.gdd.de/downloads/whitepaper-zur-pseudonymisierung [01.04.2020].

Schwartmann, Rolf/Weiß, Steffen (Hrsg.): Entwurf für einen Code of Conduct zum Einsatz DS-GVO konformer Pseudonymisierung. Ein Arbeitspapier der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2019 (Gesellschaft für Datenschutz und Datensicherheit e. V.), 2019, URL: https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/p9-code-of-conduct.pdf [01.04.2020].

Spindler, Gerald/Hillegeist, Tobias: Langzeitarchivierung wissenschaftlicher Primärdaten, in: Neuroth, Heike/Oßwald, Achim/Scheffel, Regine; Strathmann, Stefan; Huth, Karsten (Hrsg.): nestor Handbuch. Eine kleine Enzyklopädie der digitalen Langzeitarchivierung, Version 2.3, Göttingen 2010, URL: http://nbn-resolving.de/urn/resolver.pl?urn:nbn:de:0008-2010071949, Kap. 16:14-23.

Steinert, Mark Alexander: Datenschutz-Grundverordnung und öffentliche Archive: bei der Novelle des Archivgesetzes Nordrhein-Westfalen müssen die in der EU-Datenschutz-Grundverordnung vorgesehenen Ausnahmen für öffentliche Archive genutzt werden, in: Städte- und Gemeinderat 73 (2019), S. 6–8.

Taeger, Jürgen/Gabel, Detlev (Hrsg.): DSGVO - BDSG. Kommentar, Frankfurt am Main ^{3}2019.

Taylor, Isabel: Archive und die Entwicklung der europäischen Datenschutz-Grundverordnung, in: Archivar 1/67 (2014), S. 32–39.

The National Archives (Hrsg.): Guide to archiving personal data (The National Archives), 2018, URL: https://www.nationalarchives.gov.uk/documents/information-management/guide-to-archiving-personal-data.pdf [01.04.2020].

van Honacker, Karin: Die EU-Datenschutz-Grundverordnung und ihre Auswirkungen auf Archive: das Beispiel Belgien, in: Archivpflege in Westfalen-Lippe 90 (2019), S. 22–28.

Winter, Christian/Battis, Verena/Halvani, Oren: Herausforderungen für die Anonymisierung von Daten. Technische Defizite, konzeptuelle Lücken und rechtliche Fragen bei der Anonymisierung von Daten, in: Zeitschrift für Datenschutz 11/2019, S. 489–493.

VII.2 Rechtsquellenverzeichnis

Europäische Datenschutzgesetze

DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 (ABl. L 119 vom 4. Mai 2016, S. 1–88) zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
Richtlinie (EU) 2016/680	Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 (ABl. L 119/89 vom 4. Mai 2016, S. 89) zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (JI-Richtlinie)

Nationale Datenschutzgesetze

BayDSG	Bayerisches Datenschutzgesetz vom 15. Mai 2018 (GVBl. S. 230, BayRS 204-1-I), geändert durch § 6 des Gesetzes vom 18. Mai 2018 (GVBl. S. 301)
BbgDSG	Gesetz zum Schutz personenbezogener Daten im Land Brandenburg (Brandenburgisches Datenschutzgesetz – BbgDSG) vom 8. Mai 2018 (GVBl. I Nr. 7)
BDSG a.F.	Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14.01.2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 30.10.2017 (BGBl I S. 3618) m.W.v. 09.11.2017
BDSG n.F.	Bundesdatenschutzgesetz, Artikel 1 des Gesetzes vom 30.06.2017 (BGBl. I S. 2097, in Kraft getreten am 25.05.2018 und geändert durch Gesetz vom 20.11.2019 (BGBl. I S. 16226) m.W.v. 26.11.2019
BlnDSG	Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz – BlnDSG), verkündet als Artikel 1 des Gesetzes vom 13. Juni 2018 (GVBl. S. 418)
BremDSG-VOAG	Bremisches Ausführungsgesetz zu EU-Datenschutz-Grundverordnung vom 8. Mai 2018 (Brem. GBl. Nr. 38, S. 131)
DSG LSA	Gesetz zum Schutz personenbezogener Daten der Bürger (Datenschutzgesetz Sachsen-Anhalt – DSG LSA), in der Fassung der Bekanntmachung vom 13. Januar 2016 (GVBl LSA S. 24), zuletzt geändert durch Artikel 1 des Gesetzes vom 21. Februar 2018 (GVBl. LSA S. 10)

DSG M-V	Datenschutzgesetz für das Land Mecklenburg-Vorpommern, verkündet als Artikel 1 des Gesetzes zur Anpassung des Landesdatenschutzgesetzes und weiterer datenschutzrechtlicher Vorschriften […] vom 22. Mai 2018 (GVOBl. M-V S. 193)
DSG NRW	Datenschutzgesetz Nordrhein-Westfalen, verkündet als Artikel 1 des Nordrhein-Westfälischen Datenschutz-Anpassungs- und Umsetzungsgesetzes EU vom 17. Mai 2018 (GV. NRW. S. 244, 278, 404)
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz vom 3. Mai 2018 (GVBl. S. 82), geändert durch Artikel 5 des Gesetzes vom 12. September 2018 (GVBl. S. 570)
HmbDSG	Hamburgisches Datenschutzgesetz vom 18. Mai 2018, verkündet als Artikel 1 des Gesetzes zur Anpassung des Hamburgischesn Datenschutzgesetzes sowie weiterer Vorschriften an die Verordnung (EU) 2016/679 vom 18. Mai 2018 (HmbGVBl. S. 145)
LDSG BW	Landesdatenschutzgesetz Baden-Württemberg, verkündet als Artikel 1 des Gesetzes zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 vom 12. Juni 2018 (GBl. S. 173)
LDSG RP	Landesdatenschutzgesetz Rheinland-Pfalz vom 8. Mai 2018 (GVBl. 2018, S. 93)
LDSG SH	Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Daten (Landesdatenschutzgesetz – LDSG) vom 2. Mai 2018, verkündet als Artikel 1 des Gesetzes vom 2. Mai 2018 (GVOBl. S. 162)
NDSG	Niedersächsisches Datenschutzgesetz vom 16. Mai 2018, verkündet als Artikel 1 des Gesetzes zur Neuordnung des niedersächsischen Datenschutzrechts (Nds. GVBl. S. 66)
SächsDSDG	Sächsisches Datenschutzdurchführungsgesetz vom 26. April 2018 (SächsGVBl. S. 198, 199), das durch Artikel 2 Absatz 4 des Gesetzes vom 5. April 2019 (SächsGVBl. S. 245) geändert worden ist
SDSG	Saarländisches Datenschutzgesetz vom 16. Mai 2018, verkündet als Artikel 1 des Gesetzes Nr. 1941 zur Anpassung des Saarländischen Datenschutzgesetzes an die Verordnung (EU) 2016/679 vom 16. Mai 2018 (Amtsbl. I S. 254)
ThürDSG	Thüringer Datenschutzgesetz (ThürDSG), verkündet als Artikel 1 des Gesetzes vom 6. Juni 2018 (GVBl. S. 229).

Archivgesetze

ArchG LSA	Archivgesetz Sachsen-Anhalt vom 28. Juni 1995, zuletzt geändert durch Artikel 1 des Gesetzes vom 3. Juli 2015 (GVBl. LSA S. 314).
ArchGB	Gesetz über die Sicherung und Benutzung von Archivgut des Landes Berlin vom 14. März 2016 (GVBl. Nr. 8 vom 24.03.2016, S. 96)
ArchivG NRW	Gesetz über die Sicherung und Nutzung öffentlichen Archivguts im Lande Nordrhein-Westfalen (Archivgesetz Nordrhein-Westfalen – ArchivG NRW) vom 16. März 2010 (GV NRW S. 188), zuletzt geändert am 16. September 2014 (GV NRW S. 603).
BArchG	Gesetz über die Nutzung und Sicherung von Archivgut des Bundes (Bundesarchivgesetz – BArchG) vom 10. März 2017 (BGBl. I S. 410), zuletzt geändert durch Artikel 2 des Gesetzes vom 4. Dezember 2018 (BGBl. I S. 2257)
BayArchivG	Bayerisches Archivgesetz vom 22. Dezember 1989 (GVBl. S. 710), zuletzt geändert durch Gesetz vom 16. Dezember 1999 (GVBl. S. 521)
BbgArchivG	Gesetz über die Sicherung und Nutzung von öffentlichem Archivgut im Land Brandenburg (Brandenburgisches Archivgesetz – BbgArchivG) vom 7. April 1994 (GVBl. I S. 94), zuletzt geändert durch Artikel 25 des Gesetzes vom 8. Mai 2018 (GVBl. I S. 20)
BremArchivG	Gesetz über die Sicherung und Nutzung öffentlichen Archivguts im Lande Bremen vom 7. Mai 1991 (Brem.GBl. S. 159), zuletzt geändert durch Gesetz vom 2. April 2019 (Brem.GBl. S. 133)
HArchivG	Hessen: Gesetz zur Neuregelung des Archivwesens und des Pflichtexemplarrechts vom 26. November 2012 (GVBl. Nr. 24, S. 458), zuletzt geändert durch Artikel 14 des Gesetzes vom 5. Oktober 2017 (GVBl. Nr. 20, S. 297)
HmbArchG	Hamburgisches Archivgesetz vom 21. Januar 1991 (HmbGVBl. S. 7), zuletzt geändert durch Artikel 4 des Gesetzes vom 16. Juni 2005 (HmbGVBl. S. 233)
LArchG BW	Baden-Württemberg: Gesetz über die Pflege und Nutzung von Archivgut (Landesarchivgesetz – LarchG) vom 27. Juli 1987 (GBl. S. 230), zuletzt geändert durch Gesetz vom 17. Dezember 2015 (GBl. S. 1201)
LArchG M-V	Archivgesetz für das Land Mecklenburg-Vorpommern (Landesarchivgesetz – LarchivG M-V) vom 7. Juli 1997 (GVOBl. M-V 1997, S. 282), mehrfach geändert durch Artikel 1 des Gesetzes vom 8. Mai 2018 (GVOBl. M-V S. 172)
LArchG RP	Rheinland-Pfalz: Landesarchivgesetz (LArchG) vom 5. Oktober 1990 (GVBl. 1990, S. 277), zuletzt geändert durch Gesetz vom 27.11.2015 (GVBl. S. 383)

LArchG SH	Gesetz über die Sicherung und Nutzung öffentlichen Archivgutes in Schleswig-Holstein (Landesarchivgesetz – LarchG) vom 11. August 1992 (GVOBl 444), zuletzt geändert am 2. Mai 2018 (GVOBl. S. 162)
NArchG	Gesetz über die Sicherung und Nutzung von Archivgut in Niedersachsen (Niedersächsisches Archivgesetz – NArchG) vom 25. Mai 1993 (Nds. GVBl. 1993, S. 129), zuletzt geändert durch Artikel 3 des Gesetzes vom 16.05.2018 (Nds. GVBl. S. 66)
SächsArchivG	Archivgesetz für den Freistaat Sachsen (SächsArchivG) vom 17. Mai 1993 (SächsGVBl. S. 449), zuletzt geändert durch Art. 25 des Gesetzes vom 26. April 2018 (SächsGVBl. S. 198)
SArchG	Saarländisches Archivgesetz vom 23. September 1992 (Amtsbl. 1992, S. 1094), zuletzt geändert durch das Gesetz vom 22. August 2018 (Amtsbl. I S. 674)
ThürArchivG	Thüringer Gesetz über die Sicherung und Nutzung von Archivgut (Thüringer Archivgesetz – ThürArchivG) vom 29. Juni 2018 (GVBl. S. 308)

Strafgesetzbuch

StGB	Strafgesetzbuch der Bundesrepublik Deutschland vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch gesetz vom 3. März 2020 (BGBl. I S. 431)

VII.3 Abkürzungsverzeichnis

Die gängigsten Abkürzungen sind nicht aufgeführt.

BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
DSFA	Datenschutzfolgenabschätzung
DSGVO	Datenschutzgrundverordnung
DSK	Datenschutzkonferenz (Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder)
EAG	European Archives Group
ENISA	European Network and Information Security Agency
ErwG	Erwägungsgrund
FvfP	Fachverantwortlicher für Pseudonymisierung
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS)
iVm	in Verbindung mit
LfD SH	Landesbeauftragte für den Datenschutz Schleswig-Holstein
LfDI BW	Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg
LVR-AFZ	Landschaftsverband Rheinland – Archivberatungs- und Fortbildungszentrum
MAC	Message authentication code
TOMs	technische und organisatorische Maßnahmen[158]

[158] Englisch „technical and organisational measures", daher Plural-s.