Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

BSI Technische Richtlinie 03138 Ersetzendes Scannen

Bezeichnung:	Ersetzendes Scannen (RESISCAN) Anwendungshinweis R – Unverbindliche rechtliche Hinweise
Kürzel:	BSI TR-03138-R
Version:	1.3
Datum:	05.10.2021

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
1.2	15.06.2018	BSI	LibreOffice Writer
1.3	05.10.2021	BSI	Umstellung auf MS Word, Anpassung der Anlage R im Hinblick auf die Pflicht zur Führung einer Personalakte gemäß Soldatengesetz sowie kleinere Aktualisierungen

Tabelle 1: Änderungshistorie

Autoren

Alexander Roßnagel, Paul C. Johannes Universität Kassel

Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung

Herausgeber

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: resiscan@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

Abkürzungsverzeichnis

ABl.	Amtsblatt
a.F.	Alte Fassung
AO	Abgabenordnung
ArbGG	Arbeitsgerichtsgesetz
Az.	Aktenzeichen
BayEGovG	Gesetz über die elektronische Verwaltung in Bayern (Bayerisches E-Government-Gesetz)
BBG	Bundesbeamtengesetz
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BMV-Ä	Bundesmantelverträge Teil 1 (Ärzte)
BR	Bundesrat
BR-Drs.	Bundesratsdrucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT	Bundestag
BT-Drs.	Bundestagsdrucksache
BVerwG	Bundesverwaltungsgericht
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungssammlung des Bundesverfassungsgerichts
BVV	Verordnung über die Berechnung, Zahlung, Weiterleitung, Abrechnung und Prüfung des Gesamtsozialversicherungsbeitrages
BW-LKHG	Landeskrankenhausgesetz Baden-Württemberg
DB	Der Betrieb (Zeitschrift)
DSGVO	Datenschutz-Grundverordnung
DuD	Datenschutz und Datensicherheit (Zeitschrift)
EstG	Einkommenssteuergesetz
FamFG	Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit
FGO	Finanzgerichtsordnung
eGovG	Gesetz zur Förderung der elektronischen Verwaltung
eGovG NRW	Gesetz zur Förderung der elektronischen Verwaltung in Nordrhein-Westfalen
eIDAS-VO	Verordnung über elektronische Identifizierung und Vertrauensdienste
EU	Europäische Union
GBO	Grundbuchordnung
GDPdU	Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen
GG	Grundgesetz
ggf.	gegebenenfalls
GGO	Gemeinsame Geschäftsordnung der Bundesministerien
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GoB	Grundsätze ordnungsgemäßer Buchführung
GoBS	Grundsätze ordnungsgemäßer DV gestützter Buchführungssysteme
HGB	Handelsgesetzbuch
HS	Halbsatz
IT	Informationstechnologie
i. V. m.	in Verbindung mit
JAktAG	Justizaktenaufbewahrungsgesetz
KGSt	Kommunale Gemeinschaftsstelle für Verwaltungsmanagement
K&R	Kommunikation und Recht (Zeitschrift)

lit.	Litera (Buchstabe)
LKHG	Landeskrankenhausgesetz
MBO-Ä	Musterberufsordnung für Ärzte
MMR	Multimedia und Recht (Zeitschrift)
m. w. N.	mit weiteren Nachweisen
n.F.	Neue Fassung
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NStZ	Neue Zeitschrift für Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZS	Neue Zeitschrift für Sozialrecht
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz
PDF	Portable Document Format
RegR	Registraturrichtlinie
RöntgenV	Röntgenverordnung
SchrAG	Schriftgutaufbewahrungsgesetz
SGB	Sozialgesetzbuch (die Bücher sind römisch nummeriert)
SGG	Sozialgerichtsgesetz
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen
SigV	Verordnung zur elektronischen Signatur
StPO	Strafprozessordnung
TR	Technische Richtlinie
TzBfG	Teilzeit- und Befristungsgesetz
UAbs.	Unterabsatz
VDG	Vertrauensdienstegesetz
VG	Verwaltungsgericht
VITAKO	Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister in Deutschland
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
z. B.	zum Beispiel
ZDA	Zertifizierungsdiensteanbieter
ZPO	Zivilprozessordnung

Einführung

Die Technische Richtlinie „Ersetzendes Scannen (TR RESISCAN)“ verfolgt das Ziel, die Rechtssicherheit für die Anwender im Bereich des ersetzenden Scannens zu steigern. Papierdokumente, die für die Weiterbearbeitung und Aufbewahrung elektronisch erfasst werden, sollen anschließend vernichtet werden können. Rechtliche Nachteile, die durch den Verlust des Originals entstehen können, sollen durch ein TR RESISCAN konformes Vorgehen soweit wie möglich reduziert werden. Der Anwendungshinweis R stellt dabei einen Zusatz zur TR RESISCAN dar, in dem erläutert wird, in welchen Zusammenhängen das Recht die TR RESICAN beeinflusst hat und welche Bedeutung der TR RESISCAN im Rahmen der rechtlichen Bewertung des ersetzenden Scannens zukommen kann.

Von rechtlicher Seite aus betrachtet, gibt es beim ersetzenden Scannen neben zahlreichen Herausforderungen auch viele Lösungsmöglichkeiten. Die Diskussion mit der Praxis während der Entwicklung und Überarbeitung der TR RESICAN machte aber deutlich, dass es rechtliche Unsicherheiten und Missverständnisse gibt, die einer praxisorientierten Klärung bedürfen. Die hier vorliegenden rechtlichen Hinweise sollen dem Anwender bei der Einordnung und Beantwortung von rechtlichen Fragen und Problemen informativ zur Seite stehen. Der Anwendungshinweis R stellt die aktuelle Rechtslage dar, die inzwischen weitgehend an die Herausforderungen und Möglichkeiten des ersetzenden Scannens angepasst worden ist, die aber noch nicht alle praktischen Nöte der Anwender immer ausreichend berücksichtigt. Gesetzesänderungen können jedoch ausschließlich vom Gesetzgeber vorgenommen werden, der die berechtigten Interessen des Anwenders immer wieder gegen Allgemeininteressen oder die Interessen anderer Beteiligter abzuwägen hat. Er wird die gesetzlichen Vorgaben im Interesse aller fortentwickeln und dabei versuchen, einen gerechten Ausgleich der Interessen zu finden. Soweit technische Verfahren nicht den gesetzlichen Vorgaben entsprechen, wird davon abgeraten, diese anzuwenden, wenn es dem Anwender um das Erreichen einer höchstmöglichen Rechtssicherheit geht.

Zunächst werden im ersten Teil (R.1), in Ergänzung zur theoretischen Anleitung der Schutzbedarfsanalyse in der TR RESISCAN, Hinweise für eine Schutzbedarfsanalyse für verschiedene Typen von Dokumenten gegeben, für deren ersetzendes Scannen in der Praxis der größte Bedarf besteht. Diese sollen der Orientierung dienen; eine beispielhafte Einstufung der Schutzbedarfskategorien ist aufgrund der Heterogenität der einzelnen Dokumententypen nicht möglich. Die Hinweise sollen dem Anwender einen Anstoß geben, die Sicherheitsziele für sich zu gewichten. Dabei sollten alle maßgeblichen Umstände in Betracht gezogen werden. Diese können verbindliche Vorschriften sein, die eine Aufbewahrungsform und -frist regeln, aber auch alle denkbaren eigenen Interessen vor dem Hintergrund des konkreten Anwendungsfalles. Im Hinblick auf datenschutzrechtliche Aspekte muss die Sensitivität der Daten auch aus der Perspektive des Betroffenen berücksichtigt werden.

Im zweiten Teil (R.2) werden ausgewählte rechtliche Fragestellungen einer näheren Betrachtung unterzogen. Untersucht wird die Zulässigkeit des Scannens nach dem geltenden und künftigen Datenschutzrecht, Anforderungen der Dokumentation und Aufbewahrung, Gefährdungen und Schutzmöglichkeiten des Scanprodukts, die Einbeziehung externer Scandienstleistungen, die Einhaltung von besonderen Geheimhaltungspflichten, strafrechtliche Aspekte der Vernichtung von Originaldokumenten und Fragestellungen zur Beweisführung mit elektronischen Dokumenten und Scanprodukten.

Gegenüber der ersten Auflage des Anwendungshinweis R aus dem Frühjahr 2013 haben sich nicht nur vielfältige Erfahrungen mit ersetzendem Scannen angesammelt, die berücksichtigt werden müssen. Zu diesen gehören auch die Erkenntnisse aus der Simulationsstudie „Ersetzendes Scannen“, die im Herbst 2014 in der DATEV e.G. in Nürnberg zur Beweisführung mit ersetzend gescannten Dokumenten unter Beteiligung von Richtern und Rechtsanwälten durchgeführt wurde. Auch rechtliche Änderungen sind zu beachten, wie vor allem

- die Fortentwicklung des deutschen Rechts im Zuge der Digitalisierung vieler Verwaltungs- und Wirtschaftsbereiche – wie etwa durch das E-Government-Gesetz und das E-Justice-Gesetz des Bundes

von 2013, durch viele E-Government-Gesetze der Länder in der Folgezeit sowie durch viele Spezialregelungen in einzelnen Wirtschafts- und Verwaltungsbereiche

- die Fortentwicklung des Rechts der Vertrauensdienste durch die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS-VO) von 2014 und das Vertrauensdienstegesetz (VDG) von 2017, das das Signaturgesetz und die Signaturverordnung aufgehoben hat.
- die Fortentwicklung des Datenschutzrechts durch die Datenschutz-Grundverordnung (DSGVO) von 2016 und durch das an sie angepasste neue Bundesdatenschutzgesetz (BDSG), die beide vom 25. Mai 2018 an gelten werden.

R.1 – Sicherheitsziele und Hinweise zur Schutzbedarfsanalyse

Die Durchführung der fachlichen Schutzbedarfsanalyse setzt voraus, dass für jedes Dokument anhand der Sicherheitsziele „Integrität", „Authentizität", „Lesbarkeit", „Vollständigkeit", „Nachvollziehbarkeit", „Verfügbarkeit", „Verkehrsfähigkeit", „Vertraulichkeit" und „Löschbarkeit" die Schadensauswirkungen im konkreten Fall festgestellt werden. Daher werden in einem ersten Schritt diese Sicherheitsziele auf ihren rechtlichen Ursprung hin untersucht. Dadurch soll verdeutlicht werden, wie diese in Beziehung zueinanderstehen und warum die Erfüllung oder Einhaltung bestimmter Ziele im Interesse des Anwenders steht. Anschließend werden für ausgewählte, in der Praxis häufig zu digitalisierende Dokumententypen spezielle Hinweise für die Schutzbedarfsanalyse gegeben. Diese sind keineswegs abschließend. Sie sollen dem Anwender lediglich als Unterstützung dienen, um den Schutzbedarf im konkreten Fall besser bestimmen zu können.

R.1.1 Sicherheitsziele

Die **Integrität** eines Dokuments gewährleistet, dass das Dokument nicht nachträglich verändert worden ist [RFJK07, S. 44]. Die Beurteilung, ob ein unverändertes Papieroriginal zum Scannen vorliegt, ist unabhängig von der Ausgestaltung des Scanprozesses. Das Sicherheitsziel Integrität bezieht sich in dieser Richtlinie auf das Scanprodukt. Sein Inhalt soll in dem Zustand erhalten bleiben, wie er im Scanprozess erzeugt wurde. Hierfür sollten Veränderungen am elektronischen Dokument von vornherein möglichst verhindert werden. [RFJK07, S. 44]. Darüber hinaus wird im Folgenden auch vom Schutz der Integrität gesprochen, wenn zwar das elektronische Dokument verändert werden kann, diese Veränderungen aber anhand technischer Sicherungsmittel nachvollziehbar sind [RFKJ07, S. 44]. Dann kann zwar das ursprüngliche Scanprodukt nicht mehr reproduziert werden, aber es besteht zumindest das Wissen darum, dass eine Verfälschung stattgefunden und wie sich diese auf das Scanprodukt ausgewirkt hat. Die Integrität dient auch der informationellen Selbstbestimmung, weil die Veränderung von personenbezogenen Daten zu einer Speicherung falscher Daten führen kann. Da die Integrität aber auch eine essentielle Rolle bei der Beweissicherheit von Dokumenten spielt, dient sie vor allem dem Schutz des Rechtsverkehrs als öffentliches Interesse und damit dem Rechtsstaatsprinzip (vgl. [Roßn13, § 1 SigG, Rn. 8]; [Roßn16a, S. 27 und 179 ff.]).

Mit der **Authentizität** eines Dokuments wird sichergestellt, dass die in der Urkunde angegebene Person mit dem tatsächlichen Aussteller der Urkunde übereinstimmt.[1] Diese Funktion ist elementarer Bestandteil eines funktionierenden Rechtsverkehrs. Durch die Authentizität von dokumentierten Willens- und

[1] Bei einem Papierdokument wird die Authentizität durch persönliche Merkmale, z. B. die handschriftliche Unterschrift, bezeugt. Diese kann mittels mikroskopischer, messtechnischer und chemischer Analyseverfahren durch einen Schriftsachverständigen auf ihre Echtheit überprüft werden. Die Echtheit einer Unterschrift lässt sich aus den Druckcharakteristika und weiteren individuellen Merkmalen und Spuren ableiten. So lässt sich z. B. die Entstehungsreihenfolge von Schriftzügen nachvollziehen und das Alter einer handschriftlichen Schreibleistung anhand der verwendeten Tinte bestimmen. Auch mikroskopisch kleine Beschädigungen im Schriftbild lassen Rückschlüsse auf den Urheber zu. Darüber hinaus kann die Echtheit einer gesamten Urkunde untersucht werden. So können Art und Weise der Verfälschung (z. B. Rasuren oder Hinzufügungen) erkannt oder das Dokument auf nicht eingefärbte Schreibdruckrillen (Durchdruckspuren) untersucht werden, mit deren Hilfe eine Zusammengehörigkeit von mehrseitigen Schriftstücken festgestellt werden kann. All diese Merkmale können nur durch Sicherstellung des Spurenmaterials an Originalen erhoben werden. Mit dem Scannen gehen diese Merkmale verloren und sind auf dem Scanprodukt nicht mehr vorhanden oder können durch geringen technischen Aufwand manipuliert werden. Somit kann nicht mehr eindeutig bestimmt werden, ob die Daten vom angegebenen Aussteller stammen [RFJK07, S. 44f.].

Wissenserklärungen können die aus ihnen abzuleitenden Rechte und Pflichten einer konkreten Person zugeordnet werden. Die Forderung nach Authentizität leitet sich daher aus dem Rechtsstaatsprinzip ab.

Die Aufbewahrung der Dokumentation eines Vorgangs dient vor allem dem Zweck, die in der Dokumentation abgelegten Informationen jederzeit abrufen zu können. Erst die **Lesbarkeit** eines Dokuments macht diese Informationen verwertbar. Die Lesbarkeit des Scanprodukts setzt daher voraus, dass eine geeignete Hard- und Software vorhanden ist, um die auf dem Datenträger gespeicherten Informationen für den Betrachter sichtbar zu machen.

Das Gebot der **Vollständigkeit** bezieht sich sowohl auf die Akte als auch den Inhalt. Eine Akte ist vollständig, wenn der Bezug mehrerer, aufgrund eines inneren Zusammenhangs zu einer Sammlung oder Akte zusammengefasster Einzeldokumente sichergestellt ist. Die Vollständigkeit des Inhalts ist gewährleistet, wenn die Zusammengehörigkeit, Reihenfolge und Vollständigkeit der Einzelseiten des mehrseitigen Dokuments sich im elektronische Dokument widerspiegeln [RFJW08, S. 53] Es sind Maßnahmen zu treffen, die die Entnahme oder Verfälschung von Aktenteilen verhindern [KoRa16, § 29 VwVfG, Rn. 1c], z. B. durch Paginierung der einzelnen Seiten oder Zugriffsbeschränkungen. Die Vollständigkeit der Akte oder Sammlung ist Voraussetzung zur Wahrnehmung des Rechts auf Akteneinsicht [KoRa16, § 29 VwVfG, Rn. 1b]. Die inhaltliche Vollständigkeit dient auch der Gedächtnisstütze und der Beweisführung [RFJK07, S. 46f.]. Damit unterstützt das Gebot der Vollständigkeit nicht nur die Verwirklichung des Anspruchs auf rechtliches Gehör gemäß Art. 103 GG, sondern zugleich auch der Rechtsschutzgarantie nach Art. 19 Abs. 4 GG auf ein faires und effektives Verfahren.

Das Gebot der **Nachvollziehbarkeit** beschreibt den Umstand, dass der dokumentierte Vorgang durch eine unabhängige Stelle unter alleiniger Zuhilfenahme der Akte rekonstruierbar ist. Der der Akte zugrunde liegende Sachverhalt muss also aus sich heraus verständlich[2] sein; hierzu können auch alle Metadaten der Akte herangezogen werden. Die Nachvollziehbarkeit dient also der ordnungsgemäßen Kontrolle von Vorgängen als Voraussetzung eines rechtsstaatlichen, fairen Verfahrens, und damit der Gewährung effektiven Rechtsschutzes.

Die **Verfügbarkeit** ist dann gegeben, wenn Anwendungen und Informationen zu jeder Zeit durch den Anwender abgerufen werden können [BSI-GSK, S. 49]. Sie stellt damit eine Grundanforderung der Dokumentationspflicht[3] dar, denn eine Dokumentation kann ihren Zweck, z. B. als Gedächtnisstütze oder zur Beweiserleichterung, nur erfüllen, wenn auf die Informationen zugegriffen werden kann.

Die **Verkehrsfähigkeit** bezeichnet bei Originaldokumenten die jederzeitige Verfügbarkeit des Inhalts ohne technische Hilfsmittel [Musi17, § 415 ZPO, Rn. 5]. Die Verkehrsfähigkeit eines elektronischen Dokuments ist dann erreicht, wenn es in den Rechtsverkehr gebracht, insbesondere einem Gericht als Beweismittel vorgelegt werden kann. Dabei muss sichergestellt sein, dass durch entsprechende Sicherungsmittel kein Qualitätsverlust eintritt [RFJW08, S. 99].

Die **Vertraulichkeit** dient dem Schutz vor unbefugter Preisgabe von Informationen [BSI-GSK, S. 49]. Zum grundrechtlichen Schutz der Persönlichkeit gehört auch der Schutz personenbezogener Daten. Dies gilt vor allem in Anbetracht stetiger Nutzung informationstechnischer Systeme, mit deren Hilfe Daten erhoben und gespeichert werden können, die durch Auswertung weitreichende Rückschlüsse auf die Person ermöglichen [BVerfGE 120, S. 305]. Die Vertraulichkeit ist auch bezogen auf Inhalte zu gewähren, die einem bestimmten Berufsgruppen, zum Beispiel Ärzten, Rechtsanwälten, Steuerberatern und Seelsorgern, auferlegten Geheimnisschutz unterliegen oder ein Betriebs- oder Geschäftsgeheimnis darstellen. Die Wahrung der Vertraulichkeit setzt in der Regel voraus, dass der Zugang zu Daten nur einem bestimmten Kreis von Berechtigten gewährt wird und die Daten vor unberechtigtem Verbreiten geschützt werden. Diese Anforderungen leiten sich aus verschiedenen grundrechtlichen Garantien ab, nicht zuletzt aus dem

[2]Dieses Kriterium wurde dem Urteil des AG Köln, Urteil vom 17.1.2011, Az. 142 C 500/09, zu Grunde gelegt.

[3]Vorschriften zur Dokumentationspflicht finden sich in vielen Bereichen. Darauf wird jeweils im Zusammenhang mit dem jeweiligen Dokumententyp bei den Hinweisen zur Schutzbedarfsanalyse im Kapitel R.1.2 auf S. 1212 ff. eingegangen.

Grundrecht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.

Die **Löschbarkeit** von Daten wird von Löschpflichten wie z. B. §§ 20 Abs. 2 und 35 Abs. 2 Bundesdatenschutzgesetzes (BDSG a.F.) oder Art. 17 Abs. 1 DSGVO gefordert und unterstützt das Erreichen der Grundsätze der Datenvermeidung und Datensparsamkeit des § 3a Satz 1 BDSG und der Datenminimierung des Art. 5 Abs. 1 lit. c DSGVO. Personenbezogene Daten sind nur für zuvor definierte Zwecke zu erheben und nur in dem Maße, wie diese zur Erfüllung des Zwecks erforderlich sind [Simi14, § 3a BDSG, Rn. 33]. Gemäß § 3 Abs. 4 Satz 2 Nr. 5 BDSG a.F. versteht man unter Löschen von Daten das Unkenntlichmachen gespeicherter personenbezogener Daten. Es soll unabhängig von einem bestimmten Verfahren bewirkt werden, dass aus den gespeicherten Daten keine Informationen und Erkenntnisse mehr gewonnen werden können [Simi14, § 3 BDSG, Rn. 173].

R.1.2 Hinweise zur Schutzbedarfsanalyse

Um den konkreten Schutzbedarf für zu verarbeitende Datenobjekte zu ermitteln, muss jeder Anwender, wie in der TR RESISCAN dargestellt [BSI-TR03138, S. 17, Maßnahme A.G.2], eine fachliche Schutzbedarfsanalyse durchführen. Hierfür werden im Folgenden einige beispielhafte Betrachtungen zum Schutzbedarf ausgewählter Dokumenttypen vorgestellt, die zur Orientierung dienen sollen. Sie sind unverbindlich. Sie sollen und können eine aktuelle und konkrete Schutzbedarfsanalyse nicht ersetzen. Folgende Dokumententypen werden näher beschrieben:

1. Gerichtsakten
2. Verwaltungsunterlagen
3. Sozialversicherungsunterlagen
4. Medizinische Dokumentation
5. Kaufmännische Buchführungsunterlagen
6. Besteuerungsunterlagen
7. Personalakten.

Zunächst wird für jeden Dokumententyp erläutert, ob und gegebenenfalls unter welchen Voraussetzungen ein ersetzendes Scannen nach der derzeitigen Rechtslage zulässig ist. Anschließend werden für die oben beschriebenen Sicherheitsziele spezielle Hinweise gegeben. Diese sind eine Hilfestellung bei der Einstufung des konkreten Schutzbedarfs des Scanprodukts. Die Schutzbedarfskategorien werden durch typische Schadensauswirkungen beschrieben.[4] Ob die Schadensauswirkungen „nicht nennenswert“, „beträchtlich“, „existentiell bedrohlich“ oder „katastrophal“ sind, ist von einer Vielzahl von Voraussetzungen abhängig, nicht zuletzt von den konkreten Gegebenheiten des jeweiligen Geschäftsvorfalles und Dokumententyps. Die fachliche Schutzbedarfsanalyse ist von jedem Anwender der TR RESISCAN [BSI-TR03138] vor dem Hintergrund dieses konkreten Anwendungsfalls zu prüfen und festzustellen. Aufgrund der Heterogenität der einzelnen Bestandteile einer Akte kann eine pauschale Empfehlung hier nicht gegeben werden. Der konkrete Anwendungsfall ist sehr viel facettenreicher, als dies hier dargestellt werden kann – die Spanne reicht von der Bagatelle bis zum verfahrensentscheidenden Blatt. Der Schutzbedarf muss daher vom Verantwortlichen in jeden Fall selbst bestimmt und eingeordnet werden.

Es werden im Folgenden hauptsächlich bundesrechtliche Vorschriften berücksichtigt. Jede Stelle hat darüber hinaus selbständig zu prüfen, ob für sie spezielles Bundes- oder Landesrecht zur Anwendung kommt.

[4] Zur Definition der Schadenskategorien s. [BSI-TR03138], Tabelle 20, S. 53.

R.1.2.1 Gerichtsakten

Aus dem Rechtsstaatsprinzip des Art. 20 Abs. 1 GG und der Garantie des umfassenden und effektiven Rechtsschutzes nach Art. 19 Abs. 4 GG durch unabhängige Gerichte lässt sich im Interesse einer funktionsfähigen Rechtspflege eine Pflicht zur Führung sowie Aufbewahrung von Akten herleiten [BVerfGE 54, S. 277, 291], [Wilk11, S. 84], [RFJW08, S. 65]. Diese Verpflichtungen ergeben sich aus dem Recht der Verfahrensbeteiligten auf Information über den Verfahrensstoff und lassen sich ausschließlich durch sorgfältige und nachvollziehbare Aktenführung und die Gewährung der Akteneinsicht[5] verwirklichen.

Gerichtsakten der Gerichte und Staatsanwaltschaften, die für ein Verfahren nicht mehr erforderlich sind, sind nach Beendigung des Verfahrens gemäß § 1 Abs. 1 Justizaktenaufbewahrungsgesetz (JAktAG)[6] so lange aufzubewahren, wie ein schutzwürdiges Interesse der Verfahrensbeteiligten oder sonstiger Personen oder ein öffentliches Interesse ihre Erhaltung erfordern. Bei der Bestimmung der Aufbewahrungsfristen ist nach § 2 Abs. 2 Satz 2 Nr. 2 JAktAG ein Interesse der Verfahrensbeteiligten an Ausfertigungen, Auszügen oder Abschriften aus den Gerichtsakten auch nach Beendigung des Verfahrens zu berücksichtigen. Ebenso kann nach § 2 Abs. 2 Satz 2 Nr. 4 JAktAG das Interesse von Verfahrensbeteiligten, Gerichten oder Justizbehörden bestehen, die Gerichtsakten nach Abschluss des Verfahrens für Wiederaufnahmeverfahren, zur Wahrung der Rechtseinheit, zur Fortbildung des Rechts und für sonstige verfahrensübergreifende Zwecke der Rechtspflege zur Verfügung zu haben. Die Vorschriften des Justizaktenaufbewahrungsgesetz gelten für alle von Gerichten und Staatsanwaltschaften geführten Akten, unabhängig von Medium oder Speicherart.[7] Die Aufbewahrungspflicht besteht nach § 1 Satz 2 JAktAG auch für Aktenregister, Namensverzeichnisse und Karteien, auch wenn diese elektronisch geführt werden. Der Aktenbegriff des JAktAG folgt dem der für das jeweilige Gericht geltende Prozessordnung. Unter die Aufbewahrungspflicht fallen nur Bestandteile von Akten, also solche Schriftstücke oder Dateien die aktenwürdig sind und aktenreife haben. Nach § 298a Abs. 1a ZPO werden Prozessakten ab den 1. Januar 2026 zwingend elektronisch geführt.[8] Sie dürfen bereits heute elektronisch geführt werden. Entsprechende Regelungen zur elektronischen Aktenführung gelten in allen übrigen Verfahrensordnungen (vgl. z. B. § 32 StPO). Die technischen und organisatorischen Rahmenbedingungen sollen jeweils durch Rechtsverordnungen bestimmt werden.

Die Prozessordnungen enthalten ergänzende Vorschriften zur Führung und Aufbewahrung von Prozessakten. Um im Gerichtsverfahren eine elektronische Aktenführung zu ermöglichen, wurden in den jeweiligen Prozessordnungen entsprechende Regelungen getroffen, z. B. §§ 298 und 298a ZPO für den Zivilprozess, die §§ 32, 32e StPO für das Strafverfahren und § 55b VwGO[9] für den Verwaltungsprozess.[10] Die

[5] Dieses Recht ergibt sich unmittelbar aus dem Recht auf rechtliches Gehör (Art. 103 Abs. 1 GG) und informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) [KoRa16, § 29 VwVfG, Rn. 3], [BLAH12, § 299 ZPO, Rn. 2].

[6] Gesetz zur Aufbewahrung und Speicherung von Akten der Gerichte und Staatsanwaltschaften nach Beendigung des Verfahrens - Justizaktenaufbewahrungsgesetz vom 22.3.2005 (BGBl. I S. 837, 852), das zuletzt durch Artikel 4 des Gesetzes vom 5.7.2017 (BGBl. I S. 2208) geändert wurde. Die Änderungen wurden zum 1.1.2018 wirksam. Mit ihnen wurde das Schriftgutaufbewahrungsgesetz (SchrAG) unbenannt und sein Anwendungsbereich erheblich ausgeweitet, Das JAKtAG gilt für alle Gerichte und Staatsanwaltschaften. Das SchrAG galt nur für Gerichtsakten des Bundes und des Generalbundesanwalts. Rechts- und Verwaltungsvorschriften der Bundesländer, die noch zum SchrAG Entsprechendes regeln, sind aufgehoben worden oder fallen hinter das Bundesrecht.

[7] Das SchrAG stellte noch auf den Begriff des Schriftguts ab, welchen es definierte und für elektronische Akten entsprechend geltend ließ.

[8] Vorschrift seit dem 1.1.2018 in Kraft.

[9] VG Wiesbaden, Urteil vom 26.9.2014, Az. 6 K 691/14.WI.A, Rn. 19.

[10] Identische Regelungen finden sich für Sozialgerichte in § 65b SGG, für Finanzgerichte in § 52b FGO, für Arbeitsgerichte in § 46e ArbGG, für Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit in § 14 FamFG, für die elektronische Grundakte in § 138 GBO; s. auch § 110b OWiG für Bußgeldverfahren.

Vorschriften der Prozessordnungen wurden zum 1.1.2018 einander angeglichen[11] und auch den Vorschriften des Verwaltungsrechts, wie z. B. § 7 eGovG, angepasst [BHR+14, § 7 EGovG, Rn. 6].

Gemäß § 298a Abs. 2 ZPO (insoweit gleichlautend § 32e StPO) sind bei elektronischer Aktenführung, die in Papierform vorliegenden Unterlagen in ein elektronisches Dokument zu übertragen. Dabei ist nach dem Stand der Technik sicherzustellen, dass das elektronische Dokument mit den vorliegenden Schriftstücken und sonstigen Unterlagen bildlich und inhaltlich übereinstimmt. Das elektronische Dokument ist mit einem Übertragungsnachweis zu versehen, der das bei der Übertragung angewandte Verfahren und die bildliche und inhaltliche Übereinstimmung dokumentiert. Zu dokumentieren ist auch der Übertragungszeitpunkt. Dieser Übertragungsnachweis entspricht nicht dem Vermerk nach § 298a Abs. 3 ZPO, denn der Übertragungsnachweis kann automatisiert erstellt werden und muss nicht personalisiert sein [BT-Drs. 17/12634, S. 30]. Wird allerdings ein von den verantwortenden Personen handschriftlich unterzeichnetes gerichtliches Schriftstück übertragen, ist der Übertragungsnachweis mit einer qualifizierten elektronischen Signatur des Urkundsbeamten der Geschäftsstelle zu versehen.

§ 298a ZPO gilt vornehmlich zur Vermeidung von Medienbrüchen bei neu eingereichten Unterlagen auf Papier zur einer vorhandenen elektronischen Akte. Grundsätzlich ist sie aber auch auf die Digitalisierung von Altbeständen von Akten anzuwenden. Nach § 299 a Satz 1 ZPO können zur Vorhaltung eines Datenarchivs Prozessakten abgeschlossener Verfahren auf Bild- (Mikroverfilmung) oder andere (digitalen) Datenträger übertragen werden. Die Übertragung muss nach ordnungsgemäßen Grundsätzen erfolgen.[12] Wenn auch ein schriftlicher Nachweis darüber vorliegt, dass die Wiedergabe mit der Urschrift übereinstimmt, können die Gerichte den Prozessbeteiligten anstelle der Urschriften Ausfertigungen, Auszüge und Abschriften von dem Bild- oder Datenträger erteilen. Werden diese Vorgaben erfüllt, können die Papierakten vernichtet oder zurückgegeben werden [Musi17, § 299a ZPO, Rn. 1].

Es wird grundsätzlich zwischen Akten laufender Verfahren und Akten rechtskräftig abgeschlossener Verfahren differenziert. Allerdings können die Originale in Papierform nach den zivilprozessualen Bestimmungen bereits sechs Monate nach der Übertragung vernichtet werden, sofern sie nicht rückgabepflichtig sind. Diese Frist bemisst sich unabhängig vom Verfahrensstand. Wird die Urschrift oder die Ausfertigung einer Urkunde nach § 420 ZPO im Rahmen einer Beweisaufnahme oder aufgrund einer gerichtlichen Anordnung nach den §§ 142, 273 Abs. 2 Nr. 5 ZPO vorgelegt, soll diese ebenfalls in die elektronische Akte übertragen werden, um diese vollständig zu halten. Das Papierdokument muss aber als Beweismittel erhalten werden [BT-Drs. 17/12634, S. 30]. Für den Strafprozess enthält § 32e Abs. 4 StPO eine inhaltlich vergleichbare Regelung, die allerdings auf eine ausdrückliche Nennung der Vernichtungsmöglichkeit verzichtet und ausschließlich die Mindest- und Höchstaufbewahrungs- bzw. speicherfristen regelt. Darüber, ob ein Dokument im Anschluss an diese Fristen vernichtet oder zurückgegeben werden muss, ist im Strafverfahren nach Maßgabe des jeweiligen Einzelfalles zu entscheiden [BT-Drs. 18/9416]. Für Dokumente, die im Strafverfahren als Beweismittel sichergestellt sind, gelten die Aufbewahrungs- und Speicherfristen gemäß § 32e Abs. 34 Satz 1 StPO ohnehin nicht.

Somit besteht eine grundsätzliche Möglichkeit für das ersetzende Scannen von Gerichtsakten. Aus den oben genannten Regelungen ergeben sich folgende Kriterien für die Ausgestaltung der Aufbewahrung von Gerichtsakten:

- umfassender und effektiver Rechtsschutz,
- funktionsfähige Rechtspflege,
- das Recht auf Akteneinsicht, Ausfertigungen, Auszüge und Abschriften,

[11] Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10.10.2013, BGBl. I S. 3786.

[12] Z. B. Richtlinie für die Mikroverfilmung von Schriftgut in der Rechtspflege und Justizverwaltung enthalten (abgedruckt in Justiz 1976, S. 231) für die Übertragung auf Mikrofilm; TR-RESISCAN für die Digitalisierung.

- die Fortbildung des Rechts sowie
- Vertrauen in die Justiz.

Darüber hinaus existieren noch weitere Kriterien, die allerdings nur bei einer einzelfallbezogenen Schutzbedarfsanalyse herangezogen werden können, wie die Bedeutung des Dokuments im Prozess, z. B. als Beweismittel oder fristwahrendes Schriftstück. Zu beachten ist außerdem, dass sich der Schutzbedarf für einzelne Dokumentenarten aus oder für ein Gerichtsverfahren nach dem Verwender des jeweiligen Dokuments stark unterscheidet. So sind z. B. gerichtlich vollstreckbare Titel[13] für den Verwender, der sich damit an ein Gericht wendet, nur unter Vorlage des Originals vollstreckbar. Vom ersetzenden Scannen ist insoweit diesem abzuraten und das Original aufzubewahren. Das Gericht, das aus einem Titel vollstreckt hat, diesen entwertet und an den Schuldner zurückgegeben hat, kann nach Abschluss des Verfahrens die dazugehörige Akte unter den oben genannten Voraussetzungen ersetzend scannen.

Aus all diesen Gründen kann die hier vorgenommene Schutzbedarfsanalyse nur beispielhaft sein. Es sind die Kriterien im konkret vorliegenden Fall zu bewerten, um den Schutzbedarf für den jeweiligen Anwendungsfall zu ermitteln. Hinsichtlich einer abstrakt-generellen Schutzbedarfsfeststellung für das ersetzende Scannen von Gerichtsakten auf der Grundlage der TR RESISCAN und der Integration dieser in die Organisatorisch-technischen Leitlinien für den elektronischen Rechtsverkehr mit den Gerichten und Staatsanwaltschaften (OR-Leit-ERV) sowie der Ergänzung der Musterrechtsverordnung über die elektronische Aktenführung hatte die Bund-Länder-Kommission für Informationstechnik in der Justiz (BLK) bereits mit Beschluss vom 12. und 13. Mai 2018 um Fortführung der Aktivitäten entsprechend der Planungen der AG Elektronischer Rechtsverkehr gebeten.

Anwendungsgebiet	*Vorschriften zum Ersetzenden Scannen*	*Voraussetzungen für die Vernichtung der Papieroriginale*
Gerichtsakten	Für rechtskräftig abgeschlossene Verfahren: § 299a ZPO für Prozessakten	• Übertragung des Papierdokuments nach „ordnungsgemäßen Grundsätzen“ • Schriftlicher Nachweis über die Überein-stimmung mit der Urschrift
	Für laufende Gerichtsverfahren: §§ 298, 298a ZPO in Papierform eingereichte Schriftstücke	• Übertragungsnachweis im Scanprodukt (Zeitpunkt der Übertragung, angewandtes Verfahren) • Vernichtung der Originale oder Rückgabe nicht vor sechs Monaten nach Übertragung

Tabelle 2: Vorschriften und Voraussetzungen für das ersetzende Scannen von Gerichtsakten am Beispiel der Zivilprozessakte

[13] Tabellenauszüge, Mahnbescheide, Urteile

Grundwerte[14]	*Sicherheitsziel*	*Hinweise zur Einstufung des Schutzbedarfs*
Integrität	Integrität[15]	Der Schutzbedarf erhöht sich *bei laufenden Verfahren*, da jede unsichtbare Veränderung den Ausgang des Prozesses beeinflussen kann.
		Bei abgeschlossenen Verfahren besteht kein Risiko für die ordnungsgemäße Verfahrensdurchführung und Rechtskonformität des Gerichtsverfahrens selbst.
	Authentizität	Ohne einen eindeutigen Bezug zum Aussteller des Originals verliert das Dokument seine Aussagekraft und kann ggf. seine Funktion nicht mehr erfüllen.
	Vollständigkeit	Der Wert einer Akte ergibt sich gerade aus der Gesamtheit der in ihr enthaltenen Einzeldokumente.
	Nachvollziehbarkeit	Vor *Eintritt der Rechtskraft* spricht die Möglichkeit der Vernichtung der Originale sechs Monate nach Übertragung für einen hohen Schutzbedarf.
		Auch *nach dem Eintritt der Rechtskraft* spricht die Möglichkeit der Vernichtung der Verfahrensunterlagen für einen höheren Schutzbedarf. Aktenbestandteile könnten dann immer noch für Entscheidungen über Wiedereinsetzung in den vorigen Stand und Wiederaufnahme eines Verfahrens von Bedeutung sein. Urteile können für weitere Prozesse sowie für die Fortbildung des Rechts von Bedeutung sein.
Verfügbarkeit	Verfügbarkeit	Für *laufende Prozesse* müssen gemäß § 299 ZPO die bei Gericht mit dem Verfahren betrauten Personen auf die Akten zugreifen können und es besteht ein Recht auf Akteneinsicht.

[14] Die Grundwerte (GW) der IT-Sicherheit [BSI-Glossar] verdeutlichen die Zuordnung der Sicherheitsziele zu den Sicherheitsmaßnahmen im Aufbaumodul [BSI-TR03138, S. 16, Abb. 2, sowie S. 29 ff.].

[15] Bei der genauen Einschätzung des Schutzbedarfs sind z. B. die mögliche Schadenshöhe und der genaue Dokumententyp im Gerichtsverfahren zu berücksichtigen.

Grundwerte[14]	*Sicherheitsziel*	*Hinweise zur Einstufung des Schutzbedarfs*
		Für *abgeschlossene Prozesse* könnte ein schutzwürdiges Interesse der Verfahrensbeteiligten oder Dritter sowie ein öffentliches Interesse an der Erhaltung der Akten bestehen.
	Lesbarkeit	*Sowohl bei laufenden als auch bei abgeschlossenen Prozessen* müssen die Dokumente während der Aufbewahrungsfrist dauerhaft sichtbar gemacht werden können.
	Verkehrsfähigkeit	Der Schutzbedarf ist sehr hoch, da die Dokumente während eines laufenden Verfahrens zwischen den Gerichten, Rechtsanwälten sowie den Vertragsparteien ausgetauscht werden müssen (Recht auf Akteneinsicht gemäß § 299 ZPO).
Vertraulichkeit	Vertraulichkeit	Personenbezogene Daten und Geschäftsgeheimnisse müssen vor einer unbefugten Kenntnisnahme geschützt werden können.
	Löschbarkeit	Jede einzelne Akte muss nach Ablauf der jeweiligen Aufbewahrungsfrist gelöscht werden können. Bei ihrer Bestimmung sind nach § 2 Abs. 2 Satz 2 JAktAG auch die Interessen der Verfahrensbeteiligten, Dritter oder der Öffentlichkeit an der weiteren Aufbewahrung zu berücksichtigen.

Tabelle 3: Hinweise zur Schutzbedarfsanalyse für Gerichtsakten

R.1.2.2 Verwaltungsunterlagen

Ebenso wie die Gerichte ist auch die Verwaltung aufgrund des Rechtsstaatsprinzips nach Art. 20 Abs. 2 und Abs. 3 GG und des Grundsatzes des fairen, objektiven und wahrheitsgetreuen Verwaltungsverfahrens zur Aktenführung und zur Dokumentation verpflichtet. Diese Pflicht ergibt sich mittelbar aus dem Recht der Verfahrensbeteiligten auf Akteneinsicht gemäß § 29 VwVfG [BVerfG, NJW 1983, S. 2135], [BVerwG, NVwZ 1988, S. 621f.], [StBS 14, § 29, Rn. 30]. Die allgemeine Dokumentationspflicht umfasst die Aufgabe der Verwaltung, ordnungsgemäß Akten zu führen und alle wesentlichen Vorgänge, die für die Durchführung des Verwaltungsverfahrens und für seine spätere Nachvollziehbarkeit relevant sind, in Niederschriften oder Aktenvermerken festzuhalten, Schriftwechsel aufzubewahren und so den gesamten Vorgang aktenkundig zu machen [StBS14, § 29, Rn. 30], [KoRa16, § 29 Rn. 1b], [BaRo12, § 29 VwVfG, Rn. 8]. Neben dem Gebot der Aktenmäßigkeit werden die Gebote der Vollständigkeit und der wahrheitsgetreuen Aktenführung differenziert [KoRa16, § 29, Rn. 11a], [StBS14, § 29, Rn. 32]. Fehler der Vollständigkeit oder der

inhaltlichen Richtigkeit können im Streitfall zu einer Umkehr der Beweislast führen [OVG Greifswald, NVwZ 2002, S. 104], [StBS14, § 26 VwVfG, Rn. 12].[16]

Die Behörden des Bundes sollen nach § 6 eGovG ihre Akten ab dem 1. Januar 2020 elektronisch führen.[17] § 7 eGovG enthält Vorgaben zum ersetzenden Scannen. Die Regelungen verpflichten nicht zur Digitalisierung von Altbeständen von Papierakten. Die Entscheidung dazu liegt noch im Ermessen der Behörden [BHR+14, § 7 EGovG, Rn. 4] [Roßn13b, S. 2713f.]. § 6 eGovG gilt bereits seit dem 1. August 2013. Anstelle von Papierdokumenten sind deren elektronische Wiedergaben in der elektronischen Akte aufzubewahren. Bei der Übertragung in die elektronische Akte ist nach dem Stand der Technik[18] sicherzustellen, dass die elektronischen Dokumente mit den Papierdokumenten bildlich und inhaltlich übereinstimmen, wenn sie lesbar gemacht werden. Papierdokumente sollen nach der Übertragung vernichtet oder zurückgegeben werden, sobald eine weitere Aufbewahrung nicht mehr aus rechtlichen Gründen oder zur Qualitätssicherung des Übertragungsvorgangs erforderlich ist.[19] Konkrete Vorgaben zum Scanprozess macht das Gesetz nicht.

Auch die Akten- und Geschäftsordnungen des Bundes, der Länder und der Gemeinden sehen neben der papierbasierten auch eine elektronische Aktenführung und Aufbewahrung vor. Nach § 12 der Gemeinsamen Geschäftsordnung der Bundesministerien (GGO)[20] sind elektronische Verfahren in den Arbeitsabläufen dieser Behörden soweit wie möglich zu nutzen. Voraussetzung hierfür ist gemäß § 12 Abs. 2 Satz 1 GGO, dass der Stand und die Entwicklung der Vorgangsbearbeitung jederzeit (im Rahmen der Aufbewahrungsfristen) aus den in Papierform oder elektronisch geführten Akten nachvollziehbar ist [RFJW08, S. 68]. Die Nachvollziehbarkeit setzt insbesondere voraus, dass die Akte vor Veränderungen geschützt ist und die jeweiligen Urheber und Erstellungszeitpunkte der Dokumente dauerhaft festgestellt werden können [Fisc06, S. 39 f.], [AgElVa11, Abs. 11, 22]. Neben der Nachvollziehbarkeit müssen die einzelnen Dokumente zweifelsfrei identifizierbar bleiben, wieder auffindbar sein sowie mit den übrigen Dokumenten desselben Vorgangs in Beziehung gesetzt werden können [StBS14, § 29, Rn. 30]. Gemäß § 12 Abs. 2 GGO sind die Einzelheiten der Dokumenten- und Aktenverwaltung der Bundesministerien der Registraturrichtlinie (RegR)[21] zu entnehmen. Nach der amtlichen Erläuterung zu § 6 RegR können bei ausschließlich elektronisch gespeichertem Schriftgut Eingänge in Papierform, die nicht an den Einsender zurückgeschickt werden, und Ausgänge, bei denen in Papierform abschließend gezeichnet wurde, nach elektronischer Erfassung vernichtet werden, soweit die Aufbewahrung dieser Dokumente nicht von anderen Vorschriften erfasst wird. Konkrete Anforderungen an den Scanprozess werden nicht definiert [Wilk11, S. 91]. sich bis auf wenige Ausnahmen[22] keine differenzierten Regelungen zum ersetzenden Scannen..

Aus den oben genannten Regelungen ergeben sich folgende Kriterien für die Ausgestaltung der Aufbewahrung von Verwaltungsunterlagen:

- Fairness, Objektivität und Wahrheitstreue des Verwaltungsverfahrens (Verbot der Aktenverfälschung),

[16] FG Münster, Urteil vom 24.11.2015, Az. 14 K 1542/15 AO.

[17] Ähnliche Soll-Vorgaben in Bundesländern allerdings mit abweichenden Fristen z. B. § 9 Abs. 3 EGovG NRW ab 1.1.2022, Art. 7 Abs. 1 BayEGovG ab 1.7.2017.

[18] S. hierzu BT-Drs. 17/11473, 30f.

[19] Die Bundesländer regeln Entsprechendes, s. z. B. § 10 EGovG NRW, Art. 7 Abs. 3 BayEGovG.

[20] Abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/themen/moderne-verwaltung/ggo.pdf.

[21] Registraturrichtlinie für das Bearbeiten und Verwalten von Schriftgut in Bundesministerien; abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/themen/moderne-verwaltung/registraturrichtlinie.html.

[22] In einzelnen Bundesländern liegen Verwaltungsvorschriften vor, die die Anwendung der TR-RESISCAN zum ersetzenden Scannen verbindlich vorgeben so z.B. Verwaltungsvorschrift zum ersetzenden Scannen in der Landesverwaltung nach dem E-Government Gesetz Nordrhein-Westfalen Runderlass des Ministeriums für Wirtschaft, Innovation, Digitalisierung und Energie. Stand 17.09.2021

- Recht auf Akteneinsicht,
- Aktenmäßigkeit und
- Vollständigkeit der Aktenführung.

Außerdem sind die Akteninhalte häufig Grundlage für die Bewertungen von Mitarbeitern im öffentlichen Dienst. Sie dienen auch als Beweismittel in Widerspruchs- und Gerichtsverfahren. Bei Aufforderung sind elektronische Akten elektronisch vorzulegen.[23]

Schutzbedarfsanalysen sind bereichs-, behörden- oder sogar amts- und dokumentenspezifisch zu erstellen. Die Kommunale Gemeinschaftsstelle für Verwaltungsmanagement (KGSt) hat in Zusammenarbeit mit kommunalen Praktikern der der Bundes-Arbeitsgemeinschaft der kommunalen IT-Dienstleister in Deutschland (VITAKO) auf Grundlage ihrer Kriterien zur Risikobewertung „Eintrittswahrscheinlichkeit" und „Schadensvolumen" eine exemplarische Analyse des kommunalen Schutzbedarfs für das ersetzende Scannen erstellt [KGSt17, S. 22f]. Danach ist in der Kommunalverwaltung in der Regel davon auszugehen, dass aufgrund eines fehlenden Papieroriginals keine beträchtlichen oder gar katastrophalen Schadensauswirkungen zu erwarten sind. In einer detaillierten Schutzbedarfsanalyse [KGSt17, S. 46 ff.] werden Scanstrategien zu spezifischen Dokumentenarten aufgestellt.

Für die Schutzbedarfsfeststellung können sich Behörden auch an dem Gesetz zum Abbau verzichtbarer Anordnungen der Schriftform im Verwaltungsrecht des Bundes vom 29. März 2017[24] orientieren. In diesem Gesetz hat der Gesetzgeber in 181 unterschiedlichen Gesetzen und Verordnungen 476 Rechtsvorschriften geändert, um Schriftformerfordernisse ganz zu streichen oder um die Möglichkeit der Nutzung einfacher elektronischer Verfahren zu ergänzen [Bund16]. Durch den Verzicht auf die Schriftform nimmt der Gesetzgeber bewusst eine Reduzierung des Beweiswert der verwendeten Dokumente in Kauf und gibt sich mit dem Beweiswert einfacher elektronischer Dokumente zufrieden, um unnötige bürokratische Anforderungen zu verringern. Weitere Orientierungen können die Empfehlungen des IT-Planungsrats für die Zuordnung von Vertrauensniveaus in der Kommunikation zwischen Verwaltung und Bürgerinnen und Bürgern bzw. der Wirtschaft vom 13. März 2015 [IT-P15] haben. Diese beziehen sich zwar auf die Vertrauenserwartung und Vertrauenssicherungen in der Kommunikation, können aber auch auf die kommunizierten Dokumente übertragen werden. Diese Empfehlungen verweisen auf die Technische Richtlinie Elektronische Identitäten und Vertrauensdienste des Bundesamts für Sicherheit in der Informationstechnik (BSI) TR-03017-1, die auch das Thema Vertrauensniveaus und Vertrauensmechanismen bei der Dokumentenübermittlung im Rahmen konkreter Verwaltungsdienstleistungen betrifft.

[23] S. zu § 106 BBG OVG NRW, Beschluss vom 5.4.2016, Az. 1 B 203/16; VG Wiesbaden, Urteil vom 20.1.2015, Az. 6 K 1567/14.WI; VG Köln, Beschluss vom 11.2.2016, Az. 15 L 2263/15.

[24] BGBl. I S. 626.

Anwendungsgebiet	*Vorschriften zum ersetzenden Scannen*	*Voraussetzungen für die Vernichtung oder Rückgabe der Papieroriginale*
Verwaltungsunterlagen	§7 EGovG für Behörden des Bundes	• Papierausgang, soweit nach Übertragung in eine elektronische Wieder¬gabe in eine elektronische Akte eine weitere Aufbewahrung des Originals nicht mehr aus rechtlichen Gründen oder zur Qualitätssicherung des Übertragungsvor-gangs erforderlich ist. • Papiereingang, grundsätzlich wie Papierausgang. Zusätzlich ist vor Vernichtung zu prüfen, ob eine Zurückgabe erfolgen muss oder kann.
	§ 6 RegR für Dokumente der Bundesministerien	• Papiereingang, wenn er nicht an den Einsender zurückgesandt wird • Papierausgang, wenn er abschließend in Papierform gezeichnet ist[25]

Tabelle 4: Vorschriften und Voraussetzungen für das ersetzende Scannen von Verwaltungsunterlagen

Grundwerte[26]	*Sicherheitsziel*	*Hinweise zur Einstufung des Schutzbedarfs*
Integrität	Integrität	Akten dürfen nicht verfälscht werden: Jede Veränderung an bestimmten Dokumenten könnte den Ablauf des Verwaltungsverfahrens beeinflussen, abhängig davon, welchen Einfluss das Dokument auf das Verfahren hat.

[25] Im konkreten Anwendungsfall ist zu prüfen, ob der Dokumentenausgang elektronisch erfolgen kann und ob die Aufbewahrung einer inhaltlich mit dem Ausgangsschreiben übereinstimmenden elektronischen Kopie, die ohne einen Scanvorgang erstellt werden kann, ausreichend ist. Außerdem ist sicherzustellen, dass die Originaldokumente nicht nach anderen Vorschriften aufbewahrungspflichtig sind (amtliche Erläuterung zu § 6 RegR).

[26] Die Grundwerte (GW) der IT-Sicherheit [BSI-Glossar] verdeutlichen die Zuordnung der Sicherheitsziele zu den Sicherheitsmaßnahmen im Aufbaumodul [BSI-TR03138, S. 16, Abb. 2, sowie S. 29 ff.].

Grundwerte[26]	*Sicherheitsziel*	*Hinweise zur Einstufung des Schutzbedarfs*
	Authentizität	Für die Rekonstruktion des Vorgangs muss der jeweilige Urheber (Aussteller des Originals, Ersteller des Transfervermerks etc.) der einzelnen Dokumente und Datenobjekte festgestellt werden können.
	Vollständigkeit	Der Wert einer Akte ergibt sich gerade aus der Gesamtheit der in ihr enthaltenen Einzeldokumente.
	Nachvollziehbarkeit	Dient der ordnungsgemäßen Erfüllung der Aufbewahrungspflicht der Verwaltungsbehörden.
Verfügbarkeit	Verfügbarkeit	*Für laufende Verwaltungsverfahren* muss schnell auf Akten zugegriffen werden können, z. B. zur Wahrnehmung des Rechts auf Akteneinsicht nach § 29 VwVfG.
		Für abgeschlossene Verwaltungsverfahren könnte im Einzelfall ein schutzwürdiges Interesse an der Verfügbarkeit der Akten bestehen, z. B. bei Anträgen auf Wiederaufnahme oder Wiedereinsetzung in den vorherigen Stand
	Lesbarkeit	Die Dokumente müssen jederzeit lesbar gemacht werden können, um das Handeln der Behörden später rekonstruieren und überprüfen zu können.
	Verkehrsfähigkeit	Die Dokumente müssen zwischen den Behörden, Aufsichtsinstanzen, Parlamenten und Verfahrensbeteiligten ausgetauscht werden können.
Vertraulichkeit	Vertraulichkeit	Je nach Sachverhalt enthalten Verwaltungsunterlagen personenbezogene Daten oder andere schützenswerte Daten, z. B. Betriebsgeheimnisse. Diese sind vor unbefugter Kenntnisnahme und Missbrauch zu schützen.

Grundwerte[26]	*Sicherheitsziel*	*Hinweise zur Einstufung des Schutzbedarfs*
	Löschbarkeit	Die Löschbarkeit personenbezogener Daten muss gemäß Art. 17 DSGVO und § 20 Abs. 2 Nr. 2 BDSG a.F. möglich sein, wenn feststeht, dass deren Kenntnis für die in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben nicht mehr erforderlich ist. Das Scanprodukt muss nach Ablauf der Aufbewahrungsfrist löschbar sein.

Tabelle 5: Hinweise zur Schutzbedarfsanalyse für Verwaltungsunterlagen

R.1.2.3 Sozialversicherungsunterlagen

Für den Bereich der Sozialversicherung hat der Gesetzgeber Vorschriften eingeführt, die die Aufbewahrung elektronisch erzeugter und in die elektronische Form gebrachter Dokumente betreffen. Nach § 110a Abs. 2 Satz 1 SGB IV kann die Sozialversicherungsbehörde an Stelle der schriftlichen Unterlagen diese als Wiedergabe auf einem Bildträger oder auf einem anderen dauerhaften Datenträger aufbewahren, soweit dies unter Beachtung der Wirtschaftlichkeit und Sparsamkeit erfolgt und den Grundsätzen der ordnungsgemäßen Aufbewahrung[27] entspricht. Dabei muss gemäß § 110a Abs. 2 Satz 2 SGB IV sichergestellt sein, dass bei der Erfassung und bei der Wiedergabe der schriftlichen Unterlage – wenn sie lesbar gemacht werden – die bildliche und inhaltliche Übereinstimmung mit dem Original gewährleistet ist.[28] Darüber hinaus müssen die Unterlagen während der Dauer der Aufbewahrungsfrist jederzeit zur Verfügung stehen und unverzüglich inhaltlich und bildlich lesbar gemacht werden können. Entsprechend § 110b SGB IV können Unterlagen, die für die öffentlich-rechtliche Tätigkeit nicht mehr erforderlich und nach § 110a Abs. 2 SGB IV digitalisiert wurden, zurückgegeben oder vernichtet werden. Eine Vernichtung darf nach § 110b Abs. 3 SGB IV jedoch nur dann erfolgen, wenn kein Grund zur Annahme besteht, dass durch die Vernichtung der Dokumente schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

Eine Spezialregelung ist § 9 Abs. 5 Satz. 5 BVV, wonach Entgeltunterlagen für die Berechnung der Sozialversicherungsbeiträge nach § 28f SGB IV in Verbindung mit § 8 BVV ersetzend gescannt werden dürfen. Der Scan schriftlicher Entgeltunterlagen mit Unterschriftserfordernis ist mit einer fortgeschrittenen Signatur des Arbeitgebers zu versehen. Dazu kann das nach dem Vierten Sozialgesetzbuch ausgestellte Zertifikat verwendet werden.

Für den Bereich der Sozialversicherung gelten ansonsten die gleichen Regelungen wie für den Bereich der Verwaltung, so dass die Kriterien für die Ausgestaltung der Aufbewahrung von Verwaltungsunterlagen auch auf die Aufbewahrung von Sozialversicherungsunterlagen übertragen werden können:

- Fairness, Objektivität und Wahrheitstreue des Verwaltungsverfahrens (Verbot der Aktenerfälschung),

[27] Nach § 110c Abs. 1 SGB IV können die Spitzenverbände der Träger der Sozialversicherung und die Bundesagentur für Arbeit Verwaltungsvereinbarungen abschließen, die das Nähere zu den Grundsätzen ordnungsgemäßer Aufbewahrung regeln.

[28] Zum 1. Januar 2016 wurde durch das 5. SGB IV-ÄndG die Regelung aufgehoben, dass über die Feststellung der Übereinstimmung ein Nachweis zu führen ist; aufgehoben wurde auch die Vermutungsregel des § 110d SGB IV, die die Vermutung der Richtigkeit der gescannten Dokumente an den Transfervermerk mit qualifizierter elektronischer Signatur knüpfte.

- Recht auf Akteneinsicht gemäß § 25 SGB X,
- Aktenmäßigkeit und
- Vollständigkeit der Aktenführung.

Darüber hinaus existieren noch weitere Kriterien, die allerdings nur bei einer einzelfallbezogenen Schutzbedarfsanalyse herangezogen werden können. Die hier vorgenommene Schutzbedarfsanalyse erfolgt nur beispielhaft. Es sind die Kriterien im konkret vorliegenden (Regel-)Fall zu bewerten, um den Schutzbedarf für den jeweiligen Anwendungsfall zu ermitteln. Es existiert bisher keine exemplarische Schutzbedarfsanalyse oder Musterverfahrensanweisung für Sozialversicherungsunterlagen. Rechtliche und praktische Hinweise zum ersetzenden Scannen von Sozialversicherungsunterlagen unter Bezugnahme auf die TR-RESISCAN erteilt das Bundesversicherungsamt mit dem Leitfaden „Elektronische Kommunikation und Langzeitspeicherung elektronischer Daten“ [ADBV16, S. 39 ff.].

Anwendungsgebiet	*Vorschriften zum ersetzenden Scannen*	*Voraussetzungen für die Vernichtung oder Rückgabe der Papieroriginale*
Sozialversicherungsunterlagen	§ 110a Abs. 2 SGB IV	Übertragung nach den Grundsätzen ordnungsgemäßer Aufbewahrung. Dabei gilt insbesondere zu beachten: • Speicherung auf einem dauerhaften Träger • bildliche und inhaltliche Übereinstimmung • jederzeitige lesbare Verfügbarkeit.
	§ 9 BVV i.V.m. § 28f SGB IV	Der Scan von Entgeltunterlagen mit Schriftformerfordernis muss mit einer fortgeschrittenen Signatur gesichert werden.

Tabelle 6: Vorschriften und Voraussetzungen für das ersetzende Scannen von Sozialversicherungsunterlagen

Grundwerte[29]	*Sicherheitsziel*	*Hinweise zur Einstufung des Schutzbedarfs*
Integrität	Integrität	Jede Veränderung an bestimmten Dokumenten könnte den Ablauf des Sozialversicherungsverfahrens beeinflussen, abhängig davon, welchen Einfluss das Dokument auf das Verfahren hat. Das Verbot der Aktenverfälschung soll sich daher im Schutzbedarf niederschlagen.

[29] Die Grundwerte (GW) der IT-Sicherheit [BSI-Glossar] verdeutlichen die Zuordnung der Sicherheitsziele zu den Sicherheitsmaßnahmen im Aufbaumodul [BSI-TR03138, S. 16, Abb. 2, sowie S. 29 ff.].

Grundwerte[29]	*Sicherheitsziel*	*Hinweise zur Einstufung des Schutzbedarfs*
	Authentizität	Für die Rekonstruktion des Vorgangs muss der jeweilige Urheber (Aussteller des Originaldokuments, Ersteller des Transfervermerks etc.) der einzelnen Dokumente und Datenobjekte festgestellt werden können.
	Vollständigkeit	Der Wert einer Akte ergibt sich aus der Gesamtheit der in ihr enthaltenen Einzeldokumente.
	Nachvollziehbarkeit	Dient der ordnungsgemäßen Erfüllung der Aufbewahrungspflicht der Behörden.
Verfügbarkeit	Verfügbarkeit	Für *laufende Verfahren* muss unabhängig vom Stand des Verfahrens die jederzeitige Verfügbarkeit der Akte gewährleistet sein, § 110a Abs. 2 Satz 2 Nr. 1b) SGB IV, z. B. für das Recht auf Akteneinsicht gemäß § 25 SGB X.
		Für *abgeschlossene Verfahren* könnte im Einzelfall ein schutzwürdiges Interesse an der Verfügbarkeit der Akten bestehen, z. B. bei Anträgen auf Wiederaufnahme oder Wiedereinsetzung in den vorherigen Stand
	Lesbarkeit	Die Dokumente müssen gemäß § 110a Abs. 2 SGB IV jederzeit lesbar gemacht werden können, um das Handeln der Behörden später rekonstruieren zu können.
	Verkehrsfähigkeit	Die Dokumente müssen zwischen den Behörden, Aufsichtsinstanzen und Verfahrensbeteiligten ausgetauscht werden können.
Vertraulichkeit	Vertraulichkeit	Sozialversicherungsrechtliche Dokumentationen enthalten sensitive personenbezogene Daten, die vor unbefugter Kenntnisnahme und Zugriff zu schützen sind.

Grundwerte[29]	*Sicherheitsziel*	*Hinweise zur Einstufung des Schutzbedarfs*
	Löschbarkeit	Sozialversicherungsunterlagen müssen gemäß § 110b Abs. 1 SGB IV nach Ablauf der jeweiligen Aufbewahrungsfrist gelöscht werden können.

Tabelle 7: Hinweise zur Schutzbedarfsanalyse für Sozialversicherungsunterlagen

R.1.2.4 Medizinische Dokumentation

Die Vorschriften zum Behandlungsvertrag in §§ 630a ff. BGB regeln umfassend die zuvor durch die Rechtsprechung geprägten Grundsätze des Arzthaftungs- und Behandlungsrechts. Mit der gesetzlichen Regelung soll die Rechtsstellung der Patienten verbessert und die Wahrnehmung von Patientenrechten gegenüber Behandelnden und der eigenen Krankenversicherung gefördert werden [BT-Drs. 17/10488, S. 9]. Die Vorschriften richten sich nicht nur an Ärzte, sondern auch an Angehörige anderer Gesundheits- und Heilberufe wie Heilpraktiker, Psycho- oder Physiotherapeuten [BT-Drs. 17/10488, S. 11].

Hinsichtlich des ersetzenden Scannens ist vor allem die Dokumentation der Behandlung gemäß § 630f BGB von Bedeutung. Diese Pflicht folgt auch aus den eigenen Regelwerken einzelner Berufe, so zum Beispiel § 10 Abs. 5 der Musterberufsordnung für deutsche Ärztinnen und Ärzte (MBO-Ä)[30] oder § 57 Abs. 1 Bundesmantelvertrag-Ärzte (BMV-Ä).[31]

Die medizinische Dokumentation ist gemäß § 630f Abs. 1 BGB in Form einer Patientenakte vom Behandelnden in unmittelbarem zeitlichem Zusammenhang mit der Behandlung zu führen. Gemäß § 630f Abs. 2 Satz 1 BGB ist der Behandelnde verpflichtet, eine umfassende Dokumentation zu erstellen, indem sämtliche aus fachlicher Sicht für die derzeitige oder zukünftige Behandlung wesentlichen Merkmale und Ergebnisse aufgezeichnet werden. Die Aufzeichnung ist nicht abschließend und nennt zum Beispiel Anamnesen, Diagnosen, Befunde, Eingriffe, Aufklärungen und Einwilligungen. Die Patientenakte ist gemäß § 630f Abs. 3 BGB zehn Jahre aufzubewahren, beginnend mit dem Abschluss der Behandlung, soweit nicht nach anderen Vorschriften andere Aufbewahrungsfristen bestehen.

Die medizinische Dokumentation ermöglicht es dem Patienten, Kenntnis über den Behandlungsverlauf zu erlangen. Sie ist damit eine wesentliche Voraussetzung dafür, dass der Patient sein Recht ausüben kann, anderweitig sachkundige Auskünfte über seinen Gesundheitszustand sowie über einen weiteren Behandlungsbedarf einzuholen [RFJW08, S. 74], [Fisc06, S. 34]. Als weitere im Interesse des Patienten liegende medizinische Dokumentationszwecke sind die Therapiesicherung und die Erfüllung der Rechenschaftspflicht der Ärzte anerkannt [LaKe10, § 55, Rn. 5 ff.], [Wilk11, S. 102]. Hingegen ist es umstritten, ob die medizinische Dokumentenerstellung auch zum Zwecke der gerichtlichen und außergerichtlichen Beweissicherung erfolgt und demzufolge den Umfang der zu erstellenden Dokumentation bestimmt [QuZu14, § 12, Rn. 70], [Wilk11, S. 102]. Allerdings ist es angesichts des im medizinischen Bereich hohen Schadensrisikos für den Patienten und seines Unvermögens, selbst eine für die Beweisführung notwendige Dokumentation zu führen, sachgerecht, die Beweissicherung als einen Dokumentationszweck anzusehen [LaKe10, § 55, Rn. 8], [BT-Drs. 17/10488, S. 26]. Dies betrifft insbesondere die Art und Weise der Dokumentation (z. B. hinsichtlich Format, Speichermedium und Metadaten) und

[30](Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte - MBO-Ä 1997, in der Fassung des Beschlusses des 118. Deutschen Ärztetages 2015 in Frankfurt a.M., abrufbar unter http://www.bundesaerztekammer.de/recht/berufsrecht/muster-berufsordnung-aerzte/muster-berufsordnung/

[31]Vertrag vom 21.8.2013, in der Fassung vom 5.12.2017, in Kraft getreten am 1.1.2018, abrufbar unter http://www.kbv.de/media/sp/BMV_Aerzte.pdf.

nicht deren Inhalt. Inhaltlich zum Patienten zu dokumentieren ist nur, was aus medizinischer Sicht erforderlich ist.

Insbesondere im Rahmen der Beweisführung bei Behandlungsfehlern hat die medizinische Dokumentation durch die Regelung des Behandlungsvertrages im Bürgerlichen Gesetzbuch eine besondere Bedeutung gewonnen. Gemäß § 630h Abs. 3 BGB wird vermutet, dass der Behandelnde eine medizinisch gebotene wesentliche Maßnahme und ihr Ergebnis nicht getroffen hat, wenn diese in der Patientenakte nicht aufgezeichnet wurde. Dadurch ist der Behandelnde auch im eigenen Interesse verstärkt dazu angehalten, die medizinische Dokumentation ordnungsgemäß zu führen.

Die Patientenakte kann in Papierform oder originär elektronisch geführt werden. Im Gegensatz zu § 10 Abs. 5 MBO-Ä, der Aufzeichnungen auf elektronischen Datenträgern besonderen Sicherungs- und Schutzmaßnahmen unterwirft, um eine Veränderung, Vernichtung oder unrechtmäßige Verwendung zu verhindern, ist gemäß § 630f Abs. 1 Satz 2 BGB eine Veränderung der Daten zulässig, solange neben dem ursprünglichen Inhalt der Zeitpunkt der Veränderung erkennbar bleibt. Unzulässig ist daher das Löschen von Daten; nur Ergänzungen sind gestattet. Dies ist gemäß § 630f Abs. 1 Satz 3 BGB auch für elektronische Patientenakten durch den Einsatz geeigneter Software sicherzustellen [MüK16, § 630f BGB, Rn. 10] [BT-Drs. 17/10488, S. 26].

Jedoch enthalten weder der neue § 630f BGB noch die Regeln der MBO-Ä oder die BMV-Ä eine ausdrückliche Regelung, nach der es gestattet ist, die papiernen Dokumente nach der Digitalisierung zu vernichten oder eine elektronische Dokumentation in ein anderes Format zu überführen ([RoWi06, S. 2147], [RFJW08, S. 75], a.A. [HuKa17, § 15 Rn. 93]). Das Entfernen oder Vernichten von Blättern, Bildern oder sonstigen Datenträgern ist angesichts der Aufbewahrungspflicht nach § 630f Abs. 1 Satz 2 BGB unzulässig [MüK16, § 630f BGB, Rn. 10].

Am 29. Dezember 2015 ist das Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur Änderung weiterer Gesetze (eHealthG) in Kraft getreten.[32] Das eHealth-Gesetz soll die sektorübergreifende digitale Vernetzung im Gesundheitswesen vorantreiben, den flächendeckenden Aufbau der dafür erforderlichen IT-Infrastruktur im Gesundheitswesen (Telematikinfrastruktur) für den Austausch patientenbezogener Daten absichern und diese als zentrale digitale Infrastruktur für das Gesundheitswesen zukunftsfest gestalten [PaHo16]. Die Einführung dieser digitalen Infrastruktur wird als Beschleuniger für den Einsatz von (ersetzenden) Scanmaßnahmen wirken. Jedoch enthält auch das eHealth-Gesetz keine ausdrückliche Regelung zu Vernichtung von papiernen Dokumenten nach der Digitalisierung.

Einzig in Bezug auf Röntgenbilder und sonstige Aufzeichnungen, die mit einer Röntgenuntersuchung in Zusammenhang stehen, ist eine Digitalisierung mit dem Ziel der anschließenden Vernichtung der Originale nach § 28 Abs. 1 Satz 2 Röntgenverordnung (RöntgenV) zulässig [RFJW08, S. 75], [Wilk11, S. 103]. Sie können nach § 28 Abs. 4 RöntgenV als Wiedergabe auf einem Bild- oder Datenträger aufbewahrt werden, wenn sichergestellt ist, dass die Wiedergaben oder die Daten mit den Bildern oder Aufzeichnungen bildlich oder inhaltlich übereinstimmen und während der Dauer der Aufbewahrungsfrist innerhalb angemessener Zeit lesbar gemacht werden können.[33] Es muss sichergestellt sein, dass während der Aufbewahrungszeit keine Informationsveränderungen und Informationsverluste eintreten können. Nach § 28 Abs. 3 RöntgenV sind Röntgenaufnahmen zehn Jahre und Aufzeichnungen über Röntgenbehandlungen 30 Jahre aufzubewahren.

Aus den oben genannten Regelungen ergeben sich folgende Kriterien für die Ausgestaltung der Aufbewahrung medizinischer Dokumentation:

- Akteneinsicht (Patient),
- Therapiesicherung,

[32] BGBl. I, S.2408.

[33] Aufgrund der Regelung des § 28 RöntgenV muss nach derzeitiger Rechtslage davon ausgegangen werden, dass weder § 630f BGB noch § 10 MBO-Ä, § 57 BMV-Ä oder § 13 EKV so gelesen werden können, dass auch nachträglich digitalisierte Medien von den entsprechenden Vorschriften erfasst werden.

- Erfüllung der Rechenschaftspflicht des Arztes,
- Zuordnung der Verantwortlichkeit sowie
- Beweisführung und Beweissicherung.

Für medizinische Dokumentationen existiert bisher keine allgemeine Schutzbedarfsanalyse oder Musterverfahrensanweisung speziell zum ersetzenden Scannen. Für das Gesundheitswesen wurden jedoch allgemein anerkannte Sammlungen zu unterschiedlichen Dokumentenarten im Zusammenhang mit dem Schriftformerfordernis und elektronischen Signaturen erstellt [CCCE10]. Auf diese kann hinsichtlich der Kategorisierung der Dokumentenarten für eine ausdifferenzierte Schutzbedarfsanalyse für das ersetzende Scannen zurückgegriffen werden.

Anwendungsgebiet	*Vorschriften zum ersetzenden Scannen*	*Voraussetzungen für die Vernichtung der Papieroriginale*
Medizinische Dokumentation	§ 28 Abs. 4 RöntgenV	• Bildliche und inhaltliche Übereinstimmung [34] • Herstellung der Lesbarkeit innerhalb angemessener Zeit • keine Informations-veränderungen und Informationsverluste

Tabelle 8: Vorschriften und Voraussetzungen für das ersetzende Scannen medizinischer Dokumentation

Grundwerte[35]	*Sicherheitsziel*	*Hinweise zur Einstufung des Schutzbedarfs*
Integrität	Integrität	Jede unsichtbare Veränderung könnte den Verlauf einer aktuellen oder zukünftigen Behandlung beeinflussen und unter Umständen die Gesundheit und das Leben des Patienten/der Patientin beeinträchtigen.
	Authentizität	Die Authentizität des Originals – und ggf. der im Rahmen des Scanprozesses daraus abgeleiteten Datenobjekte – ist für mögliche Schadensersatzprozesse von hoher Relevanz.

[34] Bei der Erfassung von medizinisch relevanten Dokumenten (z. B. Röntgenbilder) werden unter Umständen höhere Anforderungen bzgl. der Auflösung der Scanprodukte gestellt. Deshalb müssen die geeigneten Scanparameter jeweils in Abhängigkeit von den verarbeiteten Dokumenttypen gewählt werden.

[35] Die Grundwerte (GW) der IT-Sicherheit [BSI-Glossar] verdeutlichen die Zuordnung der Sicherheitsziele zu den Sicherheitsmaßnahmen im Aufbaumodul [BSI-TR03138, S. 16, Abb. 2, sowie S. 29 ff.].

Grundwerte[35]	*Sicherheitsziel*	*Hinweise zur Einstufung des Schutzbedarfs*
	Vollständigkeit	Der Wert einer Akte ergibt sich aus der Gesamtheit der in ihr enthaltenen Einzeldokumente. Für Patientenakten ist dies von höchster Bedeutung.
	Nachvollziehbarkeit	Nachvollziehbarkeit ist für die ordnungsgemäße ärztliche Dokumentations- und Aufbewahrungspflicht von höchster Relevanz.
Verfügbarkeit	Verfügbarkeit	Medizinische Daten können für die spätere Behandlung des Patienten benötigt werden. Unter Umständen müssen medizinische Daten eines Kindes bis ins hohe Alter aufbewahrt werden, weil ihre Kenntnisse auch dann relevant sein können.
	Lesbarkeit	Die Dokumente müssen bei *laufenden Behandlungen* dauerhaft und schnellstmöglich sichtbar gemacht werden können.
		Auch bei *abgeschlossenen Behandlungen* müssen die Dokumente für eine mögliche weitere Behandlung dauerhaft lesbar gemacht werden können.
	Verkehrsfähigkeit	Besonders wichtig für das Akteneinsichtsrecht des Patienten sowie für den Austausch z. B. zwischen mehreren behandelnden Ärzten und Krankenkassen, aber auch zwischen den Beteiligten und Gerichten im Falle eines Arzthaftungsprozesses.
Vertraulichkeit	Vertraulichkeit[36]	Medizinische Dokumentation enthält besonders schützenswerte personenbezogene Daten besonderer Kategorie gemäß Art. 9 Abs. 1 DSGVO.[37]

[36]Die Vertraulichkeitsanforderungen haben keinen Einfluss auf den Beweiswert des Scanprodukts. Sie dienen ausschließlich dem Schutz der besonderen personenbezogenen Daten des Patienten sowie der Gewährleistung der Schweigepflicht des Arztes. Weiterführende Hinweise zu Letzterem s. Kapitel R.2.4.2, S. 38.

[37]§ 3 Abs. 9 BDSG a.F.

Grundwerte[35]	*Sicherheitsziel*	*Hinweise zur Einstufung des Schutzbedarfs*
	Löschbarkeit	Patientenakten müssen nach Ablauf der jeweiligen Aufbewahrungsfrist gelöscht werden können.

Tabelle 9: Hinweise zur Schutzbedarfsanalyse für medizinische Dokumentation

R.1.2.5 Kaufmännische Buchführungsunterlagen

Gemäß §§ 238 ff. HGB ist jeder Kaufmann zur Buchführung verpflichtet. Aus den Büchern müssen sich seine Handelsgeschäfte und die Lage des Vermögens des Kaufmanns und dessen Entwicklung übersichtlich und nachprüfbar nachvollziehen lassen [KoKR17, § 238, Rn. 4]. Die Buchführungspflicht dient vor allem dem Gläubigerschutz, erfüllt eine Beweissicherungs- und Selbstinformationsfunktion und dient der Sicherung des Rechtsverkehrs [KoKR17, § 238, Rn. 4]. Jeder Kaufmann ist nach §§ 238 ff. HGB verpflichtet, seine Handelsbücher nach den Grundsätzen ordnungsgemäßer Buchführung vollständig, richtig, zeitgerecht und geordnet zu führen; zusammen mit Belegen sowie empfangenen und gesendeten Handelsbriefen sind diese sechs oder zehn Jahre aufzubewahren. In Rechtsstreitigkeiten kann das Gericht gemäß § 258 HGB auf Antrag oder von Amts wegen die Vorlegung der Handelsbücher anordnen.

§ 239 Abs. 4 und § 257 Abs. 3 HGB ermöglichen den Kaufleuten und Handelsgesellschaften, die zur Buchführung verpflichtet sind, die Handelsbücher oder die sonst erforderlichen Aufzeichnungen und Unterlagen statt in Papierform auch als Wiedergabe auf einem Bildträger oder anderen Datenträgern zu führen und aufzubewahren. Unter Datenträger ist jedes Medium zu verstehen, dass es ermöglicht, die Bücher oder Aufzeichnungen unmittelbar und jederzeit reproduzierbar festzuhalten [EBJS14, § 257, Rn. 26]. Dies ermöglicht neben der originär elektronischen Aktenführung auch das Scannen und die elektronische Aufbewahrung, sofern diese im Sinne von § 239 Abs. 4 Satz 1 HGB den „Grundsätzen der ordnungsgemäßen Buchführung“ (GoB) entspricht. Gemäß §§ 239 Abs. 4 Satz 2 und 257 Abs. 3 Satz 1 Nr. 2 HGB muss sichergestellt werden, dass die Daten während der Dauer der Aufbewahrungsfrist verfügbar und jederzeit innerhalb angemessener Frist lesbar gemacht werden können. Die Wiedergabe muss nach § 257 Abs. 3 Satz 1 Nr. 1 HGB mit den empfangenen Handelsbriefen und den Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich übereinstimmen, wenn sie lesbar gemacht werden.

Die „Grundsätze der ordnungsgemäßen Buchführung“ werden für die elektronische Datenverarbeitung durch die „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff“ (GoBD“)[38] spezifiziert und konkretisiert [EBJS14, § 257, Rn. 25].[39] Bei Einhaltung dieser Grundsätze sowie der sonstigen Anforderungen der § 239 Abs. 4 und § 257 Abs. 3 HGB dürfen die Originalunterlagen nach dem Scanvorgang vernichtet werden [EBJS14, § 257, Rn. 22], [RFJW08, S. 73].

Aus den oben genannten Regelungen ergeben sich folgende Kriterien für die Ausgestaltung der Aufbewahrung kaufmännischer Buchführung:

- Gläubigerschutz,
- Beweisführung und Beweissicherung sowie

[38] Die GoBD wurden durch das BMF-Schreiben vom 14.11.2014 veröffentlicht und gelten für alle Veranlagungszeiträume, die nach dem 31.12.2014 beginnen. Die GoBD ersetzten mit Wirkung zum 1.1.2015 die „Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme“ (GoBS) und die „Grundsätze zum Datenzugriff und Prüfbarkeit digitaler Unterlagen“ (GDPdU).

[39] Andere Prüfungsrichtlinien, wie z. B. [IDW RS FAIT 3] für Wirtschaftsprüfer, werden ebenso wie die GoBS von der TR-RESISCAN nicht berührt.

- Schutz des Rechtsverkehrs.

Die hier vorgenommene Schutzbedarfsanalyse erfolgt nur beispielhaft. Es sind die Kriterien im konkret vorliegenden (Regel-)Fall zu bewerten, um den Schutzbedarf für den jeweiligen Anwendungsfall zu ermitteln. Es existiert bisher keine allgemeine exemplarische Musterverfahrensanweisung. Bestehende Verfahrensanweisungen differenzieren nach Dokumentarten. Bestimmte Originaldokumente[40] sind unter Berücksichtigung eventueller sachlicher und zeitlicher Aufbewahrungserfordernisse von der Vernichtung auszunehmen [AWV16, S. 30f].

Anwendungsgebiet	*Vorschriften zum ersetzenden Scannen*	*Voraussetzungen für die Vernichtung der Papieroriginale*
Kaufmännische Buchführungs-unterlagen	§ 239 Abs. 4 HGB für Handelsbücher § 257 Abs. 3 HGB für sonstige Unterlagen	• Einhaltung der Grundsätze der ordnungsgemäßen Buchführung (GoB) • jederzeitige Verfügbarkeit und Herstellung der Lesbarkeit innerhalb angemessener Frist • bildliche Übereinstimmung (empfangene Handelsbriefe, Buchungsbelege), sonst inhaltliche Übereinstimmung (andere Unterlagen)

Tabelle 10: Vorschriften und Voraussetzungen für das ersetzende Scannen von kaufmännischen Buchführungsunterlagen

Grundwerte[41]	*Sicherheitsziel*	*Hinweise zur Einstufung des Schutzbedarfs*
Integrität	Integrität	Der Grundsatz der ordnungsgemäßen Buchführung erfordert die Richtigkeit und Unveränderbarkeit der kaufmännischen Unterlagen. Bei Nichteinhaltung kann dem Kaufmann die Nichtanerkennung seiner Buchführung drohen, woraus ein steuerlicher Nachteil entstehen kann.

[40] Solche, wegen ihrer Beweiskraft, dem mit ihnen verbundenen öffentlichen Glauben oder gesetzlicher Bestimmung mit hoher Bedeutung im Original, wie z. B. notarielle Urkunden, Testate unter Siegelverwendung, Eröffnungsbilanzen und Abschlüsse, Verfahrensdokumentation zur Belegablage, Wertpapiere, Zollpapiere mit fluoreszierendem Original-Stempel.

[41] Die Grundwerte (GW) der IT-Sicherheit [BSI-Glossar] verdeutlichen die Zuordnung der Sicherheitsziele zu den Sicherheitsmaßnahmen im Aufbaumodul [BSI-TR03138, S. 16, Abb. 2, sowie S. 29 ff.].

Grundwerte[41]	*Sicherheitsziel*	*Hinweise zur Einstufung des Schutzbedarfs*
	Authentizität	Aus dem Grundsatz ordnungsgemäßer Buchführung leitet sich zwar eine Pflicht zur Prüfung der Authentizität eingehender Geschäftsbriefe ab, aber gemäß § 14 Abs. 4 UStG ist die Unterschrift kein notwendiger Bestandteil einer vom Kaufmann ausgestellten Rechnung. Daher ist die Zuordnung des Briefes zum ausstellenden Unternehmen über übliche Identifikatoren, z. B. den Briefkopf, ausreichend.
	Vollständigkeit	Der Grundsatz der ordnungsgemäßen Buchführung (GoB) erfordert die lückenlose Erfassung aller Geschäftsvorfälle.
	Nachvollziehbarkeit	Die Nachvollziehbarkeit dient der ordnungsgemäßen Erfüllung der Aufbewahrungspflicht der Kaufleute.[42]
Verfügbarkeit	Verfügbarkeit	Für die Dauer der Aufbewahrungsfrist müssen die Dokumente innerhalb angemessener Frist nutzbar sein.
	Lesbarkeit	Die Lesbarkeit muss innerhalb angemessener Frist hergestellt werden können. Sie ermöglicht z. B. die Prüfbarkeit der Bücher durch einen sachverständigen Dritten.
	Verkehrsfähigkeit	Bei Rechtsstreitigkeiten sind die Handelsbücher auf Anordnung des Gerichtes gemäß §§ 258, 259 HGB durch den Kaufmann vorzulegen.

[42] Die Schadensauswirkung ist in der Regel überschaubar, da finanzielle Grundlagen im Zweifel geschätzt werden können.

Grundwerte[41]	*Sicherheitsziel*	*Hinweise zur Einstufung des Schutzbedarfs*
Vertraulichkeit	Vertraulichkeit	Enthalten Buchführungsunterlagen Betriebs- und Geschäftsgeheimnissen oder personenbezogene Daten, kann eine besondere Sicherung der Daten notwendig sein. Dies gilt besonders, wenn die Digitalisierung durch einen externen Dienstleister durchgeführt wird.
	Löschbarkeit	Gemäß Art. 17 Abs. 1 lit. a DSGVO müssen Daten u.a. gelöscht werden, wenn sie für den Zweck für den sie verarbeitet wurden nicht mehr notwendig sind.[43] Im Fall der Auftragsdatenverarbeitung sind Dienstleister entsprechend zu verpflichten.

Tabelle 11: Hinweise zur Schutzbedarfsanalyse für kaufmännische Buchführungsunterlagen

R.1.2.6 Besteuerungsunterlagen

Gemäß § 147 Abs. 3 AO hat die steuerpflichtige Person die für die Besteuerung relevanten Unterlagen im Sinne von § 147 Abs. 1 Nr. 1, 4, 4a AO zehn Jahre lang und sonstige Unterlagen, z. B. Handels- und Geschäftsbriefe, sechs Jahre lang aufzubewahren. Die Aufbewahrung stellt eine wesentliche Grundlage für die Nachvollziehbarkeit steuerlich relevanter Vorgänge und ihrer Kontrolle durch das zuständige Finanzamt dar [Klei16, § 147, Rn. 1], [Fisc06, S. 42].

Mit Ausnahme der Jahresabschlüsse, der Eröffnungsbilanz und der Unterlagen im Sinne von § 147 Abs. 1 Nr. 4a AO können die in Abs. 1 aufgeführten Unterlagen ähnlich wie nach den Buchführungsvorschriften des Handelsgesetzbuches auch als Wiedergabe auf einem Bildträger oder auf anderen Datenträgern aufbewahrt werden. Nach § 147 Abs. 6 AO kann die Mitwirkungspflicht gegenüber der Finanzbehörde erfüllt werden, indem ihr Einsicht in die gespeicherten Daten gegeben wird, der Steuerpflichtige die Daten nach den Vorgaben der Finanzbehörde auswertet oder der Finanzbehörde die gespeicherten Unterlagen auf einem maschinell verwertbaren Datenträger zur Auswertung überlässt. Hat sich der Steuerpflichtige gemäß § 147 Abs. 2 AO zur Aufbewahrung seiner Unterlagen auf Datenträgern entschlossen, sind die Grundsätze der ordnungsgemäßen Buchführung zu beachten. Außerdem muss gemäß § 147 Abs. 2 Nr. 1, 2 AO sichergestellt werden, dass die Wiedergabe der Unterlagen, wenn sie lesbar gemacht werden, mit den empfangenen Handels- und Geschäftsbriefen und Buchungsbelegen bildlich und mit den anderen Unterlagen inhaltlich überstimmen. Während der Aufbewahrungsfrist müssen sie jederzeit verfügbar und unverzüglich lesbar gemacht und maschinell ausgewertet werden können. Für Steuerzwecke ist es daher zulässig, unter Einhaltung der Voraussetzungen des § 147 Abs. 2 AO Unterlagen in Papierform zu scannen und die Originale anschließend zu vernichten [RFJW08, S. 74], [RoWi06, S. 2146], [Wilk11, S. 100].

[43] Nach bisherigem Recht § 35 BDSG a.F.

Für gescannte Steuerunterlagen sind die „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff“ (GoBD) zu beachten.

Aus den oben genannten Regelungen ergeben sich folgende Kriterien für die Ausgestaltung der Aufbewahrung steuerlich relevanter Unterlagen:

- Beweiskraft der Buchführung,
- Datenzugriff,
- Nachvollziehbarkeit und Kontrolle steuerlich relevanter Vorgänge,
- Beweissicherung sowie
- Schutz des Rechtsverkehrs.

Die hier vorgenommene Schutzbedarfsanalyse erfolgt nur beispielhaft. Es sind die Kriterien im konkret vorliegenden (Regel-)Fall zu bewerten, um den Schutzbedarf für den jeweiligen Anwendungsfall zu ermitteln. Existierende Die gemeinsam von der Bundessteuerberaterkammer und dem Deutschen Steuerberaterverband e.V. erarbeitete Musterverfahrensdokumentation zur Digitalisierung und elektronischen Aufbewahrung von Belegen inkl. Vernichtung der Papierbelege, differenziert nach Dokumentarten und bestimmte Originaldokumente[44] sind unter Berücksichtigung eventueller sachlicher und zeitlicher Aufbewahrungserfordernisse von der Vernichtung auszunehmen [BSDS14, S. 15f.].

Anwendungsgebiet	*Vorschriften zum ersetzenden Scannen*	*Voraussetzungen für die Vernichtung der Papieroriginale*
Besteuerungsunterlagen	§ 147 Abs. 2 AO	• Einhaltung der Grundsätze der ordnungsgemäßen Buchführung (GoB) • jederzeitige Verfügbarkeit und Herstellung der Lesbarkeit innerhalb angemessener Frist • bildliche Übereinstimmung (hinsichtlich empfangener Handelsbriefe, Buchungsbelege), sonst inhaltliche Übereinstimmung (hinsichtlich anderer Unterlagen) • Möglichkeit maschineller Auswertung

Tabelle 12: Vorschriften und Voraussetzungen für das ersetzende Scannen von Besteuerungsunterlagen

[44] S. oben Fn. 37.

Grundwerte[45]	*Sicherheitsziel*	*Hinweise zur Einstufung des Schutzbedarfs*
Integrität	Integrität	Der Integrität kommt eine hohe Bedeutung zu, da jede unsichtbare Veränderungen die Festsetzung der Steuerlast beeinflussen kann.
	Authentizität	Eine eindeutige Zuordnung zum Aussteller der Unterlagen, die steuerlich relevant sind, muss gewährleistet sein.
	Vollständigkeit	Die Vollständigkeit der Besteuerungsunterlagen ergibt sich aus dem Grundsatz der ordnungsgemäßen Buchführung (GoB).
	Nachvollziehbarkeit	Die Nachvollziehbarkeit hat den Zweck, dass sich ein sachverständiger Dritter (z. B. die Finanzverwaltung) innerhalb angemessener Zeit einen Überblick über die Geschäftsvorfälle und die Lage des Unternehmens machen kann.
Verfügbarkeit	Verfügbarkeit	Auf Verlangen der Finanzbehörde müssen Besteuerungsunterlagen nach § 200 Abs. 1 S. 2 AO innerhalb der Aufbewahrungsfrist im Rahmen einer Außenprüfung vorgelegt werden können.
	Lesbarkeit	Zur Vorlage bei der Finanzbehörde müssen die steuerlich relevanten elektronischen Dokumente gemäß § 147 Abs. 5 AO lesbar gemacht werden können. Dies gilt gemäß § 147 Abs. 6 iVm § 200 Abs. 1 Satz 2 AO auch bei Außenprüfungen.
	Verkehrsfähigkeit	Hat der Steuerpflichtige ursprünglich in Papierform erstellte Unterlagen digital archiviert, muss er dem Prüfer die Einsichtnahme ermöglichen. Auch die elektronische Auswertung muss möglich sein.

[45] Die Grundwerte (GW) der IT-Sicherheit [BSI-Glossar] verdeutlichen die Zuordnung der Sicherheitsziele zu den Sicherheitsmaßnahmen im Aufbaumodul [BSI-TR03138, S. 16, Abb. 2, sowie S. 29 ff.

Grundwerte[45]	*Sicherheitsziel*	*Hinweise zur Einstufung des Schutzbedarfs*
Vertraulichkeit	Vertraulichkeit	Bei Betriebs- und Geschäftsgeheimnissen sowie bei der Speicherung personenbezogener Daten kann eine besondere Sicherung der Daten notwendig sein. Dies gilt besonders dann, wenn die Digitalisierung durch externe Dienstleister durchgeführt wird.
	Löschbarkeit	Gemäß Art. 17 Abs. 1 lit. a DSGVO müssen personenbezogene Daten u.a. gelöscht werden, wenn sie für den Zweck für den sie verarbeitet wurden nicht mehr notwendig sind.[46] Im Fall der Auftragsdatenverarbeitung sind Dienstleister entsprechend zu verpflichten.

Tabelle 13: Hinweise zur Schutzbedarfsanalyse von Besteuerungsunterlagen

R.1.2.7 Personalakten

Der Begriff der Personalakte ist nicht gesetzlich definiert. Er umfasst alle Urkunden, Schriftstücke und sonstigen Vorgänge, die mit dem Arbeitsverhältnis in einem inneren Zusammenhang stehen und an denen der Arbeitgeber ein sachliches und berechtigtes Interesse[47] hat [DiSc08, S. 928 m. w. N.]. Personalakten dienen sowohl betrieblichen Interessen als auch solchen der einzelnen Mitarbeiter [RWWO09, § 87, Rn. 6], nicht nur während des Beschäftigungsverhältnisses, sondern auch danach.

Eine generelle Pflicht zur Führung von Personalakten besteht z.B. für Beamte in der Bundesverwaltung gemäß § 106 Abs. 1 Satz 1 Bundesbeamtengesetz (BBG) sowie Beamte der Landesverwaltungen nach den Landesbeamtengesetzen der Länder oder für Soldaten gemäß § 29 Soldatengesetz. In privaten Betrieben besteht eine solche Pflicht, abgesehen von wenigen Verwahrungsvorschriften für besondere Unterlagen, z. B. § 257 HGB, § 147 AO oder § 41 Abs. 1 S. 9 EStG, nicht [RWWO09, § 87, Rn. 7].

Einige Bestandteile von Personalakten erfordern die Schriftform, wie z. B. befristete Arbeitsverträge nach § 14 TzBfG, Verträge mit nachvertraglichen Wettbewerbsverboten nach § 74 Abs. 1 HGB, Aushebungsverträge und Kündigungsschreiben nach § 623 BGB. Dies hindert aber nicht daran sie nach Abschluss oder Wirksamwerden ersetzend zu scannen [LüSp17]. Mangels gesetzlicher Vorschriften zur Führung und Aufbewahrung von betrieblichen Personalakten im Allgemeinen richtet sich die Zulässigkeit ersetzenden Scannens derjenigen Dokumente, für die Verwahrungsvorschriften bestehen, nach den spezialgesetzlichen Regelungen der § 257 HGB für kaufmännische Buchführungsunterlagen, § 147 AO für Besteuerungsunterlagen, § 41 Abs. 1 Satz 9 EstG für Aufzeichnungen zu Lohnzahlungen sowie § 9 Abs. 5 BVV für sozialversicherungsrechtliche Entgeltunterlagen. § 257 HGB wurde im Rahmen der kaufmännischen Buchführungsunterlagen (R.1.2.5), § 147 AO im Rahmen der Besteuerungsunterlagen (R.1.2.6) und § 9 Abs. 5 BV im Rahmen der Sozialversicherungsunterlagen erläutert. Für die Aufzeichnungen

[46] Nach bisherigem Recht § 35 Abs. 2 BDSG a.F.

[47] Ein berechtigtes Interesse des Arbeitgebers kann neben der Personalplanung und Lohnabrechnung auch der individuelle Werdegang eines Arbeitnehmers sein oder die Sozialauswahl im Falle der Notwendigkeit betrieblicher Kündigungen [DiSc08, S. 928].

nach § 41 Abs. 1 Satz 9 EStG gelten die Ausführungen zu den Besteuerungsunterlagen analog, da Sinn und Zweck vergleichbar sind. Bei der Schutzbedarfsanalyse sind die einzelnen Dokumente aus der Personalakte somit immer dem jeweiligen Dokumententyp (z. B. kaufmännische Buchführung, Besteuerungsunterlagen, Entgeltunterlagen) zuzuordnen. Es wird auf die Ausführungen an entsprechender Stelle oben verwiesen.

Die elektronische Transformation betrieblicher Personalakten ist darüber hinaus nach dem Bundesdatenschutzgesetz zu beurteilen. Die Zulässigkeit des ersetzenden Scannens richtet sich in der Regel nach Art. 6 Abs. 1 DSGVO, wobei auch eine Dienst- oder Betriebsvereinbarung als Erlaubnisnorm in Frage kommen kann. Insbesondere sind die personenbezogenen Daten der Mitarbeiter vertraulich zu behandeln und vor unbefugter Kenntnisnahme zu schützen. Dies gilt in besonderem Maße für besonders schützenswerte Daten im Sinne des Art. 9 Abs. 1 DSGVO wie Aussagen zu Gesundheit des Arbeitnehmers.

Personalakten der Bundesverwaltung dürfen nach § 106 Abs. 1 Satz 3 BBG „in Teilen oder vollständig automatisiert geführt werden". Wird die Personalakte nur in Teilen automatisiert geführt, entsteht eine Hybridakte. Zu dieser bestimmt § 106 Abs. 2 Satz 5 BBG: „Wird die Personalakte nicht vollständig in Schriftform oder vollständig automatisiert geführt, legt die personalverwaltende Stelle jeweils schriftlich fest, welche Teile in welcher Form geführt werden und nimmt dies in das Verzeichnis nach Satz 4 auf." Eine explizite Regelung zur Umwandlung bereits bestehender Akten oder Zugänge zu den Akten ist den Vorschriften der §§ 106 bis 114 BBG nicht zu entnehmen.

Mit § 106 Abs. 1 „Satz 3 wird klargestellt, dass die Personalakte *sowohl* in Schriftform *als auch* automatisiert ‚elektronisch') geführt werden kann, ohne dass damit ein Verstoß gegen das ‚Verbot der geheimen Personalakten' vorliegt" [BT-Drs. 16/7076, S. 125].[48] Die Regelung schließt somit einen Formzwang für die Aktenführung aus. Diese Zielsetzung wird ebenfalls deutlich, wenn hinsichtlich der Hybridakten wegen der notwendigen „Eindeutigkeit der Personalakte" eine „parallele Führung gleicher Aktenteile in Papierform und in elektronischer Form ... zu vermeiden" ist [BT-Drs. 16/7076, S. 125]. Daher hat nach § 106 Abs. 2 Satz 5 BBG „die personalverwaltende Stelle jeweils schriftlich fest(zulegen), *welche Teile* in *welcher Form* geführt werden". Zur vollständigen Führung der Akte in elektronischer Form ist nach der amtlichen Begründung u.a. ein ausreichender technischer Standard erforderlich, der eine vergleichbare Beweissicherheit wie eine Papierakte gewährleistet: Dies wird insbesondere durch qualifizierte elektronische Signaturen erreicht [BT-Drs. 16/7076, S. 125]. Weder der Gesetzestext noch die amtliche Begründung beziehen sich eindeutig auf die Frage der Umwandlung ursprünglich papierner Aktenbestandteile in die elektronische Form und schon gar nicht auf deren Vernichtung.[49] Vielmehr hält die amtliche Begründung fest, dass die „Einführung entsprechender (= elektronischer) Aktenführung" nicht mit „Einschränkungen der Rechte der Beamtinnen und Beamten ... verbunden" sein dürfen [BT-Drs. 16/7076, S. 125].

Allerdings ist auch festzuhalten, dass eine vollständige Aktenführung ohne Scannen von Papierunterlagen in der Praxis schwer vorstellbar ist. Insofern muss das Scannen von Papierunterlagen als Teil des Gesetzesprogramms verstanden werden.[50] Der Hinweis, dass wegen der notwendigen „Eindeutigkeit der Personalakte" eine „parallele Führung gleicher Aktenteile in Papierform und in elektronischer Form ... zu vermeiden" ist, deutet darauf hin, dass in der weiteren Logik dieser Entwicklung auch ein ersetzendes Scannen liegt [BT-Drs. 16/7076, S. 125]. Eine eindeutige Erlaubnis zur Vernichtung beweisrelevanter Urkunden der Beamtin oder des Beamten und damit ein Eingriff in deren Grundrechtsbereich ist allerdings weder dem Gesetzestext noch seiner Begründung zu entnehmen. Vielmehr deutet die einzige Regelung, die die Vernichtung von Aktenteilen zulässt, nämlich § 113 Abs. 4 BBG, auf das Gegenteil. Danach dürfen Personalakten erst nach Ablauf der gesetzlichen Aufbewahrungsfristen des § 113 Abs. 1 bis 3 BBG vernichtet werden. Daher wird dringend empfohlen, das ersetzende Scannen in § 106 BBG ausdrücklich zu erlauben!

[48] S. zu § 106 Abs. 1 BBG OVG NRW, Beschluss vom 5.4.2016, Az. 1 B 203/16; *VG Wiesbaden*, Urteil vom 20.1.2015, Az. 6 K 1567/14.WI; *VG Köln*, Beschluss vom 11.2.2016, Az. 15 L 2263/15.

[49] Für zulässig hält dies wohl *OVG NRW*, Beschluss vom 5.4.2016, Az. 1 B 203/16.

[50] So ist wohl auch *VG Köln*, Beschluss vom 11.2.2016, Az. 15 L 2263/15.

R.2 – Rechtliche Fragen im Zusammenhang mit dem ersetzenden Scannen

Zusätzlich zu den rechtlichen Rahmenbedingungen bezüglich verschiedener Dokumententypen in R.1 soll das nun folgende Kapitel einen Einblick in ausgewählte rechtliche Problemfelder geben, die regelmäßig im Rahmen des ersetzenden Scannens entstehen. Aus ihnen werden spezifische Anforderungen an den Anwender abgeleitet. Die Ausführungen dienen dem besseren Verständnis und sollen eine Hilfestellung bei der Beurteilung und Einordnung der einzelnen Dokumente im Rahmen der Schutzbedarfsanalyse bieten. Die Betrachtungen haben lediglich informatorischen Charakter und sind nicht Bestandteil einer eventuellen Zertifizierung.

Das folgende Kapitel beschäftigt sich zunächst mit datenschutzrechtlichen Grundlagen. Danach werden mögliche rechtliche Konsequenzen nicht ordnungsgemäßer Dokumentation und Aufbewahrung erörtert, um sich anschließend beweisrechtlichen Fragestellungen zu widmen. Weiterhin werden Gefährdungen des Scanprodukts aufgezeigt sowie die Möglichkeit, diese zu vermeiden. Im Anschluss wird auf die datenschutz- und strafrechtlichen Problematiken der externen Scandienstleistungen eingegangen. Zum Schluss folgt eine kurze Darstellung, wann eine Vernichtung von Originaldokumenten strafrechtlich relevant werden kann.

R.2.1 Datenschutz

Durch die Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGVO)[51] wird das gesamte Datenschutzrecht auf eine neue Grundlage gestellt. Sie gilt allerdings erst ab dem 25. Mai 2018 und wird dann mit all ihren Regelungen in allen Mitgliedstaaten unmittelbar Teil ihrer Rechtsordnung.

Zur Einpassung der Datenschutz-Grundverordnung in das deutsche Recht trifft das neue Bundesdatenschutzgesetz vom 30. Juni 2017 in seinem ersten und zweiten Teil ergänzende Regelungen. Das neue Bundesdatenschutzgesetz (BDSG n.F.) tritt ebenfalls erst zum 25. Mai 2018 in Kraft und hebt zu diesem Zeitpunkt das bisherige Bundesdatenschutzgesetz (BDSG a.F.) auf. Auch die Bundesländer passen ihre Landesdatenschutzgesetze an die Datenschutz-Grundverordnung an. Bund und Länder passen in der kommenden Zeit auch nach und nach viele bereichsspezifische Datenschutzregelungen in speziellen Gesetzen an die Verordnung an.

Neben dem Bundesdatenschutzgesetz hat der Bundesgesetzgeber durch das Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17. Juli 2017 bereits die Datenschutzregelungen des Sozialgesetzbuchs I und X sowie die Datenschutzvorschriften der Abgabenordnung ebenfalls an die Vorgaben der Datenschutz-Grundverordnung angepasst.

Im Folgenden werden die einschlägigen Regelungen sowohl des bisherigen Bundesdatenschutzgesetzes als auch die künftig geltenden Regelungen der Datenschutz-Grundverordnung und des sie ergänzenden neuen Bundesdatenschutzgesetz genannt. Sie werden bis zum bzw. ab dem Stichtag des 25. Mai 2018 gelten.

Wird ein Papierdokument, das personenbezogene Daten enthält, gescannt und in ein elektronisches Dokument übertragen, liegt bei der Erzeugung des Scanprodukts eine Speicherung und damit eine Datenverarbeitung nach Art. 4 Abs. 1 DSGVO und § 3 Abs. 4 Satz 2 Nr. 1 BDSG a.F. vor. Die Übertragung der Information von Papier auf ein digitales Medium ist potenziell mit einer Risikoerhöhung verbunden, da zum einen kein Veränderungsschutz besteht und die Daten insgesamt flüchtig sind. Zum anderen ist ein paralleler Zugriff mehrerer Nutzer auf personenbezogene Daten möglich [Wilk11, S. 203f.], [RFJW08, S. 61]. Die folgenden Ausführungen beschäftigen sich mit der Frage, nach welchen Vorschriften öffentliche und nicht-öffentliche Verantwortliche Daten verarbeiten dürfen und unter welchen Voraussetzungen das

[51] EU ABl. L 119 vom 4.5.2016, 1.

Scannen als Datenverarbeitung erforderlich im Sinne der Vorschriften der Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes a.F. ist.

R.2.1.1 Datenschutzrechtliche Zulässigkeit des Scannens

Bei der Beurteilung der Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung unterscheidet das bisherige Bundesdatenschutzgesetz zwischen einem Datenumgang durch öffentliche und private Stellen. Soweit das Scannen von Papierdokumenten durch eine öffentlich-rechtliche Stelle (z. B. Verwaltungsbehörden) erfolgt, ist dies nach § 14 Abs. 1 Satz 1 BDSG a.F. dann zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Die Zulässigkeit des Scannens und die damit verbundene Datenverarbeitung durch eine öffentlich-rechtliche Stelle für andere als in § 14 Abs. 1 Satz 1 BDSG genannte Zwecke ergibt sich aus § 14 Abs. 2 BDSG a.F. Dies ist gemäß § 14 Abs. 2 Nr. 1 und 2 BDSG a.F. der Fall, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder der Betroffene eingewilligt hat. Gemäß § 14 Abs. 2 Nr. 3 BDSG a.F. ist die Datenverarbeitung durch das Scannen auch dann zulässig, wenn sie offensichtlich im Interesse des Betroffenen erfolgt und kein Grund zur Annahme besteht, dass der Betroffene in Kenntnis des von der Behörde verfolgten Zwecks seine Einwilligung verweigern würde. In erster Linie erfolgt das Scannen von Papierdokumenten im Interesse der Behörde, um die Vorteile der elektronischen Aktenführung wie Kosteneffizienz, schnellere Dokumentenbearbeitung oder Akteneinsicht für sich zu nutzen [Wilk11, S. 204f.]. Angesichts der mit der Verarbeitung elektronischer Daten potenziell verbundenen Risiken kann nicht grundsätzlich davon ausgegangen werden, dass ein informierter Betroffener ohne Weiteres in das ersetzende Scannen von Papierdokumenten einwilligen würde [Wilk11, S. 205].

Nicht-öffentliche Stellen (z. B. Freiberufler oder Unternehmen) dürfen die Datenverarbeitung gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG a.F. durchführen, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit der betroffenen Person erforderlich ist. Darüber hinaus ist die Datenverarbeitung durch nicht-öffentliche Stellen gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG a.F. zulässig, soweit es zur Wahrung ihrer berechtigten Interessen erforderlich ist und wenn kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung überwiegt. Um einen effektiven Datenschutz zu gewährleisten, sind an diese Interessenabwägung strenge Maßstäbe zu stellen [Simi14, § 28, Rn. 98 ff.]. Bei der Erhebung von Gesundheitsdaten ist ferner § 28 Abs. 7 BDSG a.F. zu beachten. Das Erheben besonders schützenswerter personenbezogener Daten im Sinne von § 3 Abs. 9 BDSG a.F. ist dann zulässig, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder der Behandlung oder der Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder sonstige Personen, die einer entsprechenden Schweigepflicht unterliegen, erfolgt.

Die Datenschutz-Grundverordnung soll eigentlich nicht zwischen öffentlichen und privaten Verantwortlichen unterscheiden. Dennoch enthalten ihre Regelungen zur Zulässigkeit Tatbestände, die für private und öffentliche Verantwortliche unterschiedlich passen. Das Scannen von Papierdokumenten mit personenbezogenen Daten ist eine Datenverarbeitung nach Art. 4 Nr. 2 DSGVO, die vor allem für private Verantwortliche zulässig ist, wenn eine der folgenden Bedingung für sie gilt. Nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO ist die Datenverarbeitung zulässig, wenn die betroffene Person hierzu ihre Einwilligung gegeben hat. Einwilligungen, die jederzeit widerrufen werden können, sind allerdings keine geeignete Grundlage für eine Scan-Routine eines Unternehmens. Die Datenverarbeitung ist weiter nach Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO zulässig, wenn sie für die Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist. Dies dürfte für nachträgliche Scan-Vorgänge selten der Fall sein. Wichtiger ist die Bedingung des Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO, nach der die Datenverarbeitung zulässig ist, wenn sie zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen erforderlich ist. Hier wirken alle gesetzlichen Verpflichtungen zur Aufbewahrung von Unterlagen und die rechtlichen Erlaubnisse, dies in elektronischer Form zu tun, auch als datenschutzrechtliche Erlaubnistatbestände. Schließlich ist nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO jede Datenverarbeitung zulässig, die zur Wahrung der berechtigten Interessen

des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.[52] Zwar ist der geringere Zeit- und Kostenaufwand der Aufbewahrung der gescannten Dokumente und der schnellere und einfachere Umgang mit ihnen ein berechtigtes Interesse. Selbst wenn das ersetzende Scannen für die Wahrung dieses berechtigten Interesses erforderlich ist (hierzu sogleich), muss eine Abwägung mit den schutzwürdigen Interessen der betroffenen Person erfolgen. In diese gehen vor allem das Risiko, das mit dem ersetzenden Scannen verbunden ist, und die risikoreduzierenden Maßnahmen des Verantwortlichen ein [KüBu17, Art. 6, Rn. 149 ff.]. Insofern ist die objektive Risikobewertung im Rahmen der Schutzbedarfsfeststellung auch relevant für die datenschutzrechtliche Zulässigkeit des ersetzenden Scannens.

Für öffentlich-rechtlich handelnde Verantwortliche ist vor allem der Erlaubnistatbestand des Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO von Bedeutung. Dieser erlaubt die Datenverarbeitung, sofern sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Nach Art. 6 Abs. 3 DSGVO darf jeder Mitgliedstaat der Union die Regeln erlassen oder beibehalten, die diese Aufgaben näher bestimmen. Insofern ist Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO nur eine „Scharniernorm", die auf die gesetzlichen Erlaubnisse zur Datenverarbeitung nach deutschem Recht verweist [Roßn18, § 1 Rn. 33, § 7 Rn. 8]. Im Ergebnis bedeutet dies: Wenn eine deutsche Norm – wie die in Kap. R 1 genannten – das ersetzende Scannen erlaubt oder voraussetzt, dann ist dieses auch nach der Datenschutz-Grundverordnung erlaubt. Die Wertungen die im Rahmen des bisherigen Bundesdatenschutzgesetzes angestellt wurden, können somit weitgehend auch auf die Bewertung nach der Datenschutz-Grundverordnung übertragen werden.

Bei der Verarbeitung von besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO, zu denen u.a Gesundheitsdaten, genetische Daten und biometrische Daten sowie Daten gehören, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, ist zu beachten, dass diese grundsätzlich nicht verarbeitet werden dürfen. Dies ist jedoch nach Art. 9 Abs. 2 DSGVO ausnahmsweise zulässig, wenn u.a. die betroffene Person eingewilligt hat, wenn die Verarbeitung erforderlich ist, um Rechte oder Pflichten aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes auszuüben oder zu erfüllen, die Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist oder wenn die Verarbeitung für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich erforderlich ist [Roßn18, § 8, Rn. 284]. Im letzten Fall müssen die Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal muss einem Berufsgeheimnis unterliegen [KüBu17, Art. 9, Rn. 138 ff.]. Zusätzlich oder in Präzisierung der Erlaubnisse des Art. 9 Abs. 2 DSGVO regelt § 22 BDSG n.F. weitere Erlaubnisse zur Verarbeitung besonderer Kategorien personenbezogener Daten [Roßn18, § 8, Rn. 320].

Maßgebliches Kriterium für die datenschutzrechtliche Zulässigkeit des ersetzenden Scannens ist nach bisherigem und künftigem Datenschutzrecht neben weiteren Anforderungen immer die Erforderlichkeit der Datenverarbeitung. Wann diese gegeben ist, soll im nächsten Abschnitt näher erläutert werden.

R.2.1.2 Erforderlichkeit

Der Umgang mit personenbezogenen Daten unterliegt dem Grundsatz der Erforderlichkeit. Dieser ist vor allem beim (nachträglichen) Scannen zu prüfen. Nach diesem Grundsatz ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten auf das notwendige Maß zu beschränken [BVerfGE 65, S. 46]. Die Erforderlichkeit ergibt sich für das Bundesdatenschutzgesetz a.F. aus der Zweckbindung der Datenverarbeitung und bedarf einer Überprüfung im Einzelfall sowie einer Abwägung der Interessen der

[52] Dieser Erlaubnistatbestand gilt nach Art. 6 Abs. 1 UAbs. 2 DSGVO ausdrücklich nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

datenverarbeitenden Stelle sowie der betroffenen Person. Für die Datenschutz-Grundverordnung ergibt sich die Erforderlichkeit aus dem Text der jeweiligen Erlaubnistatbestände sowie aus dem Grundsatz der Datenminimierung des Art. 5 Abs. 1 lit. c DSGVO [Roßn18, § 3 Rn. 62 und 70 ff.].

In der Regel wird die dokumentationsführende Stelle dazu berechtigt sein, die Daten von vornherein elektronisch zu erheben. Wenn eine originär elektronische Datenerhebung zulässig ist und keine Anhaltspunkte vorliegen, dass der Betroffene in diese elektronische Datenverarbeitung nicht einwilligen würde, spricht viel dafür, dass auch das Scannen von Papierdokumenten, die personenbezogene Daten enthalten, zulässig ist. Mit dem Scannen und der anschließenden Speicherung auf einem elektronischen Medium sind die gleichen Zugriffsrisiken verbunden wie mit der elektronischen Datenerhebung. In solchen Fällen ist auch die mit dem Scannen verbundene Vervielfältigung der Daten aus Sicht des Daten- und Geheimnisschutzes kein zusätzliches Risiko [Wilk11, S. 205], [RFJW08, S. 62].

Zwar führt allein der Umstand, dass die elektronische gegenüber der papierbasierten Dokumentenführung mit einem deutlich geringeren Zeit- und Kostenaufwand verbunden ist, nicht automatisch zur Erforderlichkeit im Sinn des Datenschutzrechts. Diese wird aber in der Regel gegeben sein, wenn die verantwortliche Stelle ihre Datenverarbeitung auf ein elektronisches Dokumentenmanagement umgestellt hat. Sind die zunächst auf Papier festgehaltenen Informationen solcher Art, dass sie von vornherein auch elektronisch hätten erhoben werden dürfen, steht einer Digitalisierung datenschutzrechtlich nichts entgegen, wenn keine Anhaltspunkte dafürsprechen, dass die betroffene Person ihre Daten nicht zur Verfügung gestellt hätte [RFJW08, S. 62], [Wilk11, S. 205]. Auch wenn das Scannen der Erhaltung der Lesbarkeit dienen soll und andernfalls ein dauerhafter Verlust der Daten zu befürchten wäre, kann die Erforderlichkeit des Scannens bejaht werden [Wilk11, S. 204], [RFJW08, S. 52]. Dies ist bei solchen Papierdokumenten der Fall, die nur einmal existieren und mit der Zeit verblassen, z. B. Ausdrucke auf Thermopapier. Auch die notwendige schnelle Verfügbarkeit der Daten an verschiedenen Orten, wie bei Patienteninformationen, kann für die Erforderlichkeit der elektronischen Datenvorhaltung durch Scannen der Originaldokumente sprechen.

R.2.2 Rechtliche Konsequenzen nicht ordnungsgemäßer Dokumentation und Aufbewahrung

Papierdokumenten wird aufgrund ihrer spezifischen Eigenschaften und der Tatsache, dass sie sich in der Vergangenheit als zuverlässiges Perpetuierungsmedium bewährt haben, im Rechtsverkehr ein hohes Vertrauen entgegengebracht. Dieses Grundvertrauen in eine nachweisbare Dokumentation von rechtlich relevanten Erklärungen besteht gegenüber elektronischen Dokumenten nicht, da sie ohne weiteres keine vergleichbaren Sicherheitsmerkmale aufweisen. Gleiches gilt für eingescannte Dokumente.[53] Daher müssen die Scanverfahren und Scanprodukte so ausgestaltet sein, dass sie eine vergleichbare Vertrauensgrundlage erzeugen können.

Die ordnungsgemäße Aufbewahrung von Dokumenten trägt notwendigerweise dazu bei, dass das Handeln nachvollzogen und auf seine Rechts- und Ordnungsmäßigkeit überprüft werden kann [Fisc06, S. 43]. Nach der Vernichtung oder der Rückgabe der Papierdokumente muss die verantwortliche Stelle oder die Person, die zur ordnungsgemäßen Aufbewahrung von Dokumenten verpflichtet ist, in der Lage sein, die Eindeutigkeit, Richtigkeit und die Übereinstimmung der elektronischen Dokumente mit den früheren papiernen Originalen nachweisen zu können [BfDI23, S. 63]. Eine Verletzungshandlung besteht dann, wenn nicht ausgeschlossen werden kann, dass das eingescannte Dokument nicht dem Original entspricht und im Ergebnis nicht als glaubwürdige Grundlage herangezogen werden kann [RFJW08, S. 60].

Die materiell-rechtlichen Konsequenzen, die aus der Verletzung der Dokumentations- und Aufbewahrungspflicht resultieren, unterscheiden sich danach, welche geschützten Interessen – öffentliche oder individuelle – von ihr betroffen sind.

[53] S. z. B. FG Münster, Urteil vom 24.11.2015, Az. 14 K 1542/15 AO.

R.2.2.1 Konsequenzen bei Verletzung öffentlicher Interessen

Die materiell-rechtlichen Konsequenzen, die aus der Verletzung von Dokumentations- und Aufbewahrungspflichten resultieren können, ergeben sich aus dem jeweils zur Anwendung kommenden Rechtsgebiet. So können die Verletzungen der medizinischen Dokumentations- und Aufbewahrungspflicht zum einen eine Verletzung von berufs- oder standesrechtlichen Pflichten darstellen, die Gegenstand berufsrechtlicher Verfahren sein können. Zum anderen kann die Verletzung solcher Pflichten auch strafrechtliche Konsequenzen nach sich ziehen. Ein Arzt verletzt die ihm nach § 203 StGB obliegende ärztliche Schweigepflicht,[54] wenn Dritte unberechtigten Zugriff auf die ärztliche Dokumentation erlangen. Zudem kann er sich wegen Verletzung des Datenschutzes nach §§ 43 oder 44 BDSG a.F. oder nach Art. 83 DSGVO sanktioniert werden. Ein Arzt setzt sich dem Vorwurf der Urkundenfälschung nach § 267 StGB aus,[55] wenn er die Patientendaten gezielt nachträglich manipuliert, z. B. die von seinem Laborpersonal ermittelten und in die Krankenakte des Patienten eingetragenen Messwerte nachträglich verändert [Fisc17, § 267, Rn. 34].

Werden handels- und steuerrechtliche Aufbewahrungspflichten verletzt, kann dies zunächst zu finanziellen Nachteilen führen. So können sowohl Steuervergünstigungen versagt als auch die Bilanzansätze berichtigt oder eine Steuerschätzung gemäß § 162 Abs. 2 Satz 2 AO vorgenommen werden. Nach § 162 Abs. 2 Satz 2 AO sind die Besteuerungsunterlagen insbesondere zu schätzen, wenn der Steuerpflichtige seine Bücher und Aufzeichnungen, die er nach den Steuergesetzen zu führen hat, der Finanzbehörde nicht oder nicht vollständig vorlegen kann. Im Ergebnis könnte dies bedeuten, dass eingescannte Besteuerungsunterlagen, bei denen das Original bereits vernichtet worden ist und die nicht lesbar, nicht verfügbar oder nicht vollständig sind, zu einer nachteiligen Steuerschätzung führen können. Der Grund, warum der Steuerpflichtige seine Bücher nicht vorlegen kann, ist für die Finanzbehörde ohne Bedeutung. Auf die Unmöglichkeit der Nichtvorlage kann der Steuerpflichtige sich nur dann berufen, wenn sie auf Maßnahmen der Finanzverwaltung oder Finanzgerichte zurückzuführen sind [PaKo09, § 162, Rn. 61]. Darüber hinaus können die Verletzungen der Buchführungs- und Aufzeichnungspflicht nach § 379 AO als eine Steuerordnungswidrigkeit geahndet werden.

Im Handels- und Steuerrecht ergeben sich die gleichen Rechtsfolgen. Die Verletzung der handelsrechtlichen Buchführungspflicht zieht auch die Verletzung der steuerrechtlichen Buchführungspflichten nach sich. Denn die Mängel der kaufmännischen Buchführung beeinträchtigen die steuerrechtliche Beweiskraft der handelsrechtlichen Bücher, woraus als Folge die Schätzung der Besteuerungsgrundlagen gemäß § 162 Abs. 1 Satz 1 AO resultieren kann [BaHo12, § 238, Rn. 21]. Ein Verstoß gegen die handelsrechtlichen Buchführungspflichten (GoB) kann gemäß §§ 331 bis 335 HGB als Straftat mit einer Freiheits- oder einer Geldstrafe oder als eine Ordnungswidrigkeit mit einem Bußgeld sanktioniert werden.

R.2.2.2 Konsequenzen bei Verletzung individueller Interessen

Sind individuelle Interessen von der Vernichtung des Originals nach dem Scannen betroffen, ist zu unterscheiden, ob die ordnungsgemäße Dokumentation und Aufbewahrung eine vertragliche Hauptleistungs- oder bloße Nebenpflicht[56] darstellt. Individuell kann ein Dienstleister dazu verpflichtet sein, die Dokumente aufzubewahren und herauszugeben. Besteht ein Anspruch eines Dritten auf die Herausgabe und ist dies der aufbewahrenden Stelle nicht möglich, kann der Anspruchsberechtigte

[54] Bei Verletzung der Schweigepflicht kann eine Geld- oder eine Freiheitsstrafe bis zu einem Jahr verhängt werden. Zur Strafbarkeit bei Offenbarung von Patientengeheimnissen gemäß § 203 StGB s. auch Kapitel R.2.4.2.

[55] Als Strafe sieht § 267 Abs. 1 StGB Geldstrafe oder Freiheitsstrafe bis zu fünf Jahren vor. Im Rahmen der Strafzumessung kann die Qualität der falschen Urkunde berücksichtigt werden, ob sie z. B. infolge ungeschickter Vorgehensweise sofort als Fälschung erkannt werden kann.

[56] In der Regel die ordnungsgemäße Dokumentation und Aufbewahrung Nebenpflicht sein, um die Hauptleistungspflicht, nämlich die ordnungsgemäße Bearbeitung der übertragenen Aufgaben, zu erfüllen.

Schadensersatzansprüche geltend machen, wenn die Vernichtung des papiernen Originals ursächlich für die Entstehung des Schadens war [RFJW08, S. 86].

Wenn jedoch die Dokumentation und die Aufbewahrung lediglich Nebenpflichten (Sekundärpflichten) darstellen, so können Schadensersatzansprüche nicht unmittelbar geltend gemacht und auch nicht selbständig eingeklagt werden. Denn die Sekundärpflichten dienen nur dazu, die Erfüllung der Primärpflicht zu unterstützen. Solange die Primärpflicht erfüllt wird, kann kein Anspruch aus der Nebenpflicht begründet werden. Ihre Verletzung kann erst dann geltend gemacht werden, wenn sie ursächlich für die bei der geschädigten Person eingetretene Verletzung ist. Die Vorgangsdokumentation erfolgt, um eine ordnungsgemäße Bearbeitung der Aufgaben nachzuweisen, so dass regelmäßig eine Verletzung dieser Aufgabe selbst, jedoch nicht die unterbliebene Aufbewahrung – in dem Fall die Vernichtung des Originals – die schadensbegründende Handlung darstellt [RFJW08, S. 46f.], [RFJK07, S. 110].

Ein anderes Ergebnis könnte sich allerdings ergeben, wenn sich aus der Verletzung der Aufbewahrungspflichten Folgeschäden ergeben. Eine fehlerhafte ärztliche Dokumentation oder eine fehlende Zugriffsmöglichkeit auf sie, kann z. B. bei einer erneuten Behandlung dazu führen, dass eine unsachgemäße Nachbehandlung vorgenommen wird [Fisc06, S. 46 f.] und [RFJW08, S. 86], weil das gescannte Dokument z. B. nicht lesbar, nicht verkehrsfähig oder nicht vollständig ist.

Wird die Vertraulichkeit von gescannten Dokumenten nicht gewahrt, können sich ebenfalls Schadensersatzansprüche aus der Verletzung des Daten- und Geheimnisschutzes ergeben. Dabei kommen bei einem Verstoß gegen die ärztliche Schweigepflicht deliktische Ansprüche nach § 823 Abs. 2 BGB i. V. m. § 203 StGB oder aus § 823 Abs. 1 BGB (Verletzung des allgemeinen Persönlichkeitsrechts) in Betracht. Werden solche Verletzungen von einer öffentlichen Stelle begangen, können ebenfalls Schadenersatzansprüche wegen Amtspflichtverletzungen gemäß Art. 34 GG i. V. m. § 839 BGB bestehen [Schu14, § 839, Rn. 1].

R.2.3 Mehrseitige, beglaubigte Dokumente

Problematisch kann es sein, Dokumente ersetzend zu scannen, bei denen die Verbindung mehrerer Seiten durch eine öffentliche Stelle bestätigt wurde, z. B. die notarielle Beglaubigung mehrseitiger Dokumente durch ein Siegel (Aufkleber oder Stempel) oder eine Siegelschnur. Die Verbindung mit einem Siegel oder einer Siegelschnur dient dazu, die Zusammengehörigkeit der Einzelseiten als ein Dokument und somit die Vollständigkeit zu sichern. Indem das Siegel oder die Siegelschnur im Rahmen der organisatorischen Vorbereitung der Dokumente für das Scannen aufgelöst wird, wird nicht nur die Urkundenqualität des Dokuments aufgehoben. In der Zukunft kann auch kein Beweis mehr erbracht werden, dass das papierne Dokument vormals notariell beglaubigt worden war. Dies ist insbesondere bei Willenserklärungen von Bedeutung, bei denen die notarielle Beurkundung gesetzlich vorgeschrieben ist.[57] Das Scannen solcher Dokumente, bei denen die Verbindung von Einzelseiten durch eine öffentliche Stelle besonders bestätigt worden ist, ist mittels geeigneter Hardware (z. B. Flachbettscanner) zwar grundsätzlich möglich. Jedoch sollten die Originaldokumente aufgrund der zusätzlichen Beweisrisiken nach dem Scanprozess nicht vernichtet, sondern besonders aufbewahrt (oder asserviert) werden ([RFJW08, S. 50], [RoJa08, S. 23] [RoNe14a, S. 44] und [RoNe14b, S. 888]

R.2.4 Datenschutzrechtliche und strafrechtliche Beurteilung des externen Scannens

Abhängig von der Menge der zu scannenden Akten und der vorhandenen Infrastruktur in den Unternehmen kann es von Interesse sein, die Digitalisierung von einem externen Dienstleister vornehmen zu lassen. Dies wirft Fragen bezüglich der Zulässigkeit der Weitergabe der Daten an den Scandienstleister in datenschutzrechtlicher, aber auch in strafrechtlicher Hinsicht auf.

[57] Gesetzlich vorgeschrieben ist die notarielle Beurkundung z. B. für § 15 Abs. 2 GmbHG für die Abtretung eines Anteils an einer GmbH oder § 311b Abs. 1 Satz 1 BGB bei Grundstückskaufverträgen.

R.2.4.1 Datenschutzrecht

Die Verarbeitung personenbezogener Daten erlangt eine besonders hohe Bedeutung, wenn das Scannen von Papierdokumenten durch externe Dienstleister übernommen wird. Die Regelungen zur Datenverarbeitung im Auftrag nach künftigem Datenschutzrecht verfolgen zwar die gleiche Zielsetzung wie die bisherigen Regelungen, die Verantwortung des Auftraggebers zu wahren und die Rechtskonformität der Verarbeitung durch den Auftragnehmer sicher zu stellen. Sie unterscheiden sich von den bisherigen Regelungen jedoch in mehreren Details.

Bis zum 25. Mai 2018 ist in den Fällen der Auftragsverarbeitung § 11 BDSG a.F. (oder die entsprechende Vorschrift in den jeweiligen Landesdatenschutzgesetzen a.F. oder in Spezialvorschriften wie den Landeskrankenhausgesetzen) zu berücksichtigen, der die Datenverarbeitung im Auftrag regelt. Wenn eine wirksame Auftragsdatenverarbeitung vorliegt und die Datenerhebung durch den Auftraggeber zulässig ist, ist auch das Scannen durch externe Dienstleister im Allgemeinen unbedenklich. Die Datenweitergabe vom Auftraggeber an den Auftragnehmer ist nämlich gemäß § 3 Abs. 8 Satz 3 BDSG a.F. keine Datenübermittlung an Dritte [Simi14, § 3, Rn. 244], [Simi14, § 11, Rn. 43], [RFJW08, S. 62]. Trotzdem liegt hierin eine Nutzung der Daten gemäß § 3 Abs. 5 BDSG a.F. Ob diese zulässig ist, muss für den Auftraggeber geprüft werden. Sie ist ohne Einwilligung des Betroffenen nur im Rahmen der gesetzlichen Ermächtigungsgrundlagen, insbesondere §§ 12 ff. BDSG a.F. und §§ 28 ff. BDSG a.F. zulässig [Roßn03, Kap. 4.6, Rn. 101]. Die durch den externen Dienstleister stattfindende Datenverarbeitung muss allen Anforderungen genügen, die auch von dem Auftraggeber zu erfüllen wären [Simi14, § 11, Rn. 48]. Hierbei ist zu beachten, dass sich die Sicherungsmaßnahmen zur Gewährleistung des Datenschutzes dann sowohl auf das Papierdokument als auch auf das Scanprodukt beziehen müssen [RFJW08, S. 62].

Bei der Auftragsdatenverarbeitung ist für öffentliche Stellen des Bundes und für nicht-öffentliche Stellen § 11 BDSG zu beachten, wenn nicht Fachgesetze eine speziellere Regelung treffen, wie z. B. § 80 SGB X a.F. Die Verantwortlichkeit für die Einhaltung des Datenschutzes liegt damit bei der Auftragsdatenverarbeitung beim Auftraggeber.

Spezialnormen können die Weitergabe besonderer Daten verbieten oder einschränken. Dies gilt nach § 30 AO a.F. für Daten, die dem Steuergeheimnis unterliegen und die nur unter den Voraussetzungen des § 30 Abs. 4 AO a.F. offenbart werden dürfen. Auch § 80 Abs. 5 SGB X a.F., der die Auftragsverarbeitung von Sozialdaten durch nicht-öffentliche Stellen an enge Voraussetzungen knüpft (Störung des Betriebsablaufs, Nr. 1, sowie erhebliche wirtschaftliche Vorteile, wenn nicht der gesamte Datenbestand vom Auftragnehmer gespeichert wird, Nr. 2) ist eine solche Spezialnorm. Auch § 107 BBG beschränkt den Zugriff auf Personalakten der Bundesbeamten auf einige wenige Mitarbeiter der Personalverwaltung. Deshalb ist vor der Herausgabe der personenbezogenen Daten zu prüfen, ob gesetzliche Bestimmungen die Weitergabe der Akten verbieten.

Ab dem 25. Mai 2018 ist die Auftragsverarbeitung nach Art. 28 und 29 DSGVO zu beurteilen. Danach entfällt die Ausnahme, dass die Offenlegung von personenbezogenen Daten gegenüber dem Auftragsverarbeiter keine rechtfertigungsbedürftige Form der Datenverarbeitung darstellt. Vielmehr ist die Übergabe der zu scannenden Dokumente an den Scan-Dienstleister ein Akt der Datenverarbeitung, dessen Zulässigkeit an Art. 6 Abs. 1 DSGVO zu messen ist [Roßn18, § 5 Rn. 77]. Die Offenlegung gegenüber dem Auftragsverarbeiter ist für öffentliche Verantwortliche nach Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO gerechtfertigt, wenn sie zur Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt. Dies ist dann der Fall, wenn der öffentliche Verantwortliche oder der nicht-öffentliche Verantwortliche, der im öffentlichen Interesse tätig ist, die Dokumente ersetzend scannen darf und die Scan-Tätigkeiten nicht in sinnvollem Rahmen selbst vornehmen kann. Für nicht-öffentliche Verantwortliche ist die Offenlegung gegenüber dem Auftragsverarbeiter nach Art.6 Abs. 1 UAbs. 1 lit. f DSGVO zulässig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Einem Auftragsverarbeiter Aufgaben zu übertragen, die nicht zum eigenen Kerngeschäft gehören, ist ein berechtigtes Interesse.

Erforderlich ist die Offenlegung, wenn die Scan-Arbeiten nicht in sinnvollem Rahmen selbst erledigt werden können. Die Abwägung kann dann zugunsten der berechtigen Interessen des Verantwortlichen ausgehen, wenn sichergestellt ist, dass alle Anforderungen der Art. 28 und 29 DSGVO erfüllt werden und damit die Risiken für die schutzwürdigen Interessen der betroffenen Person auf ein vertretbar geringes Maß reduziert werden [Roßn18, § 5 Rn. 77]. Der Auftragsverarbeiter kann seine Scan-Tätigkeit nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO auf einen Scandienstleister übertragen, wenn die Interessenabwägung wegen seiner Maßnahmen nach Art. 28 und 29 DSGVO zu seinen Gunsten ausfällt.

Allerdings gilt die Zulässigkeit der Offenlegung gegenüber dem Auftragsverarbeiter nur, soweit die zu verarbeitenden Daten keiner besonderen Datenkategorie des Art. 9 Abs. 1 DSGVO unterfallen. Zwar verschließt sich die Verordnung der Verarbeitung solcher Daten im Auftrag nicht grundsätzlich. Da aber Art. 9 Abs. 2 DSGVO keine dem Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO vergleichbare Regelung enthält, scheidet eine Interessenabwägung insoweit aus. Eine Offenlegung ist nur zulässig, wenn sie nach Art. 9 Abs. 2 DSGVO gerechtfertigt werden kann [Roßn18, § 5 Rn. 78].

Bestehende Regelungen für den öffentlichen Bereich, die eine Weitergabe besonderer Daten verbieten oder einschränken (s. oben), können auch unter der Geltung der Datenschutz-Grundverordnung weitergelten. Nach Art. 6 Abs. 3 Satz 3 DSGVO kann der jeweilige Mitgliedstaat eigene Regelungen erlassen oder beibehalten, die im Anwendungsbereich der Bedingungen des Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO u.a. Bestimmungen darüber enthalten, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen. Insofern können Regelungen wie § 30 Abs. 9 AO n.F., § 80 SGB X n.F. und § 107 BBG weiterhin Anwendung finden.

Soweit besondere Verschwiegenheitspflichten zu beachten sind, ist Folgendes zu beachten: Eine zulässige Auftragsverarbeitung legitimiert den Umgang mit personenbezogenen Daten durch den Auftragnehmer. Daraus folgt aber nicht die Zulässigkeit der Offenbarung von Daten, die besonderen gesetzlichen Verschwiegenheitspflichten, wie z. B. der ärztlichen Schweigepflicht oder dem anwaltlichen Mandantengeheimnis, unterliegen. Geheimhaltungspflichten schützen vor allem das Vertrauensverhältnis zwischen dem Geheimnisträger und dem Betroffenen. § 1 Abs. 3 Satz 2 BDSG a.F. und § 1 Abs. 2 Satz 3 BDSG n.F. stellen klar, dass die Datenschutzregelungen die Verpflichtung zur Wahrung besonderer Geheimhaltungspflichten unberührt lassen [Simi14, § 1 Rn. 175]. Die Datenschutz-Grundverordnung enthält keine vergleichbare Vorschrift, durch die das grundsätzliche Verhältnis zwischen dem Datenschutzrecht und den Geheimhaltungspflichten festgestellt wird. In mehreren Vorschriften setzt die Verordnung jedoch Geheimhaltungspflichten voraus und nimmt auf sie Bezug [Roßn18, § 8, Rn. 313 ff.]. Dadurch wird zum einen anerkannt, dass es zwischen Geheimhaltungs- und Datenschutzvorschriften Überschneidungsbereiche gibt, und zum anderen gerade kein Anwendungsvorrang des europäischen Datenschutzrechts vor den nationalen Geheimhaltungspflichten statuiert. Insofern gelten nach allen Datenschutzregeln die Geheimhaltungspflichten neben dem Datenschutzrecht. [Roßn18, § 8, Rn. 329].

Wegen dieser Parallelgeltung kann nicht jede datenschutzrechtliche Einwilligung zur Legitimierung der Offenbarung geheimnisgeschützter Daten ausreichen [JaRW11a, S. 228], [JaRo11, S. 142]. Solche Geheimnisse dürfen nur offenbart werden, wenn gesetzliche Offenbarungspflichten[58] bestehen oder der Betroffene (etwa Patient, Mandant) wirksam in die Offenbarung eingewilligt hat [JaRo11, S. 142], [BfDI22, S. 27]. Die Erklärung zur Entbindung von der gesetzlichen Schweigepflicht und die datenschutzrechtliche Einwilligung haben eine unterschiedliche inhaltliche Reichweite [JaRo11, S. 145][59] und gegebenenfalls unterschiedliche

[58]Diese kann sich aus z. B. aus § 53 StPO, § 383 ZPO, §§ 295, 296, 297, 298 SGB V, § 284 i. V. m. § 295 SGB V oder §§ 6, 7 IfSG (Infektionsschutzgesetz) ergeben.

[59]Schutz vor den Risiken der modernen Datenverarbeitung einerseits, Schutz vor einer Weitergabe sensitiver Informationen andererseits.

Adressaten.[60] Sie können daher nicht gleichgesetzt werden [Roßn18, § 8 Rn. 333], [JaRo11, S. 144f], [JaRW11b, S. 645]. Eine wirksame datenschutzrechtliche Einwilligung kann eine Entbindung von der Schweigepflicht allenfalls dann ersetzen, wenn sie ausdrücklich eine Datenweitergabe umfasst [JaRo11, S. 145].[61]

Zusammenfassend kann festgehalten werden, dass Anwender, die besonderen Geheimnispflichten unterliegen, sowohl eine datenschutzrechtliche Einwilligung über die Verarbeitung der Daten als auch eine Entbindung von der Schweigepflicht zu Zwecken der Datenverarbeitung beim Betroffenen einholen müssen.

R.2.4.2 § 203 StGB

Nach der Neufassung des § 203 StGB durch das Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen vom 30. Oktober 2017[62] ist die Beauftragung eines externen Scandienstleisters keine unbefugte Offenbarung und damit keine Verletzung von Privatgeheimnissen gemäß § 203 StGB mehr, auch wenn dafür eine Entbindung von der Schweigepflicht fehlt.[63]

Zwar ist gemäß § 203 Abs. 1 StGB den dort genannten Berufsgruppen untersagt, Geschäftsgeheimnisse oder dem persönlichen Lebensbereich angehörende Geheimnisse zu offenbaren, die ihnen in ihrer beruflichen Funktion anvertraut worden sind. Zu diesen Berufsträgern gehören unter anderem Angehörige von Heilberufen, Rechtsanwälte, Wirtschaftsprüfer, Steuerberater, aber auch Sozialpädagogen oder Angehörige von privaten Kranken-, Lebens- und Unfallversicherungen. Die Übergabe der Dokumente zum Scannen stellt ein Offenbaren im Sinn dieser Vorschrift dar. Jedoch dürfen nach dem neuen Abs. 3 Satz 2 HS 1 des § 203 StGB diese Geheimnisträger „fremde Geheimnisse gegenüber … Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist“. Die Gesetzesbegründung definiert diese mitwirkenden Personen als solche, „die zwar an der beruflichen oder dienstlichen Tätigkeit der schweigepflichtigen Person mitwirken, also in diese Tätigkeit in irgendeiner Weise eingebunden werden und Beiträge dazu leisten, allerdings ohne in die Sphäre des Berufsgeheimnisträgers eingegliedert zu sein“ [BT-Drs. 18/11936, S. 22]. Dafür, wann eine Mitwirkung an der beruflichen oder dienstlichen Tätigkeit des Berufsgeheimnisträgers vorliegt, gibt der Beispielkatalog in der Gesetzesbegründung Anhaltspunkte. Dieser erfasst neben Schreibarbeiten und Rechnungswesen auch IT-bezogene Tätigkeiten wie „Einrichtung, Betrieb, Wartung – einschließlich Fernwartung – und Anpassung informationstechnischer Anlagen, Anwendungen und Systeme aller Art“ sowie die „Bereitstellung von informationstechnischen Anlagen und Systemen zur externen Speicherung von Daten“ [BT-Drs. 18/11936, S. 22].

Für die nach § 203 Abs. 3 Satz 2 StGB befugte Offenbarung sind lediglich die Einbindung in die berufliche Tätigkeit des Berufsgeheimnisträgers und das Einvernehmen mit diesem. Die Verarbeitung und die Aufbewahrung der Dokumente gehört zu der beruflichen Tätigkeit des Berufsgeheimnisträgers. Wenn er die Dokumente scannen darf, erlaubt ihm § 203 Abs. 3 Satz 2 StGB, hierfür auch einen externen Dienstleister zu beauftragen. Da die Übergabe der Dokumente für die Inanspruchnahme des Scandienstleisters erforderlich

[60] Adressat der datenschutzrechtlichen Erklärung ist die verantwortliche Stelle, Adressat der Schweigepflicht hingegen der Geheimnisträger. Beide können, müssen aber nicht identisch sein.

[61] Die Problematik der Entbindung von der gesetzlichen Schweigepflicht und datenschutzrechtlichen Einwilligung trifft sowohl Ärzte in Privatpraxen als auch Krankenhäuser. Die Landeskrankenhausgesetze lösen diese Problematik meist nicht. Einzig das Landeskrankenhausgesetz Baden-Württemberg (BW-LKHG) unterscheidet in Ansätzen zwischen datenschutzrechtlicher Einwilligung und Entbindung von der Schweigepflicht. Das Scannen von Patientenakten ist unter bestimmten Voraussetzungen nach § 48 Abs. 2 BW-LKHG zulässig. Als Rechtsfolge hat der Geheimnisverpflichtete (Arzt) dann nach § 49 BW-LKHG nicht unbefugt im Sinne des § 203 StGB Patientengeheimnisse offenbart [GUKK12, § 49 BW-LKHG, S. 1].

[62] BGBl. I, 2541.

[63] Zu den rechtlichen Grundlagen des ersetzenden Scannens bei medizinischer Dokumentation s. Kapitel R.1.2.4.

ist, darf der Berufsgeheimnisträger ihm die Dokumente übergeben und der Scandienstleisters die Dokumente scannen, ohne dabei ein strafrechtliches Risiko einzugehen.

Das Gleiche gilt nach § 203 Abs. 3 Satz 2 HS 2 StGB für Scandienstleister, „wenn diese „sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit" der in § 203 Abs. 1 und 2 StGB genannten Berufsgeheimnisträger mitwirken.

Zum Ausgleich werden die „mitwirkenden Personen" nach dem neuen Abs. 4 des § 203 StGB ebenfalls einer Strafandrohung unterworfen.[64] Der Scandienstleister muss sich zur Geheimhaltung verpflichten und muss dafür sorgen, dass alle weiteren Personen, deren er sich bedient, zur Geheimhaltung verpflichtet werden.[65] Er wird nach § 203 Abs. 4 Satz 1 StGB mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn er unbefugt ein fremdes Geheimnis offenbart, das ihm durch seine Tätigkeit als mitwirkende Person bekannt geworden ist. Er wird gemäß § 203 Abs. 4 Satz 2 Nr. 2 StGB ebenso bestraft, wenn ein Geheimnis von einer weiteren mitwirkenden Person offenbart wird und er nicht dafür Sorge getragen hat, dass diese weitere Person zur Geheimhaltung verpflichtet wird. Schließlich wird die mitwirkende Person gemäß § 203 Abs. 4 Satz 2 Nr. 3 StGB bestraft, wenn sie nach dem Tod des Berufsgeheimnisträgers ein Geheimnis unbefugt offenbart, das er von der verstorbenen Person oder aus deren Nachlass erfahren hat.

Auch der beauftragende Berufsgeheimnisträger muss eine neue strafrechtliche Pflicht übernehmen. Er muss dafür Sorge tragen, dass die „mitwirkende Person" zur Geheimhaltung verpflichtet wird, und wird nach § 203 Abs. 4 Satz 2 Nr. 1 StGB bestraft, wenn er diese Pflicht nicht erfüllt hat und die „weitere Person" ein Geheimnis unbefugt offenbart.

R.2.5 Strafbarkeit der Vernichtung von Originaldokumenten

Die Gesetze zur Förderung der elektronischen Verwaltung, der elektronischen Justiz und der Bearbeitung elektronischer Dokumente in anderen Wirtschafts- und Gesellschaftsbereichen zeigen, dass der Gesetzgeber elektronische Dokumente den Papierurkunden weitgehend gleichsetzen will. Auch will er das ersetzende Scannen, das einem ordnungsgemäßen Prozess wie der TR-RESISCAN folgt, unterstützen. Diese rechtliche Bewertung ist auch bei der Frage einer möglichen Strafbarkeit von ersetzendem Scannen zu beachten und reduzieren das Strafbarkeitsrisiko bei einem ordnungsmäßen Routineverfahren sehr. Allerdings bleiben sachliche Unterschiede zwischen elektronischen Dokumenten und Papierurkunden bestehen, die vom Recht – z. B. dem Beweisrecht – anerkannt werden. Daher ist nicht vollständig auszuschließen, dass ersetzendes Scannen durch das Vernichten von Originalurkunden im Einzelfall eine strafbare Urkundenunterdrückung gemäß § 274 StGB darstellen kann. Hierzu gilt es folgende Hinweise zu beachten.

Strafbar ist die Vernichtung von Urkunden, deren Verfügungsrecht einem nicht allein zusteht. Handelt es sich um eine Fotokopie, die eindeutig als solche zu erkennen ist, hat die Vernichtung jedenfalls keine strafrechtlichen Konsequenzen [ScSc14, § 267, Rn. 42a], [Fisc17, § 267, Rn. 19, 20]. Das Verfügungsrecht ist nicht zu verwechseln mit dem Eigentum an einer Urkunde. Es beschreibt vielmehr, wem das Recht zusteht, die Herausgabe der Urkunde oder die Einsichtnahme in die Urkunde zu verlangen (Beweisführungsrecht) [ScSc14, § 274, Rn. 5], [LaKü14, § 274, Rn. 2].

Bereits erwähnt wurde in diesem Zusammenhang der Ausschluss der Vernichtung der medizinischen Dokumentation.[66] Dieser stehen die Aufbewahrungsfristen wie in § 10 Abs. 5 MBO-Ä oder § 57 Abs. 1 BMV-Ä entgegen. Viel wichtiger ist das Beweissicherungsinteresse des Patienten, um im Schadensfall eine fehlerhafte Behandlung nachzuweisen [Wilk11, S. 102]. Auch aus diesem Grund ist eine Vernichtung medizinischer Dokumentationen in der Regel vor Ablauf der gesetzlichen Aufbewahrungsfristen

[64] Die Gesetzesbegründung, BT-Drs. 18/11936, 20, spricht von einer „Verlängerung" des strafrechtlichen Geheimnisschutzes.

[65] Die Pflicht zur Verpflichtung zur Geheimhaltung entfällt, wenn die sonstige mitwirkende Person selbst Berufsgeheimnisträger ist.

[66] Zu den rechtlichen Grundlagen des ersetzenden Scannens bei medizinischer Dokumentation s. Kapitel R.1.2.4.

ausgeschlossen.[67] Das Beweisführungsrecht des Patienten oder Dritter an medizinischen Dokumentationen endet jedoch in der Regel mit Ablauf gesetzlicher Aufbewahrungsfristen. Es kann im Einzelfall darüber hinausgehen, z. B. wenn es in einem konkreten Rechtsstreit gerade auf bestimmte Originalurkunden ankommt. Ist ein jedoch Beweisführungsinteresse ausgeschlossen, scheidet auch eine Urkundenunterdrückung, deren Verbot die Verletzung dieses Interesses verhindern soll, aus.

Das Beweisführungsrecht geht einher mit einer Vorlagepflicht, nach der der Inhaber der Urkunde verpflichtet ist, diese auf Verlangen eines Dritten vorzulegen. Eine solche Vorlagepflicht begründet z. B. § 422 ZPO, wenn der Beweisführer[68] nach bürgerlich-rechtlichen Vorschriften eine Vorlage der Urkunde verlangen kann. Ein solches Recht findet sich z. B. für Gesellschafter in §§ 118, 157, 166, 233 HGB. In der Praxis ist § 810 BGB in Verbindung mit § 630g BGB besonders wichtig, um die Einsichtnahme in Patientenakten in Arzthaftungsprozessen zu ermöglichen [Musi12, § 422, Rn. 1].

Eine öffentlich-rechtliche Vorlagepflicht, die bloßen Überwachungsaufgaben dient, schließt nicht notwendig das alleinige Verfügungsrecht des Urkundeninhabers aus [ScSc14, § 274, Rn. 5], [LaKü14, § 274, Rn. 2]. Eine solche öffentlich-rechtliche Vorlagepflicht besteht z. B. in § 97 AO gegenüber Finanzbehörden.

Zur Erfüllung des Straftatbestands von § 274 StGB muss der Täter subjektiv auch mit Nachteilszufügungsabsicht handeln, wobei er sicheres Wissen haben muss, dass der Nachteil Folge der Tat ist, er diesen Nachteil zumindest als notwendige Folge seines Handelns hinnimmt. [BGH, NStZ 2010, 332]. Eine Nachteilszufügungsabsicht wird in der Regel **nicht** bestehen, wenn ein Verfügungsberechtigter eine große Anzahl von Originalurkunden in einem geregelten Massenverfahren ohne Ansehung des Einzelfalls nach dem Stand der Technik ersetzend scannt und sicherstellt, dass die elektronischen Dokumente mit der Urschrift übereinstimmen.

Geht er nach TR-RESISCAN vor, will er gerade beweiskräftige elektronische Dokumente erzeugen und handelt eben **nicht** mit der Absicht, ein Beweisführungsrecht zu beeinträchtigen.

Eine Nachteilszufügungsabsicht wird dann nur im konkreten Einzelfall festzustellen sein, z. B. wenn von einer Seite bereits Ansprüche geltend gemacht worden sind, bei deren gerichtlichen Durchsetzung es auf die Originalurkunden ankommen kann und das Scanprodukt zur Beweisführung gerade nicht ausreicht.

Hinsichtlich medizinischer Dokumentationen ist zudem durch die gesetzlichen Regelungen zur Beweislast und Beweisvermutungen bei Haftung für Behandlungs- und Aufklärungsfehler nach § 630h BGB anzunehmen, dass bei Vernichtung der Originale der Patientenakte keine Nachteilszufügungsabsicht seitens der Behandelnden oder des Krankenhauses vorlag. Die Vernichtung der Originalurkunden bringt ihnen in der Regel Nachteile.

Eine Vernichtung von Originalurkunden ist in der Regel auch nicht rechtswidrig und damit straffrei, wenn der Inhaber des Beweisführungsrechts darin, wie z. B. der Patient in Bezug auf medizinische Dokumentationen eingewilligt hat [Fisc17, § 274, Rn. 10]. Zu beachten ist aber, dass auch andere, wie z. B. der Behandelnde oder Versicherer ein Beweisführungsrecht haben könnten, das einer Vernichtung entgegenstehen kann.

Der Anwender der TR-RESISCAN hat vor dem Vernichten der Urkunden demnach selbständig zu prüfen, ob Vorschriften ein Beweisführungsrecht einer dritten Person oder eine eigene Vorlagepflicht begründen und ob das Scanprodukt einen vergleichbaren Beweiswert besitzt wie die Urkunde. Soweit die gerichtlichen Verfahrensordnungen insoweit ausdrücklich einen Übertragungsnachweis mit der qualifizierten Signatur eines Urkundsbeamten vorschreiben, steht deshalb einer Vernichtung solcher urschriftersetztend eingescannter Ausgangsdokumente nichts im Weg.

[67] Nach § 630f Abs. 3 BGB sind Patientenakten über zehn Jahre nach Abschluss der Behandlung aufzubewahren, längere Aufbewahrungsfristen gelten z. B. bei Bluttransfusionen und Röntgenaufnahmen.

[68] Beweisführer in einem Prozess ist derjenige, der die Beweislast trägt. Den Beweis hat in der Regel derjenige zu erbringen, der ein Recht für sich behauptet.

Im Übrigen kann das papiergebundene Original, an dem ein Dritter ein Beweisführungsrecht oder der Anwender eine eigene Vorlagepflicht hat, in der Regel nur dann innerhalb der gesetzlichen Aufbewahrungsfrist vernichtet werden, wenn es dafür einen Zulässigkeitstatbestand (z. B. §§ 110b SGB IV) gibt und es durch ein ordnungsgemäß erzeugtes Digitalisat (nach TR RESISCAN) ersetzt wurde.

R.2.6 Gefährdung und Sicherung des Scanprodukts

Das folgende Kapitel beschäftigt sich mit Gefährdungen, die sich durch Bildveränderungen am Scanprodukt ergeben können. Anschließend werden technische Mittel beschrieben und aufgezeigt, die die Integrität und Authentizität des Scanprodukts zu schützen vermögen.

R.2.6.1 Bildveränderung

Bildveränderungen können ganz unterschiedliche Gründe und Ursachen haben. Nicht alle Bildveränderungen haben negative Auswirkungen, vielmehr können sie auch dem positiven Ziel dienen, eine Verbesserung der optischen Qualität zu erreichen.

R.2.6.1.1 Bildverbesserung

Bildverbesserungen sind in erster Linie solche Maßnahmen, die die Lesbarkeit des Scanprodukts erhöhen. Das äußere Erscheinungsbild kann so verarbeitet werden, dass das Scanprodukt eine optisch bessere Qualität aufweist als das Original. So können eine sehr kleine Schrift vergrößert, Flecken entfernt oder der Kontrast optimiert werden, so dass ursprünglich schlecht lesbare Dokumente am Bildschirm deutlich besser zu lesen sind [RoNe14b, S. 889], [RFJW08, S. 20]. Diese Maßnahmen führen nicht zu einer Veränderung des Dokumenteninhalts.

Es wird jedoch auch bei Veränderungen am elektronischen Dokument, die eine Verbesserung darstellen, ein vom Original abweichendes Abbild erzeugt. Eine genaue Abgrenzung, wann nicht mehr von bildlicher Übereinstimmung gesprochen werden kann, ist abstrakt nicht möglich. Sie beruht im konkreten Fall in weiten Teilen auf einer subjektiven Einschätzung. Die Entscheidung darüber obliegt dem Anwender unter Abwägung der Vorteile einerseits und dem Interesse an einem möglichst originalen Abbild andererseits [RFJW08, S. 52].

Wird eine bildliche Übereinstimmung zwischen Original und Scanprodukt gefordert, empfiehlt es sich, das in Frage stehende Original doppelt zu verarbeiten. Damit wird erstens die optische Qualität erhöht und zweitens ein völlig identisches Abbild festgehalten. Getätigte Veränderungen sollten in jedem Fall im Transfervermerk (s. R.2.7.4) festgehalten werden, damit diese nachvollzogen werden können und damit der Betrachter des Scanprodukts dessen Qualität abschätzen kann [RFJW08, S. 97].

R.2.6.1.2 Fehler und Manipulationen

Bildveränderungen können auch das Ziel verfolgen, den Inhalt zu verändern. Zu unterscheiden ist hierbei zwischen Fehlern einerseits und Manipulationen andererseits.

R.2.6.1.2.1 Fehler

Fehler haben entweder technische oder menschliche Ursachen und sind unfreiwilliger Natur.

Technische Gründe sind auf einen Mangel am Scansystem zurückzuführen, der dazu führt, dass der Scanner nicht ordnungsgemäß arbeitet. Die Ursachen sind vielschichtig, fehlerhafte Konfiguration der Scanner-Optik, Verschmutzung der Linse, mangelhafte Auflösung, mehrfacher Einzug[69] oder technisches Versagen können solche Gründe sein.

[69] Werden bei einem mehrseitigen Dokument mehrere Seiten gleichzeitig eingezogen, wird das Original nur unvollständig erfasst.

Technische Fehler können nicht vollständig verhindert werden. Allerdings kann durch eine hohe Basisqualität und regelmäßige, sorgfältige Wartung der technischen Systeme ein hoher Grad an Zuverlässigkeit gewährleistet werden. Verantwortlich dafür sind nicht nur die Hersteller und Kundendienste, auch die zum Scannen verantwortlichen Personen können hierzu beitragen.

Menschliche Gründe liegen vor, wenn die verantwortliche Person bei der Vorbereitung, Durchführung oder Nachbereitung Fehler begeht. Auch hier sind die Möglichkeiten denkbar weit und können nur exemplarisch aufgezeigt werden. So können Einstellungen am Scanner, die der bestmöglichen Qualität des Scanprodukts dienen sollen, händisch falsch programmiert werden. Auch kann das Original insgesamt vertauscht, versehentlich umgedreht oder in der Reihenfolge verändert eingelegt worden sein.

Die Ursachen menschlicher Fehler können ebenso minimiert werden. Notwendig hierfür ist in erster Linie eine ausführliche Handlungsanweisung, die im Unternehmen oder in der Behörde als verbindliche Grundlage anzuwenden ist und die Mitarbeiter für einen verantwortungsbewussten Umgang sensibilisieren soll.

R.2.6.1.2.2 Manipulation

Manipulationen stellen eine gezielte und verdeckte Einflussnahme auf den Dokumenteninhalt dar, um die Beweisrichtung zu verändern. Sie können am Original, im Scanprozess oder in der Nachbereitung am Scanprodukt stattfinden.

So kann das Original vor der Erfassung verfälscht oder ausgetauscht werden, es können Blätter hinzugefügt, entnommen oder die Reihenfolge verändert werden. Manipulationen am Original sind am Scanprodukt nicht mehr feststellbar, insbesondere nicht, nachdem das Original vernichtet worden ist.

Beim Scanprozess kann der Scanner oder die Datenübertragung manipuliert werden, um Inhalte vorsätzlich zu verändern oder zu unterdrücken. Möglich ist, den Scanner mit einer falschen Software zu manipulieren, die Datenübertragung über das Netzwerk oder lokal anzugreifen oder Malware einzuspielen. Eine mögliche Sicherung kann nur präventiver Art sein und muss die Sensibilisierung der Mitarbeiter und ihre besondere Verpflichtung zur ordnungsgemäßen Einhaltung der Vorschriften umfassen. Eine elektronische Signatur hilft in diesem Stadium nicht weiter, da diese nur die Integrität des (fertigen) Scanprodukts gewährleisten kann und erst ab dem Zeitpunkt wirkt, in dem das Scanprodukt mit der Signatur versehen wurde.

Ohne technische Sicherung sind Manipulationen am Scanprodukt durch Veränderung oder Löschung von Inhalten spurlos möglich [RFJW08, S. 20].[70] Um ein Auffinden zu erschweren oder unmöglich zu machen, können Metadaten verfälscht oder falsch zugeordnet werden. Durch ungeeignete Nachbearbeitung wie zu starke Rausch-Filter, zu starke Bildkompression oder Farbreduktion kann eine Unlesbarkeit erreicht werden, die das Dokument völlig unbrauchbar machen kann.

Als Schutz ist auch möglich, Scanner so zu konfigurieren, dass optimale Einstellungen erreicht werden, die von dem einzelnen Mitarbeiter nicht ohne weiteres oder nur mit übergeordneter Autorisierung verändert werden können. Dies bietet sich z. B. dann an, wenn vorwiegend Dokumente mit gleichartigen Einstellungen gescannt werden sollen.

R.2.6.1.3 Barcode

Die Originale können vor dem Scannen mit Barcodes oder Strichcodes versehen werden, die helfen die Scanprodukte zu kontrollieren, zu sortieren und wiederzufinden. Diese Codes gehören zu den Metadaten einer Datei, enthalten also Informationen zu den Eigenschaften eines Dokuments, z. B. Aussteller, Seitenanzahl, Zugehörigkeit zu einer Akte, oder dienen der Trennung der Dokumente. Der Scanner kann dadurch die Zusammengehörigkeit von Dokumenten erkennen und die Originalakte jeweils in eine separate Datei ablegen.

[70] S. z.B. *FG Münster*, Urteil vom 24.11.2015, Az. 14 K 1542/15 AO.

In der Regel wird das Aufbringen keine Bildveränderung darstellen. Ein beliebiger Betrachter des Scanprodukts wird erkennen, dass es sich dabei, wie bei einem Poststempel, um einen nachträglich aufgebrachten Schriftzug handelt. Werden jedoch Inhalte überklebt, so dass Informationen unterdrückt werden, oder wird ein inhaltlich falscher Barcode auf das Dokument geklebt, so dass dieses nicht mehr aufgefunden oder nicht indexiert werden kann, liegt eine unzulässige Manipulation vor, die in jedem Fall zu vermeiden ist.

Wird ein Barcode eingesetzt, stellt sich die Frage nach der geeigneten Stelle. Möglich wäre zum einen, ein separates leeres Blatt zu nutzen, das vor das eigentliche Dokument, zu dem es gehört, eingefügt wird. Zu denken wäre aber auch daran, den Barcode direkt auf die erste Seite des Dokuments zu kleben. Keinesfalls dürfen hierdurch andere Informationen, sei es Titel, Autor, Datum oder Seitenzahl, überklebt werden. Der Barcode darf deshalb nur auf leeren Flächen angebracht werden.

Die Benennung einer einheitlichen Stelle auf Dokumenten für das Aufbringen ist kaum möglich, da es eine Vielzahl von Ausgestaltungsvarianten gibt. Möchte man dennoch eine einheitliche Stelle festlegen, so ist in erster Linie an den Blattrand[71] zu denken, z. B. der Freiraum zwischen der Lochung, da dieser in der Regel unbeschrieben ist. Um zu vermeiden, dass sich jemand zu einem späteren Zeitpunkt darauf beruft, es wäre eine wichtige Information überklebt worden, sollte eine Stelle gewählt werden, die in der Regel unbeschrieben bleibt. Eine Vermutung würde dann dafürsprechen, dass dort tatsächliche keine Information überklebt worden ist.

R.2.7 Beweisführung

Um durch das ersetzende Scannen keine gravierenden Nachteile zu erleiden, muss der Zweck der Beweissicherung – soweit dies möglich ist – auch nach dem Scannen von Papierdokumenten erreichbar sein, selbst wenn das Original bereits vernichtet worden ist [Wilk11, S. 79]. Das Scanprodukt soll die frühere Existenz des Originals belegen und die Vermutung der Übereinstimmung des Scanprodukts mit dem Original begründen. Dies ist nicht erst in einem Gerichtsprozess, sondern bereits in der Vermeidung von Rechtsstreitigkeiten oder in der außergerichtlichen Streitbeilegung von großer Bedeutung [HaBi93, S. 689].

R.2.7.1 Beweiswert des Scanprodukts

Ein gescanntes Dokument, das in elektronischer Form vorliegt, ist im Unterschied zu Papierdokumenten keine Urkunde, da es nicht in verkörperter Form vorliegt und auch ohne technische Hilfsmittel nicht lesbar ist.[72] Demnach kann es nicht für den Urkundenbeweis genutzt, sondern lediglich als Gegenstand des Augenscheins nach § 371 Abs. 1 Satz 2 ZPO als Beweismittel in den Prozess eingeführt werden [RoNe14b, S. 888], [Musi17, § 371, Rn. 12].

Originär elektronische Dokumente, die nicht mit einer qualifizierten elektronischen Signatur versehen sind (näheres hierzu im folgenden Abschnitt), weisen daher gegenüber Papierurkunden einen geringeren Beweiswert auf.[73] Wegen ihrer hohen Fälschungssicherheit wird Papierdokumenten ein hohes Vertrauen entgegengebracht. Dieses ist aus rechtlicher Sicht dann gegeben, wenn die Unversehrtheit des Dokuments und eventuelle Veränderungen daran erkennbar sind. Diese können nicht zuletzt durch einen Sachverständigen festgestellt werden. Darüber hinaus sind Papierdokumente ohne technische Hilfsmittel lesbar und die handschriftliche Unterschrift – als ein biometrisches Merkmal – erlaubt eine eindeutige Zuordnung zum Aussteller [JaWi09, S. 101]. Darüber hinaus können Kopien in Papierform vom Original unterschieden werden. Elektronische Dokumente bedürfen dagegen für ihre Lesbarkeit technischer Hilfsmittel und können ohne Qualitätsverlust verändert und vervielfältigt werden. Wenn die Sicherheitsziele nicht durch ausreichende organisatorische und technische Maßnahmen erreicht werden

[71] Sofern Informationen am Blattrand überhaupt ausgelesen werden können.

[72] S. z.B. VG Wiesbaden, Urteil vom 9.8.2017, Az. 6 K 808/17.WI.A, Rn. 36; VG Wiesbaden, Urteil vom 7.4.2017, Az. 6 K 280/17.WI.A, Rn. 33; VG Wiesbaden, Urteil vom 28.12.2016, Az. 6 K 332/16.WI, Rn. 32.

[73] S. z.B. VG Wiesbaden, Urteil vom 28.12.2016, Az. 6 K 332/16.WI, Rn. 33.

können, besteht die Gefahr, dass das Vertrauen in elektronische Dokumente und damit auch in den elektronischen Rechts- und Geschäftsverkehr verloren geht.

Die Vernichtung des papiernen Originals führt beim ersetzenden Scannen zu einer grundsätzlichen Veränderung der Beweissituation [RoNe14b, S. 887], [RFJW08, S. 61].[74] Da ein gescanntes Dokument keine Urkundenqualität aufweist, ist es umso wichtiger, dass alle Sicherheitsziele des ersetzenden Scannens eingehalten und glaubhaft durch die Beweisführer dargelegt werden können. Insbesondere dürfte entscheidend sein, wie einer Behauptung der Fälschung des Originals oder eines Fehlers im Übertragungsvorgang begegnet werden kann. Der Beweiswert kann deutlich erhöht werden, wenn beispielsweise der Scanprozess Maßnahmen zur Minimierung dieser Risiken vorsieht und die Ordnungsmäßigkeit des Scanverfahrens nachgewiesen werden kann [RoNe14a, S. 41].[75]

Zusammenfassend kann festgehalten werden, dass mit gescannten Dokumenten im Rahmen der freien Beweiswürdigung grundsätzlich Beweis geführt werden kann. Im Regelfall akzeptieren Gerichte auch die Vorlage gescannter Dokumente.[76] Macht jedoch der Prozessgegner das Fehlen des Originals geltend oder nutzt die Schwächen des gescannten Dokuments in seinem Prozessvortrag aus, kann sich dies nachteilig für den Nutzer des Scanprodukts auswirken.[77] Da gescannte Dokumente keine Urkunden sind und ihnen daher ein geringerer Beweiswert zukommt als den zugrundeliegenden Originaldokumenten, geht das ersetzende Scannen stets mit einer Verschlechterung der Beweissituation einher. Ob dieses Risiko in Kauf genommen wird, muss im Rahmen der Risikoeinschätzung (z. B. Dokumentenart, Schadenspotenzial, Prozesskosten, Schadensersatzansprüche) durch jeden Verantwortlichen selbst entschieden werden. Je weniger sicher der Scanprozess ausgestaltet ist, desto weniger vorhersagbar ist der Ausgang der Beweisaufnahme mit einem Scanprodukt.[78]

Auf Grund der stetigen Digitalisierung des Geschäftsverkehrs auf allen Ebenen und in allen Bereichen nimmt der Bedarf zu, auch elektronischen Dokumenten eine den Urkunden entsprechende Beweiskraft zukommen zu lassen. Deshalb hat der Gesetzgeber Regelungen zu bestimmten besonders vertrauenswürdigen Sicherungsmitteln und zu den Anforderungen an diese getroffen, deren Erfüllung das besondere Vertrauen rechtfertigt. Diese Vertrauensdienste sind zum einen in der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-VO)[79] geregelt und zum anderen im Vertrauensdienstegesetz (VDG) vom 18. Juli 2017, das das Signaturgesetz und die Signaturverordnung aufgehoben und abgelöst hat. Der Gesetzgeber hat weiterhin Beweiserleichterung geschaffen, wenn diese Vertrauensdienste zur Absicherungen der elektronischen Dokumente genutzt worden sind. Solche Beweiserleichterungen finden sich in § 371a und b ZPO sowie in Art. 35 Abs. 2 und 41 Abs. 2 eIDAS-VO.

R.2.7.2 Beweiswirkung der qualifizierten Signatur nach § 371a ZPO

§ 371a ZPO enthält für private und für öffentliche elektronische Dokumente, die mit einer qualifizierten Signatur versehen sind, spezifische Beweiserleichterungen (zum Folgenden s. [Roßn13, § 371a ZPO]).

Für private qualifiziert signierte elektronische Dokumente ergibt sich nach § 371a Abs. 1 Satz 2 ZPO bei erfolgreicher Prüfung der qualifizierten elektronischen Signatur nach Art. 32 eIDAS-VO ein Anschein der Echtheit der Erklärung, der nur durch Tatsachen entkräftet werden kann, die ernstliche Zweifel an der

[74] S. z. B. VG Wiesbaden, Urteil vom 7.4.2017, Az. 6 K 280/17.WI.A, Rn. 33; VG Wiesbaden, Urteil vom 28.12.2016, Az. 6 K 332/16.WI, Rn. 34.
[75] S. z. B. VG Wiesbaden, Urteil vom 9.8.2017, Az. 6 K 808/17.WI.A, Rn. 36; VG Wiesbaden, Urteil vom 28.12.2016, Az. 6 K 332/16.WI, Rn. 35.
[76] S. z. B. OVG NRW, Beschluss vom 5.4.2016, Az. 1 B 203/16; VG Köln, Beschluss vom 11.2.2016, Az. 15 L 2263/15.
[77] S. z. B. FG Münster, Urteil vom 24.11.2015, Az. 14 K 1542/15 AO.
[78] S. Kapitel R.2.8.
[79] EU ABl. L 257 vom 28.8.2014, S. 73.

Abgabe der Erklärung durch den Signaturschlüssel-Inhaber begründen [Roßn14, S. 3690].[80] Dieser erste Anschein für die Echtheit der Erklärung umfasst die Unverfälschtheit der Erklärung und die Zuordnung der Erklärung zum Unterzeichner.[81]

Für ein öffentliches elektronisches Dokument, das qualifiziert signiert ist, gilt nach § 371a Abs. 3 Satz 2 ZPO die gesetzliche Vermutung der Echtheit nach § 437 Abs. 1 ZPO, sofern sich das Dokument nach Form und Inhalt als öffentliches Dokument darstellt. In Anlehnung an den Begriff der öffentlichen Urkunde in § 415 Abs. 1 ZPO definiert § 371a Abs. 3 Satz 1 ZPO das öffentliche elektronische Dokument als ein elektronisches Dokument, das von einer öffentlichen Behörde innerhalb der Grenzen ihrer Amtsbefugnisse oder von einer mit öffentlichem Glauben versehenen Person innerhalb des ihr zugewiesenen Geschäftskreises in der vorgeschriebenen Form erstellt worden ist. Die gesetzliche Vermutung der Echtheit hat somit zwei Voraussetzungen. Zum einen müssen – wie bei privaten elektronischen Dokumenten – die Voraussetzungen einer qualifizierten Signatur vorliegen und im Zweifelsfall bewiesen werden. Zum anderen muss sich das Dokument nach Form und Inhalt als öffentliches Dokument darstellen. Angesichts der einfachen Möglichkeit, das Erscheinungsbild zu fälschen, wird es dabei vor allem auf das Zertifikat des Signaturschlüssel-Inhabers ankommen. So muss nach § 37 Abs. 3 VwVfG bei einem Verwaltungsakt in elektronischer Form das Zertifikat die erlassende Behörde erkennen lassen [Roßn13, § 37 VwVfG, Rn. 31 ff.]. Diesen Eintrag ins Zertifikat darf der Vertrauensdiensteanbieter nach § 12 Abs. 1 Satz 3 VDG nur nach Einwilligung oder Bestätigung der Behörde vornehmen.

Ist danach von der Echtheit der Erklärung auszugehen, entspricht die Beweiswirkung echter elektronischer Dokumente denen echter (Papier-)Urkunden: Auf sie finden die Vorschriften über die Beweiskraft privater und öffentlicher Urkunden entsprechende Anwendung. Demgemäß erbringt ein privates elektronisches Dokument nach § 371a Abs. 1 Satz 1 ZPO entsprechend § 416 ZPO vollen Beweis dafür, dass die in ihnen enthaltenen Erklärungen vom Aussteller abgegeben worden sind. Öffentliche elektronische Dokumente begründen nach § 371a Abs. 3 Satz 1 ZPO gemäß §§ 415 Abs. 1, 417, 418 Abs. 1 ZPO vollen Beweis für den beurkundeten Vorgang, für amtliche Anordnungen, Verfügungen und Entscheidungen sowie für die in ihnen bezeugten Tatsachen.

§ 371a ZPO gilt allerdings nur für Willens- und Wissenserklärungen [BT-Drs. 15/4067, S. 34.] Vielfach ist der Inhalt des Originaldokuments eine Erklärung. Das Scanprodukt ist jedoch nur ein technisches Abbild, dem selbst kein eigener Erklärungsgehalt zukommt. Wird eine elektronische Signatur in einem automatischen Scanprozess an das elektronische Scanprodukt angefügt, wird keine Erklärung signiert. Die Signatur ist in diesem Fall kein Unterschriftenersatz, sondern nur ein Sicherungsmittel, das den Nachweis ermöglicht, dass das Scanprodukt nach der Signierung nicht mehr verändert wurde. Es stellt mithin die Integrität sicher ([RFJW08, S. 90], [RoWi06, S. 2148]). Daher können nur originär elektronische Dokumente § 371a ZPO in Anspruch nehmen. Ein solches originär elektronisches Dokument könnte auch ein Transfervermerk[82] als qualifiziert signierte Erklärung der scannenden Stelle sein, der die Übereinstimmung von Original und Scanprodukt bezeugt. Die Beweiserleichterung gilt in diesem Fall nur für die Übereinstimmungserklärung und nicht auch für den Inhalt des Scanprodukts [RFJW08, S. 90f.], [RoWi06, S. 2148], [RoSW09, S. 132 ff.].

R.2.7.3 Beweiswirkung des gescannten Dokuments nach § 371b ZPO

Der durch das Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013 (E-Justice-Gesetz)[83] eingeführte § 371b ZPO erklärt die Vorschriften zur Beweiskraft öffentlicher Urkunden nach §§ 415 ff. ZPO explizit auf solche Dokumente anwendbar, die vom Papier in ein elektronisches Dokument übertragen wurden. Hierzu ist nach Satz 1 als erste qualifizierende Anforderung

[80] Dadurch soll das Vertrauen in die Rechtssicherheit und Verkehrsfähigkeit elektronische Dokumente gewährleistet werden, [BT-Drs. 15/4067, S. 34].

[81] Der Schutz des Empfängers geht damit weiter als bei Urkunden, für deren Echtheit der Empfänger vollen Beweis erbringen muss, §§ 439f. ZPO.

[82] Zum Transfervermerk s. auch R.2.7.7.

[83] BGBl. I, S. 3786.

eine Übertragung nach dem Stand der Technik vorzunehmen. Die Gesetzesbegründung bezieht sich hierfür auf die TR RESISCAN [BT-Drs. 17/12634, 34]. Weiterhin muss gemäß Satz 1 als zweite qualifizierende Anforderung ein Bestätigungsvermerk die bildliche und inhaltliche Übereinstimmung des Scanprodukts mit der Urschrift bestätigen. Sind das elektronische Dokument sowie die Bestätigung zusätzlich mit einer qualifizierten elektronischen Signatur versehen, dann gilt gemäß § 371b Satz 2 ZPO die Vermutung der Echtheit der so gescannten Urkunde im Sinn des § 437 ZPO.

Da § 371b ZPO jedoch nur für öffentliche Urkunden gilt, die durch eine öffentliche Stelle in ein elektronisches Dokument übertragen wurden, findet die Vorschrift auf Belege von Privatpersonen keine Anwendung. Gescannte Belege von Privatpersonen stellen weiterhin Objekte des Augenscheins dar und unterliegen der freien Beweiswürdigung.

R.2.7.4 Beweiswirkung des qualifizierten Siegels nach Art. 35 Abs. 2 eIDAS-VO

Die eIDAS-Verordnung hat für einige der von ihr geregelten qualifizierten elektronischen Vertrauensdienste[84] eigene Regelungen zu ihren Beweiswirkungen getroffen. Diese Beweisregelungen gelten zusätzlich zu den in der Zivilprozessordnung geregelten Beweiswirkungen. Da die eIDAS-Verordnung seit dem 1. Juli 2016 in Deutschland unmittelbar als Teil der deutschen Rechtsordnung gilt und gegenüber deutschem Recht einen Anwendungsvorrang genießt, sind diese Beweisregelungen in jedem Gerichtsprozess zu beachten [Roßn16a, S. 17 ff.], [Roßn15, S. 359 ff.]. Sie gehen in ihrer Beweiswirkung über die Beweisregelungen der Zivilprozessordnung hinaus (kritisch [Roßn16b, S. 647 ff.], [Jand15, S. 1209], [JaMD15, S. 689], [Roßn14, S. 3691f.]. Für ersetzendes Scannen sind außer qualifizierten elektronischen Signaturen vor allem qualifizierte elektronische Siegel und qualifizierte elektronischen Zeitstempel von Bedeutung.

Eine solche eigene Beweisregel enthält die eIDAS-Verordnung für qualifizierte elektronische Siegel. Elektronische Siegel sind nach Art. 3 Nr. 25 eIDAS-VO „Daten in elektronischer Form, die anderen Daten in elektronischer Form beigefügt oder logisch mit ihnen verbunden werden, um deren Ursprung und Unversehrtheit sicherzustellen“. Die Verordnung hat „elektronische Siegel“ als Vertrauensdienst eingeführt, um auch juristischen Personen das Signieren zu ermöglichen. Nach der eIDAS-Verordnung ist es möglich, ein Zertifikat auszustellen, das auf eine juristische Person lautet. Ein „elektronisches Siegel“ ist technisch gesehen also eine elektronische Signatur einer juristischen Person.

Qualifiziert ist ein elektronisches Siegel nach Art. 3 Nr. 27 eIDAS-VO, wenn es die Anforderungen eines fortgeschrittenen elektronischen Siegels nach Art. 36 eIDAS-VO erfüllt, von einer qualifizierten elektronischen Siegelerstellungseinheit[85] entsprechend Anhang II der eIDAS-Verordnung erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Siegel nach Anhang III der eIDAS-Verordnung beruht. Art. 35 Abs. 3 eIDAS-VO bestimmt für qualifizierte Siegel, dass diese, soweit sie auf einem in einem Mitgliedstaat ausgestellten qualifizierten Zertifikat beruhen, in allen anderen Mitgliedstaaten als qualifiziert anerkannt werden.

Für qualifizierte Siegel gilt nach Art. 35 Abs. 2 eIDAS-VO die „Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe der Daten, mit denen das qualifizierte elektronische Siegel verbunden ist“. Die Bezeichnung „Vermutung“ darf jedoch nicht aus dem Rechtsverständnis eines einzelnen Mitgliedstaats heraus ausgelegt werden, da sie gleichzeitig für 27 weitere Mitgliedstaaten Geltung beansprucht. Sie kann daher nicht mit der „gesetzlichen Vermutung“ im Sinn von § 292 ZPO gleichgesetzt werden, sondern ist aus der Zielsetzung und Systematik der Verordnung heraus auszulegen. Um das Ziel der Verordnung zu erreichen, dass das qualifizierte elektronische Siegel ein „Nachweis“ sein soll, der „den Ursprung und die Unversehrtheit des Dokuments belegen“ kann [Erwägungsgrund 59 der eIDAS-VO], und um systemwidrige Bevorzugungen gegenüber der qualifizierten elektronischen Signatur zu vermeiden, muss die „Vermutung“ des Art. 35 Abs. 2 eIDAS-VO im Sinn eines Anscheinsbeweises ausgelegt werden

[84] Für die qualifizierte elektronische Signatur sieht Art. 25 eIDAS-VO jedoch keine Regelung zum Beweiswert vor.

[85] Hinsichtlich der Anforderungen an eine qualifizierte Siegelerstellungseinheit verweist Art. 39 Abs. 1 eIDAS-VO auf die Regelung zu einer qualifizierten Signaturerstellungseinheit in Art. 29 eIDAS-VO.

[Roßn16a, S. 183 ff.] [Roßn16b, S. 649f.], [Jand15, S. 1209], [JaMD15, S. 689]. Das bedeutet, dass qualifizierten elektronischen Siegeln die gleiche Beweiswirkung zukommt wie qualifizierten elektronischen Signaturen nach § 371a Abs. 1 Satz 2 ZPO.

Für qualifiziert gesiegelte private elektronische Dokumente finden die Regelungen zum Urkundenbeweis keine Anwendung. Hierfür fehlt ein Verweis auf die Beweiswirkung von Urkunden nach § 415 ff. ZPO, wie dieser durch § 371a Abs. 1 Satz 1 ZPO für qualifizierte elektronische Signaturen erfolgt. Aber hinsichtlich der Unversehrtheit des gescannten Dokuments und der Richtigkeit der Herkunftsangabe des Transfervermerks[86] bewirkt Art. 35 Abs. 2 eIDAS-VO einen Anscheinsbeweis, der in seiner praktischen Wirkung mit dem Beweiswert einer Urkunde vergleichbar ist.

Dagegen könnten für qualifiziert gesiegelte öffentliche elektronische Dokumente die Regelungen zum Urkundenbeweis Anwendung finden. § 371a Abs. 3 Satz 1 ZPO fordert nämlich keine qualifizierte elektronische Signatur, sondern verlangt für die entsprechende Anwendung der Vorschriften über die Beweiskraft öffentlicher Urkunden nur, dass die elektronischen Dokumente von einer öffentlichen Behörde innerhalb der Grenzen ihrer Amtsbefugnisse oder von einer mit öffentlichem Glauben versehenen Person innerhalb des ihr zugewiesenen Geschäftskreises in der vorgeschriebenen Form erstellt worden sind. Die vorgeschriebene Form für einen Verwaltungsakt kann nach § 37 Abs. 3 Satz 1 VwVfG auch durch ein elektronisches Siegel erfüllt werden. Nur wenn Schriftform gefordert wird, ist nach § 37 Abs. 3 Satz 2 VwVfG eine qualifizierte elektronische Signatur erforderlich. Soweit ein elektronisches Siegel einer Behörde die vorgeschriebene Form erfüllt, können für derart gesiegelte elektronische Dokumente auch die Beweiswirkungen von öffentlichen Urkunden nach § 415 ff. ZPO gelten [Roßn16a, S. 186].

R.2.7.5 Beweiswirkung des qualifizierten Zeitstempels nach Art. 41 Abs. 2 eIDAS-VO

Eine ähnliche Beweisregel enthält die eIDAS-Verordnung auch für qualifizierte elektronische Zeitstempel. Elektronische Zeitstempel kannte auch schon das Signaturgesetz [Roßn13, § 2 SigG, Rn. 91 ff.]. Elektronische Zeitstempel sind nach Art. 3 Nr. 33 eIDAS-VO „Daten in elektronischer Form, die andere Daten in elektronischer Form mit einem bestimmten Zeitpunkt verknüpfen und dadurch den Nachweis erbringen, dass diese anderen Daten zu diesem Zeitpunkt vorhanden waren“. In der Praxis wird ein elektronischer Zeitstempel dadurch erstellt, dass der Hashwert eines Dokuments mit der Angabe der aktuellen Uhrzeit aus einer sicheren Zeitquelle zusammen qualifiziert signiert oder gesiegelt wird. Ein „qualifizierter elektronischer Zeitstempel“ ist nach Art. 3 Nr. 34 eIDAS-VO ein elektronischer Zeitstempel, der die Anforderungen des Art. 42 eIDAS-VO erfüllt.[87]

Für solche qualifizierten elektronischen Zeitstempel gilt nach Art. 41 Abs. 2 eIDAS-VO „die Vermutung der Richtigkeit des Datums und der Zeit, die darin angegeben sind, sowie der Unversehrtheit der mit dem Datum und der Zeit verbundenen Daten“. Wie bei qualifizierten elektronischen Siegeln ist auch bei qualifizierten elektronischen Zeitstempeln die „Vermutung“ des Art. 41 Abs. 2 eIDAS-VO nicht mit der „gesetzlichen Vermutung“ des § 292 ZPO gleichzusetzen, sondern im Sinn eines Anscheinsbeweises wie für qualifizierte elektronische Signaturen nach § 371a Abs. 1 Satz 2 ZPO zu verstehen.[88]

Für qualifiziert zeitgestempelte elektronische Dokumente finden die Regelungen zum Urkundenbeweis keine Anwendung. Hierfür fehlt ein Verweis auf die Beweiswirkung von Urkunden nach § 415 ff. ZPO, wie dieser durch § 371a Abs. 1 Satz 1 und Abs. 3 Satz 1 ZPO für qualifizierte elektronische Signaturen erfolgt. Aber hinsichtlich der Echtheit des gescannten Dokuments und hinsichtlich der Integrität und Authentizität der Datums- und Zeitangabe bewirkt Art. 41 Abs. 2 eIDAS-VO einen Anscheinsbeweis. Damit erzielt er zur Datums- und Zeitangabe sogar einen höheren Beweiswert, als für Papierurkunden nach § 416 ZPO erreicht werden kann.

[86] S. hierzu Kap. 2.7.7.
[87] S. hierzu Kapitel R.2.7.6.3.
[88] S. Kapitel R 2.7.4.

R.2.7.6 Signatur, Siegel und Zeitstempel

Elektronische Signaturen, Siegel oder Zeitstempel können bei entsprechender Ausgestaltung die Authentizität und Integrität des Scanprodukts nachweisen. Authentizität und Integrität bezeichnen verschiedene Eigenschaften eines Dokuments, die bereits im Abschnitt R.1 erläutert wurden. Weder die Authentizität noch die Integrität des Originals kann anhand des Scanprodukts überprüft werden [RFJW08, S. 102f.]. Wird das Original nach dem Scannen vernichtet, tritt in jedem Fall eine Verschlechterung der Beweissituation ein, da der Nachweis der Echtheit des Originals nur am Originaldokument selbst zu führen ist [RFJW08, S. 102].

Im folgenden Kapitel wird dargestellt, wie mit Hilfe elektronischer Signaturen, Siegel oder Zeitstempel die Grundsätze der Authentizität und Integrität gewahrt werden können.

R.2.7.6.1 Signaturen

Es existieren mehrere Arten elektronischer Signaturen, die in der eIDAS-Verordnung geregelt sind. Sie verfolgen unterschiedliche Funktionen und bieten unterschiedliche Sicherheits- und Nachweisniveaus (für das SigG [Roßn13, Einl. SigG, Rn. 7 ff., 99 ff.]).

Einfache elektronische Signaturen gemäß Art. 3 Nr. 10 eIDAS-VO sind „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner (Art. 3 Nr. 9 eIDAS-VO) zum Unterzeichnen verwendet. Eine einfache Signatur ist z. B. der getippte Name und einer Erklärung oder das Bild einer eigenhändigen Unterschrift. Einfache Signaturen haben jedoch aus rechtlicher Sicht keinerlei Sicherungswert und rufen keine beweisrechtlichen Rechtsfolgen hervor [Wilk11, S. 61], da sie weder Integrität noch Authentizität gewährleisten können, so dass sie im Folgenden nicht berücksichtigt werden.

Eine fortgeschrittene elektronische Signatur ist gemäß Art. 3 Nr. 11 eIDAS-VO eine elektronische Signatur, die die Anforderungen des Art. 26 eIDAS-VO erfüllt. Sie weist gegenüber einer einfachen Signatur gemäß Art. 26 eIDAS-VO zusätzlich vier weitere Merkmale auf. Sie muss ausschließlich dem Unterzeichner zugeordnet sein (lit. a), die Identifizierung des Unterzeichners ermöglichen (lit. b), unter Verwendung elektronischer Signaturerstellungsdaten erstellt worden sein, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann (lit. c), sowie so mit den auf diese Weise unterzeichneten Daten verbunden sein, dass eine nachträgliche Veränderung der Daten erkannt werden kann (lit. d). Fortgeschrittene elektronische Signaturen bieten daher hinreichenden Integritätsschutz, wenn die Algorithmen und Parameter genutzt werden, die die Bundesnetzagentur noch für geeignet hält. Nach den Anforderungen der eIDAS-Verordnung ist für fortgeschrittene elektronische Signaturen keine sichere Signaturerstellungseinheit und kein qualifiziertes Zertifikat gefordert. Neben der Begriffsbestimmung in Art. 2 Nr. 11 eIDAS-VO und den Anforderungen des Art. 26 eIDAS-VO enthält die eIDAS-Verordnung für fortgeschrittene elektronische Signaturen nur die allgemeinen Anforderungen an die Komponenten, Prozesse und Dienste für fortgeschrittene Vertrauensdienste gemäß Art. 19 Abs. 1 eIDAS-VO. Danach muss ein Vertrauensdienst nach dem jeweils neuesten Stand der Technik ein Sicherheitsniveau bieten, das dem jeweiligen Risiko angemessen ist. Die Herausgeber von nicht-qualifizierten Zertifikaten müssen nicht zwingend eine Verifizierung der Identität des Signaturschlüssel-Inhabers vornehmen, wie dies Art. 24 Abs. 1 eIDAS-VO für qualifizierte Vertrauensdienste fordert. Sie müssen auch keinen Verzeichnis- oder Widerrufsdienst gemäß Art. 24 Abs. 4 eIDAS-VO anbieten. Die Authentizität des lediglich mit einer fortgeschrittenen elektronischen Signatur versehenen Dokuments ist daher im Allgemeinen nicht ausreichend gewährleistet (für die vergleichbare Situation nach dem Signaturgesetz [Roßn03a, S. 164 ff.], [Wilk11, S. 64]).

Qualifizierte elektronische Signaturen gemäß Art. 3 Nr. 12 eIDAS-VO weisen alle Merkmale der fortgeschrittenen elektronischen Signaturen auf. Zusätzlich müssen sie auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Signaturzertifikat gemäß Anhang I der eIDAS-Verordnung beruhen und mit einer qualifizierten elektronischen Signaturerstellungseinheit gemäß Anhang II der eIDAS-Verordnung

erstellt werden. Der Vertrauensdiensteanbieter muss unter anderem gemäß Art. 24 Abs. 1 eIDAS-VO und § 11 VDG die Identität des Signaturschlüssel-Inhabers verifizieren sowie gemäß Art. 24 Abs. 4 eIDAS-VO einen Verzeichnisdienst und einen Widerrufsdienst anbieten. Das qualifizierte Zertifikat kann gemäß Art. 3 Nr. 9 und 10 eIDAS-VO nur für natürliche Personen ausgestellt werden.

Rechtsfolgen der Verwendung qualifizierter elektronischer Signaturen sind unter anderem die Erfüllung der elektronischen Form nach § 126a BGB, § 3a Abs. 2 VwVfG, § 87a Abs. 3 und 4 AO oder § 36a Abs. 2 SGB I. Unter Umständen kommt auch die Beweiserleichterung des § 371a Abs. 1 und 3 ZPO zum Zuge.[89]

Schließlich besteht für Zertifizierungsdiensteanbieter nach § 16 Abs. 5 VDG die Möglichkeit, sich an einer Vertrauensinfrastruktur zur dauerhaften Prüfbarkeit qualifizierter elektronischer Zertifikate der Bundesnetzagentur zu beteiligen. Diese soll die Funktion anbieten, die nach § 15 Abs. 1 SigG qualifizierte elektronische Signaturen mit Anbieter-Akkreditierung geboten haben (s. hierzu [Roßn13, § 15 SigG, Rn. 52 ff., 60 ff.]). Einzelheiten soll eine künftige Vertrauensdiensteverordnung nach § 20 Abs. 2 Nr. 5 VDG enthalten.

Die Verwendung geeigneter Verfahren erlaubt den mathematischen Nachweis, dass keine Veränderung am Scanprodukt erfolgt ist [RFJW08, S. 105]. Wird ein digitales Dokument mit einer zumindest fortgeschrittenen elektronischen Signatur gemäß Art. 3 Nr. 11 eIDAS-VO versehen, lässt sich ermitteln, ob das Dokument nach Unterzeichnung verändert worden ist; sie sichert mithin die Integrität des elektronischen Dokuments. Die Verwendung einer qualifizierten elektronischen Signatur erlaubt darüber hinaus die Feststellung der Authentizität des Dokuments [Wilk11, S. 210].

Die Entscheidung für oder gegen das Anbringen von qualifizierten elektronischen Signaturen obliegt dem einzelnen Anwender, es sei denn, eine Vorschrift erfordert dies. Um diese Entscheidung herbeizuführen, sollte eine erste Einteilung anhand des Schutzbedarfs des elektronischen Dokuments vorgenommen werden. Grundsätzlich gilt, dass für ein Dokument mit normalem Schutzbedarf keine qualifizierte elektronische Signatur notwendig ist, für einen sehr hohen Schutzbedarf hingegen schon. Beurteilungsmaßstab sollte die antizipierte Verwendung durch den Anwender sein sowie die Wahrscheinlichkeit, das gescannte Dokument nicht nur intern, sondern extern im Geschäftsverkehr zu verwenden, wo es im Zweifel als Beweismittel dienen muss. Soll die Bestätigung des korrekten Scanprozesses in den Genuss der Beweiserleichterung des § 371a Abs. 1 oder 3 ZPO kommen, ist eine qualifizierte elektronische Signatur nach Art. 3 Nr. 12 eIDAS-VO unumgänglich.[90]

Um Integrität und Authentizität bestmöglich zu wahren, sollte die Signatur unmittelbar nach dem Scanprozess angebracht werden, um den Zeitraum einer möglichen Manipulation an dem ungesicherten elektronischen Dokument zu minimieren.

R.2.7.6.2 Siegel

Die eIDAS-Verordnung hat „elektronische Siegel“ als Vertrauensdienst neu eingeführt, um Zertifikate auch für eine juristische Person ausstellen zu können. Ein elektronisches Siegel ist somit eine elektronische Signatur einer juristischen Person. Es bietet daher hinsichtlich Integrität und Authentizität die gleichen Sicherheitsfunktionen wie eine elektronische Signatur. Für qualifizierte elektronische Siegel gelten daher die gleichen Sicherheitsanforderungen wie für eine qualifizierte elektronische Signatur: Sie müssen ebenfalls die Anforderungen des Art. 24 eIDAS-VO erfüllen. Sie müssen außerdem nach Art. 3 Nr. 27 eIDAS-VO ein fortgeschrittenes elektronisches Siegel sein, das von einer qualifizierten Siegelerstellungseinheit erstellt worden ist und auf einem qualifizierten Siegelzertifikat nach Anhang III der eIDAS-Verordnung beruht. Die Anforderungen an ein fortgeschrittenes Siegel in Art. 36 eIDAS-VO entspricht der Anforderungen an eine fortgeschrittene elektronische Signatur nach Art. 26 eIDAS-VO. Art. 39 Abs. 1 eIDAS-VO verweist für die Anforderungen an eine qualifizierte Siegelerstellungseinheit unmittelbar auf die

[89] Zur Beweiswirkung des § 371a ZPO s. auch Kapitel R.2.7.2.

[90] S. z. B. VG Wiesbaden, Urteil vom 9.8.2017, Az. 6 K 808/17.WI.A, Rn. 36; VG Wiesbaden, Urteil vom 28.12.2016, Az. 6 K 332/16.WI, Rn. 35.

Anforderungen an eine qualifizierte Signaturerstellungseinheit in Art. 29 eIDAS-VO. Auch die Anforderungen an ein qualifiziertes Siegelzertifikat nach Art. 38 Abs. 1 eIDAS-VO und Anhang III der eIDAS-Verordnung entsprechen denen in Anhang I der eIDAS-Verordnung für ein qualifiziertes Signaturzertifikat.

Der Unterschied zwischen qualifizierten Siegeln und qualifizierten Signaturen besteht nur in der Präzision der Authentifizierung und der Sicherheit der Geheimhaltung der Signaturerstellungsdaten. Ein Signaturzertifikat ist auf eine natürliche Person bezogen. Dementsprechend wird nach Art. 24 Abs. 1 eIDAS-VO vor der Ausstellung des Zertifikats die Identität der natürlichen Person überprüft. Sie allein ist im Zertifikat als „Unterzeichner“ (Art. 3 Nr. 9 eIDAS-VO) ausgewiesen. Diese natürliche Person allein kann über die Signaturerstellungsdaten verfügen, weil sie allein über das Wissen, die biometrischen Merkmale oder die Signaturerstellungseinheit verfügt. Da somit die Signaturerstellungsdaten allein von einer bestimmten natürlichen Person genutzt werden können und ihr allein im Signaturzertifikat zugeordnet sind, kann nur sie die Signatur „zum Unterzeichnen“ (Art. 3 Nr. 10 eIDAS-VO) verwenden und ihr die Signatur als Willenserklärung zugeordnet werden.

Dagegen verknüpft der qualifizierte Vertrauensdiensteanbieter nach Art. 3 Nr. 30 eIDAS-VO in einem Siegelzertifikat die elektronischen Siegelvalidierungsdaten mit einer juristischen Person. Da diese selbst nicht handeln kann, müssen natürliche Personen, die hierzu berechtigt sind, Handlungen und Erklärungen für die juristische Person vornehmen. Dementsprechend wird nach Art. 24 Abs. 1 eIDAS-VO vor der Ausstellung des Zertifikats die Identität der juristischen Person überprüft. Hierzu wird die Existenz der juristischen Person und die Identität eines bevollmächtigten Vertreters festgestellt. Dieser Vertreter muss aber nicht die Person sein oder zu der Personengruppe gehören, die über die Siegelerstellungsdaten verfügen kann. Im Siegelzertifikat wird allein die juristische Person als „Siegelersteller“ (Art. 3 Nr. 24 eIDAS-VO) ausgewiesen. Diese juristische Person kann nicht selbst über die Signaturerstellungsdaten verfügen, sondern muss natürliche Personen beauftragen dies zu tun. Sie bestimmt also, wer für sie Siegel erstellen darf. Daher kann es sein, dass mehrere Personen in der Lage sind, über die Sicherungsmittel zu verfügen, um Siegel zu erstellen. Da alle Siegel durch das dazugehörige Siegelzertifikat der juristischen Person zugeordnet sind, kann der Empfänger nicht erkennen, welche natürliche Person das elektronische Siegel erstellt hat. Auch hängt die Sicherheit der Signaturerstellungsdaten unter Umständen von mehreren Personen ab, von denen jede die Sicherheit kompromittieren kann. Aus diesem Grund sieht die eIDAS-Verordnung elektronische Siegel nicht zum „Unterzeichnen“ vor, wie Art. 3 Nr. 10 eIDAS-VO elektronische Signaturen, sondern beschränkt sie auf den Zweck, „Ursprung und Unversehrtheit“ der gesiegelten Daten „sicherzustellen“. Ein elektronisches Siegel ist daher kein Mittel, um eine rechtsverbindliche elektronische Willenserklärung abzugeben, sondern ein Sicherungsinstrument, um Integrität und Authentizität gesiegelter Daten überprüfbar zu machen.

Da beim Transfervermerk vor allem diese Funktion im Vordergrund steht, kann zur Sicherung des Transfervermerks[91] statt einer qualifizierten elektronischen Signatur auch ein qualifiziertes elektronisches Siegel des Unternehmens, der Organisation, der Behörde oder des Gerichts verwendet werden, das bzw. die das Scannen durchführt. Statt der Beweisregeln des § 371a Abs. 1 und 3 ZPO kommt dann die Beweisregel des Art. 35 Abs. 2 eIDAS-VO zur Anwendung.[92]

R.2.7.6.3 Zeitstempel

Mit einem elektronischen Zeitstempel[93] verknüpft ein Vertrauensdiensteanbieter elektronische Daten in nachprüfbarer Form mit einem bestimmten Zeitpunkt (Art. 3 Nr. 33 eIDAS-VO). Mit ihrer Hilfe kann nachgewiesen werden, dass die elektronischen Daten zu diesem Zeitpunkt vorhanden waren. Durch ihre Anwendung soll – wie bei einem Post- und Eingangsstempel – insbesondere eine Vor- oder Rückdatierung des elektronischen Dokuments kenntlich gemacht und somit verhindert werden (s. zu Zeitstempeln nach

[91] S. zu diesem Kapitel R 2.7.7.
[92] S. zur Beweiswirkung Kapitel R.2.7.4.
[93] S. zu diesen Kapitel R 2.7.5.

dem Signaturgesetz [Roßn13, § 2 SigG, Rn. 91, 95], [BR-Drs. 966/96, S. 32]). Die Zeitangabe in einer elektronischen Signatur oder einem elektronischen Siegel ist hierfür nicht ausreichend, da diese die Systemzeit des Rechners wiedergibt, mit dessen Hilfe die Signatur oder das Siegel erstellt wird. Die Systemzeit eines Rechners ist aber im Allgemeinen leicht manipulierbar und deshalb für die Aufnahme als Metadatum in der Regel nicht ausreichend.

Ein „qualifizierter elektronischer Zeitstempel" ist nach Art. 3 Nr. 34 eIDAS-VO ein elektronischer Zeitstempel, der die Anforderungen des Art. 42 eIDAS-VO erfüllt. Der qualifizierte elektronische Zeitstempel muss nach Abs. 1 lit. a dieser Vorschrift Datum und Zeit so mit den Daten verknüpfen, dass die Möglichkeit der unbemerkten Veränderung der Daten nach vernünftigem Ermessen ausgeschlossen ist. Er muss nach lit. b auf einer korrekten Zeitquelle beruhen, die mit der koordinierten Weltzeit verknüpft ist. Drittens muss er mit einer fortgeschrittenen elektronischen Signatur unterzeichnet oder einem fortgeschrittenen elektronischen Siegel des qualifizierten Vertrauensdiensteanbieters versiegelt oder mit einem gleichwertigen Verfahren gesichert sein.

Qualifizierte Zeitstempel werden in der Praxis dergestalt umgesetzt, dass von den Daten, die mit einem qualifizierten Zeitstempel versehen werden sollen, ein Hashwert gebildet wird, der an den Zeitstempeldiensteanbieter übermittelt wird. Dieser ermittelt Datum und Uhrzeit nach der gemäß § 4 EinhZeitG[94] definierten gesetzlichen Zeit, die von der Physikalisch-Technischen Bundesanstalt in Braunschweig per Funk verbreitet wird. Der Zeitstempeldiensteanbieter bildet einen neuen Datensatz, der bei Bedarf aus einem Verweis auf das Zertifikat des Diensteanbieters, dem Hashwert und der ermittelten Zeitangabe besteht und mit seiner eigenen fortgeschrittenen Signatur oder seinem fortgeschrittenen Siegel versehen wird.[95]

Für Zeitstempeldiensteanbieter besteht nach § 16 Abs. 5 VDG die Möglichkeit, sich an einer Vertrauensinfrastruktur zur dauerhaften Prüfbarkeit qualifizierter elektronischer Zeitstempel der Bundesnetzagentur zu beteiligen. Einzelheiten zu dieser Vertrauensinfrastruktur soll eine künftige Vertrauensdiensteverordnung nach § 20 Abs. 2 Nr. 5 VDG festlegen.

Wer qualifizierte elektronische Zeitstempel vor Gericht als Beweismittel vorlegt, kann sich nach Art. 41 Abs. 2 eIDAS-VO auf die „Vermutung" der Richtigkeit des Datums und der Zeit, die darin angegeben sind, sowie der Unversehrtheit der mit dem Datum und der Zeit verbundenen Daten berufen.[96] Damit kann mit einem qualifizierten elektronischen Zeitstempel, der an gescanntes Dokument oder an eine Gruppe von gescannten Dokumenten angebracht worden ist (s. zu dem Hashwertbaumverfahren [RoSc06, S. 95 ff.] [Wilk11, S. 246], [BSI-TR03125]) die Echtheit und Unverfälschtheit sowohl des gescannten Dokuments wie auch der Zeitangabe bewiesen werden.

R.2.7.7 Transfervermerk

Der Transfervermerk hat das Ziel, dem Scanprodukt zu größtmöglichem Beweiswert zu verhelfen und somit ein verkehrsfähiges Beweismittel zu schaffen. Da das Original nach dem Scannen vernichtet werden soll, enthält der Transfervermerk typischerweise neben Angaben zum Scanprozess auch solche zum Original selbst. Soweit dies für das gescannte Dokument gefordert wird,[97] sollte in der Transfervermerk auch die Bestätigung aufgenommen werden, dass das Scanprodukt bildlich oder inhaltlich übereinstimmt. Der Transfervermerk kann entweder in das Scanprodukt integriert, zusammen mit dem Scanprodukt in einer Akte abgelegt oder aber in den Metadaten gespeichert werden [RoSW09, 123 ff.].

[94] Gesetz über die Einheiten im Messwesen und die Zeitbestimmung (Einheiten- und Zeitgesetz - EinhZeitG) in der Fassung vom 22.2.1985 (BGBl. I S. 408).

[95] BSI, IT-Grundschutz, Maßnahmenkataloge, M 5.67 Verwendung eines Zeitstempeldienstes, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05067.html

[96] Zu dieser „Vermutung" s. R 2.7.5.

[97] S. z.B. § 298a und 371b ZPO, 110a SGB IV.

Angaben zum Original dienen dazu, die Integrität und Authentizität desselben bewerten zu können. Solche Informationen können z. B. die Beschaffenheit des Originals, die Nutzung von Vorder- und Rückseite oder, soweit vorhanden, auch auffällige Merkmale, z. B. Wasserzeichen, Stempel oder Siegel, sein. Soll das Originaldokument zurückgegeben werden, kann auch der Lagerort vermerkt werden, was bei einem eventuellen Nachscannen hilfreich sein kann. Da die Beurteilung der Echtheit der Unterschrift ohne Sachverständigen in der Regel nicht möglich ist, können hierzu keine Angaben aufgenommen werden.[98] Sollte jedoch im Einzelfall die Unterschrift des Ausstellers im Beisein der für den Scanprozess zuständigen Person vorgenommen worden sein, kann dies durchaus im Vermerk notiert werden. All dies liefert Anhaltspunkte, um vor Gericht mit dem Scanprodukt die Echtheit des Dokuments trotz dessen Vernichtung zu belegen [RoSW09, 132 ff.], [Wilk11, S. 229f.].

Angaben zum Scanprozess dienen dazu, den Prozess für Dritte nachvollziehbar zu machen. „Da ein gescanntes Dokument – gleich welche schlechte oder gute Qualität der Scan letztendlich bietet – keine Urkundenqualität aufweist, ist es umso wichtiger, dass insoweit ein dokumentierter Scan-Prozess erfolgt, der alle Sicherheitsziele des ersetzenden Scannens einhält, dies mit der Maßgabe, dass in diesem Fall eingescannte Unterlagen bezüglich ihrer Übereinstimmung mit dem Original qualifiziert signiert zu beglaubigen sind."[99] Um dies zu erreichen, ist zum einen die Bezeichnung des Systems, mit dem das Scannen stattgefunden hat, notwendig, um die Sicherheitseigenschaften der verwendeten Technik nachzuvollziehen. Möglich ist dies durch Herstellerangaben, die Gerätenummer, zusätzliche besondere Merkmale sowie durch ein Qualitätszertifikat für den Scanner [Wilk11, S. 244].

Auch die verantwortliche Stelle oder Person, die das Dokument gescannt hat, ist so genau wie möglich zu bezeichnen, um diese zurückverfolgen zu können.

Weiterhin muss der Zeitpunkt des Scannens vermerkt werden. Dies dient dem Schutz vor Fälschung durch Rück- oder Vordatierung und erneutem Scannen. Da die Systemzeit im Allgemeinen manipulierbar und fehleranfällig ist, stellt sie keine hinreichend vertrauenswürdige Quelle dar, um einen Anscheinsbeweis zu rechtfertigen [Wilk11, S. 246]. Eine Lösung bietet hier ein qualifizierter Zeitstempel eines qualifizierten Vertrauensdiensteanbieters.[100] In diesem Fall umfasst der qualifizierte Zeitstempel den Transfervermerk und signiert damit auch die im Zeitstempel angegebenen Erklärungen. Er bewirkt in einem Beweisverfahren vor Gericht die „Vermutung" nach Art. 41 Abs. 2 eIDAS-VO,[101] dass Datum und Uhrzeit richtig angegeben sind und dass diese sowie der mit ihnen verbundene Transfervermerk und das eingebundene Scanprodukt seitdem unversehrt sind. Als entgeltliche Dienstleistung kann der qualifizierte Zeitstempel jedoch mit zusätzlichen Kosten verbunden sein. Die Entscheidung für oder gegen den Einsatz von Zeitstempeln sollte daher unter Beachtung des Schutzbedarfs für jedes Dokument selbständig getroffen werden. Für Archive bietet sich die kostengünstigere Möglichkeit eines Archivzeitstempels als eines gemeinsamen Nachweises für viele Dokumente an [RoSc06, S. 95 ff.] [Wilk11, S. 246], [BSI-TR03125].

Spielen Datum und Uhrzeit in einem möglichen Rechtsstreit absehbar keine entscheidende Rolle, kann der Transfervermerk – statt ihn durch einen qualifizierten elektronischen Zeitstempel zu sichern – auch durch eine qualifizierte elektronische Signatur signiert oder durch ein qualifiziertes elektronisches Siegel gesiegelt werden. Im Fall einer qualifizierten elektronischen Signatur kämen dann die Beweisregeln des § 371a ZPO[102] und im Fall eines qualifizierten elektronischen Siegels die Beweisregel des Art. 35 Abs. 2 eIDAS-VO[103] zur Anwendung.

[98] S. hierzu auch Kapitel R.1.1.

[99] VG Wiesbaden, Urteil vom 28.12.2016, Az. 6 K 332/16.WI, Rn. 35; ähnlich VG Wiesbaden, Urteil vom 26.9.2014, Az. 6 K 691/14.WI.A, Rn. 19.

[100] S. Kapitel R.2.7.5 und R.2.7.6.3.

[101] Zu dieser „Vermutung" s. Kapitel R.2.7.5.

[102] S. Kapitel R.2.7.3.

[103] S. Kapitel R.2.7.4.

R.2.7.8 Qualitätssicherung

Trotz bester Vorkehrungen ist es nicht ausgeschlossen, dass das Scanprodukt nicht die optimale Qualität aufweist. Mängel können auf ganz unterschiedlichen Gründen beruhen, allen voran auf den oben beschriebenen technischen oder menschlichen Fehlern. Die Qualitätskontrolle hat daher den Zweck, das Dokument auf Vollzähligkeit, Vollständigkeit, Fehler- und Manipulationsfreiheit hin zu prüfen, um diese zukünftig zu vermeiden.[104]

Vollständigkeit bedeutet, dass alle zum Dokument gehörenden Bestandteile gescannt vorliegen. Bedeutung erlangt dies z. B., wenn farbige Bestandteile zum Dokument gehören und soweit der Farbe eine eigenständige Bedeutung zukommt (z. B. farbige Kürzel in der Verwaltung oder verschiedenfarbige Durchschläge) [RFJW08, S. 52], [RoNe14a, S. 47 ff.] oder wenn ein Dokument aus verschiedenen Teildokumenten besteht [RFJW08, S. 61, 67], die in einem inneren Zusammenhang stehen (wie etwa Akten).

Vollzähligkeit bezeichnet hingegen allein die Tatsache, dass die Anzahl der Seiten des Originals und des Scanprodukts übereinstimmen.

Die Qualitätssicherung wird im Wege einer Sichtprüfung vorgenommen. Diese kann als vollständige Sichtprüfung aller gescannten Dokumente durchgeführt werden, die jedoch sehr aufwändig ist und damit in der Regel nicht zu empfehlen sein wird. Möglich ist weiterhin, lediglich Stichproben vorzunehmen. Diese werden üblicherweise von der Art und Wichtigkeit der Dokumente abhängig sein. Die Quote der Stichproben hängt von einer Vielzahl von Faktoren ab. Eine generelle Empfehlung ist auf Grund der Vielzahl der möglichen Dokumentarten nicht möglich. Die Stichprobe erbringt eine gewisse Wahrscheinlichkeit, mit der gewisse Arten von Fehlern entdeckt werden können. Je höher die Quote, desto größeres Gewicht kann dieser im Rahmen der Beweiswürdigung beigemessen werden. Die abschließende Entscheidung muss dem jeweiligen Anwender der TR überlassen bleiben und sollte in einer internen Arbeitsanweisung festgelegt werden.[105]

Zunächst ist zu klären, was durch eine Qualitätssicherung überhaupt erreicht werden kann. Eine Sichtprüfung kann die Sicherstellung der optischen Qualität ermöglichen. Eine vollständige Sichtprüfung wird aber in der Regel nicht notwendig sein, da diese Art der Fehler auf technischen Einstellungen basiert und sich daher wiederholt. Hier ist also eine Stichprobe völlig ausreichend. Die Vollständigkeit des Scanprodukts kann durch einen Sichtvergleich in der Regel festgestellt werden. Probleme bereitet dies bei großen Mengen zu scannender Dokumente. Allerdings sollte der Anwender im eigenen Interesse eine Qualitätssicherung so genau wie möglich durchführen. Die inhaltliche Richtigkeit kann nicht völlig durch eine vollständige Sichtprüfung sichergestellt werden. Wurde bereits das Original manipuliert, werden das Originaldokument und das Scanprodukt übereinstimmen. Eine Qualitätssicherung in Form einer Sichtprüfung hilft dann nicht weiter. Treten Manipulationen (oder Fehler) am Scanprodukt auf, kann eine Sichtprüfung durchaus Aufschluss geben und diese aufdecken. Allerdings stellt sich die Frage der Praktikabilität. Insbesondere bei großen Mengen an Daten, sei es Zahlentabellen, Bilanzen oder Ähnliches, ist ein manueller Eins-zu-Eins-Abgleich nicht zu leisten, da dies den manuellen Vergleich jeder einzelnen Zahl voraussetzt. Zu denken wäre hier daran, nur bedeutsame Zahlen oder Daten abzugleichen, wie Zwischenergebnisse oder Endsummen. In jeden Fall muss das Verhältnis zwischen Nutzen und Aufwand gewahrt bleiben.

R.2.8 Rechtliche Risikobewertung

Eine kurze Bewertung der rechtlichen Risiken des ersetzenden Scannens sollte nach Scanobjekt, Scanprozess und Scanprodukt differenzieren:

[104] S. hierzu VG Wiesbaden, Urteil vom 9.8.2017, Az. 6 K 808/17.WI.A, Rn. 35; ähnlich VG Wiesbaden, Urteil vom 26.9.2014, Az. 6 K 691/14.WI.A, Rn. 18.

[105] Für Personalakten empfiehlt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit eine hundertprozentige Sichtprüfung sowie Verwendung qualifizierter elektronischer Signaturen an jedem einzelnen elektronischen Dokument [BfDI23, S. 63].

R.2.8.1 Vernichten des Scanobjekts

Bezogen auf das Scanobjekt sind zwei Probleme zu unterscheiden: die Zulässigkeit der Vernichtung des Originaldokuments und Beweisprobleme durch das Fehlen des vernichteten Originaldokuments:

Das ersetzende Scannen ist inzwischen in vielen Bereichen ausdrücklich durch verbindliche Vorschriften zugelassen.[106] Auch externe Dienstleister mit dem Scannen und dem Vernichten der Originale zu beauftragen, ist bei Beachtung der entsprechenden Vorgaben straf- und datenschutzrechtlich zulässig.[107]

Wo eine ausdrückliche Zulassung fehlt und Interessen Dritter oder öffentliche Interessen an der Aufbewahrung der Originaldokumente bestehen, sollte von einer Vernichtung der Originaldokumente abgesehen werden.[108] Hier könnten sogar strafrechtliche Risiken entstehen.[109] Statt die Originaldokumente zu vernichten, sollte versucht werden, sie – soweit möglich – den Berechtigten zurückzugeben. In Zweifelsfällen sollten sie aufbewahrt werden.

Sind Rechtsstreitigkeiten nicht auszuschließen und in diesen mit der Beweiseinrede zu rechnen, dass das Originaldokument nie (so) existiert hat oder vor dem Scannen gefälscht oder verfälscht worden ist, sollten die Originaldokumente aufbewahrt werden. Diesen Einreden kann ohne das Original oft nicht entgegengetreten werden.[110] Soweit diese Einreden (hinsichtlich Zeiträumen, Möglichkeiten, Motiven) plausibel sind und Hilfstatsachen fehlen, die die Behauptung, dass ein dem Scanprodukt entsprechendes Original existiert hat, beweisen können, wird die Beweisführung mit dem Scanprodukt missglücken. Dann wird der Rechtsstreit nach Beweislast entschieden. Dies kann zu einem Prozessverlust führen.

Ist die Zulässigkeit eines ersetzenden Scannens zweifelhaft oder ein Prozessverlust möglich und nachteilig, sollte das Originaldokument aufgehoben werden. Dies wird im Regelfall nur wenige Dokumente(narten) betreffen.

R.2.8.2 Durchführen des Scanprozesses

Hinsichtlich des Scanprozesses gibt es in einzelnen Bereichen bestimmte Anforderungen, die zu beachten sind.[111] Ansonsten ist das Scannen ordentlich, fehlerfrei und vollständig durchzuführen.[112] Hierzu gibt die TR RESISCAN vielfältige Hinweise. Kann die Ordentlichkeit des Scanprozesses nicht nachgewiesen werden, entsteht ein Risiko, dass die Korrektheit des Scanprodukts bezweifelt werden kann.[113] Einreden in einem Rechtsstreit, dass einzelne Seiten des Dokuments oder wichtige Information im Scanprodukt fehlen, kann dann nicht widerlegt werden.

Damit die Anforderungen an den Scanprozess eingehalten werden, sind innerhalb der Organisation entsprechende Anweisungen zu geben oder gegenüber Dienstleistern geeignete Verträge abzuschließen. Die Ergebnisse des Scannens sind durch risikoadäquate Qualitätskontrollen zu sichern.[114] Der gesamte Scanprozess ist in ein geeignetes Managementsystem einzubinden.

Um die Qualität des Scanprozesses nachweisen zu können, sind Anweisungen, Verträge, Qualitätskontrollen und sonstige Maßnahmen des Managementsystems zu dokumentieren. Für den Nachweis eines

[106] S. Kapitel R.1.2.1 bis R.1.2.8.
[107] S. Kapitel R.2.4.
[108] S. hierzu vorsichtig *VG Wiesbaden*, Urteil vom 7.4.2017, Az. 6 K 280/17.WI.A, Rn. 33; *VG Wiesbaden*, Urteil vom 28.12.2016, Az. 6 K 332/16.WI, Rn. 36; ähnlich *VG Wiesbaden*, Urteil vom 26.9.2014, Az. 6 K 691/14.WI.A, Rn. 18.
[109] S. Kapitel R.2.2 und R.2.5.
[110] S. Kapitel R.2.7.1.
[111] S. Kapitel R.1.2.1 bis R.1.2.8.
[112] S. Kapitel R.2.6.
[113] S. z.B. VG Wiesbaden, Urteil vom 26.9.2014, Az. 6 K 691/14.WI.A, Rn. 18.
[114] S. Kapitel R.2.7.8.

ordentlichen Scanprozesses ist die Auditierung des Managementsystems und die Zertifizierung der verwendeten Techniksysteme hilfreich.

Bezogen auf das einzelne Scanprodukt sollte ein Transfervermerk[115] dessen Übereinstimmung mit dem Scanobjekt bestätigen und alle relevanten Informationen über das Scanobjekt, den Scanvorgang und das Scanprodukt festhalten.[116]

R.2.8.3 Sicherung des Scanprodukts

Gescannte Dokumente werden von Unternehmen, Behörden und Gerichten weitgehend akzeptiert. Sie können als Grundlage für die weitere Verarbeitung der in ihnen enthaltenen Informationen genutzt werden.

Bezogen auf das Scanprodukt kann jedoch nicht ausgeschlossen werden, dass in einem Rechtsstreit dessen Manipulation behauptet wird. Soweit diese Einrede (hinsichtlich Zeiträumen, Möglichkeiten, Motiven) plausibel und das Scanprodukt als Beweismittel streitentscheidend ist, kann dies zu einem Verlust des Rechtsstreits führen.[117] Die Einrede kann jedoch widerlegt werden, wenn Sicherungsmittel eingesetzt werden, durch die eine Manipulation erkannt werden kann. Mit ihnen kann nachgewiesen werden, dass das Scanprodukt seit Anbringen des Sicherungsmittels nicht verändert worden ist. Als solche Sicherungsmittel kommen vor allem elektronische Signaturen, elektronische Siegel und elektronische Zeitstempel in Frage.[118] Sind diese Sicherungsmittel „qualifiziert“ im Sinn der eIDAS-Verordnung, kann der Beweisführer sogar spezifische Beweisregeln für sich geltend machen, nach denen die Echtheit des Scanprodukt rechtlich unterstellt wird.[119]

Eine besonders hohe Beweissicherheit entsteht, wenn das Scanobjekt und der Transfervermerkt zusammengefasst und beide von dem Sicherungsmittel erfasst werden.[120] Um den Vorwurf auszuschließen, das Scanprodukt vor der Signierung, Siegelung oder Zeitstempelung manipuliert zu haben, sollte das Sicherungsmittel sofort nach dem Scannen angebracht werden. Wenn Signatur, Siegel oder Zeitstempel durch einen Dritten, wie einem Scan-Dienstleister oder einem Vertrauensdiensteanbieter, die kein Manipulationsinteresse haben, angebracht worden ist, steigert dies noch die Glaubwürdigkeit des gesamten Sicherungsverfahrens.

[115] S. Kapitel R.2.7.7.
[116] S. z.B. VG Wiesbaden, Urteil vom 26.9.2014, Az. 6 K 691/14.WI.A, Rn. 19.
[117] S. Kapitel R.2.7.1.
[118] S. Kapitel R.2.7.6.
[119] S. Kapitel R.2.7.2 bis R.2.7.5.
[120] S. Kapitel R.2.7.7.

R.3 Ausblick

Viele Herausforderungen des ersetzenden Scannens sind in den letzten Jahren durch den Gesetzgeber gelöst worden. Dennoch sind in vielen Rechtsbereichen immer noch keine expliziten Vorschriften zum ersetzenden Scannen zu finden. Problematisch ist insbesondere, dass keine objektiven Gründe erkennbar sind, warum in einigen Rechtsbereichen das ersetzende Scannen durch eine gesetzliche Vorschrift erlaubt wird, in anderen Bereichen aber mangels entsprechender Vorschriften nicht. Daher besteht in diesen Rechtsbereichen noch eine rechtliche Unsicherheit auf Seiten der Praxis, die durch transparente und klare Regelungen beseitigt werden sollte. Vorbilder könnten das E-Government-Gesetz mit seinem § 7 und das E-Justice-Gesetz mit seiner Regelung zu § 298a ZPO sein. Diese Regelungen geben die Erlaubnis, Papierdokumente in elektronische Dokumente zu übertragen und die Originale anschließend zu vernichten oder zurückzugeben. Die Übertragung ist nach dem Stand der Technik durchzuführen, wofür die TR-RESISCAN herangezogen werden kann.[121]

Bisher werden gescannte Dokumente ebenso wie Kopien von Papierdokumenten beweisrechtlich als Augenscheinsobjekte eingeordnet. § 371b ZPO enthält eine spezielle Regelung des Beweiswerts für öffentliche Urkunden, die durch eine öffentliche Behörde oder durch eine mit öffentlichem Glauben versehene Person nach dem Stand der Technik in ein elektronisches Dokument übertragen worden sind. Liegt ein Nachweis vor, dass das elektronische Dokument mit der Urschrift bildlich und inhaltlich übereinstimmt, finden die Vorschriften über die Beweiskraft öffentlicher Urkunden entsprechende Anwendung. Dies entspricht der Funktion eines Transfervermerks. Auf die Ausgestaltung des Nachweises wird es entscheidend ankommen, ob die Beweisunsicherheit, die mit einer Vernichtung der Originalurkunde einhergeht, ausgeglichen werden kann. Mittels elektronischer Signaturen, Siegel oder Zeitstempel lässt sich die Unversehrtheit des Scanprodukts ab Signierung nachweisen. Problematisch bleibt aber die Einrede der Fälschung des Ursprungsdokuments [RFJW08, S. 92]. Dieses auszugleichen ist Aufgabe des § 371b ZPO.

Spezifische Beweisregeln für die meisten ersetzend gescannten Dokumente bestehen nicht. Damit bleibt eine beweisrechtliche Unsicherheit hinsichtlich der Echtheit des Originaldokuments. Durch einen Transfervermerk kann die Unsicherheit hinsichtlich des Scan-Prozesses vermindert werden. Die Verwendung qualifizierter elektronischer Signaturen, qualifizierter elektronischer Siegel oder qualifizierter elektronischer Zeitstempel können Authentizität und Integrität des Scanprodukts und des Transfervermerks nachweisen. Durch die einschlägigen allgemeinen Beweisregeln des § 371a Abs. 1 und 3 ZPO sowie der Art. 35 Abs. 2 und 41 Abs. 2 eIDAS-VO kann eine ausreichende Beweissicherheit erzeugt werden.

Die Simulationsstudie „Ersetzendes Scannen“ hat gezeigt, dass auch mit gescannten Dokumenten Beweis geführt werden kann. In dieser wurden 2013 in Nürnberg in 14 simulierten Gerichtsprozessen vor einem echten Amtsrichter und einem echten Finanzrichter unter Beteiligung mehrerer echter Rechtsanwälte über ersetzend gescannte Dokumente als Beweisgegenstand verhandelt [RoNe14a]. In diesen erleichterten zwar die Beweisregeln der Zivilprozessordnung die Beweisführung, für diese spielten aber auch bestimmte Sachverhaltsaspekte eine wichtige Rolle, wie etwa mögliche Motive, Gelegenheiten und Kenntnisse für eine Fälschung von Dokumenten oder der Zeitpunkt oder der Zeitraum möglicher Manipulationen oder Sicherungen. Dokumente genossen vor Gericht generell mehr Vertrauen, wenn sie nicht durch den Beweisführer selbst gesichert wurden, sondern von einer dritten Person, zum Beispiel einer Behörde, einem externen Dienstleister oder einem Steuerberater, dem ein Manipulationsinteresse fehlt. Als vorrangiges Mittel zur Bestätigung des Scan-Zeitpunkts und zur Sicherung des Scan-Produkts hat sich ein Zeitstempel erwiesen. Wird die Zeit durch eine unabhängige, nicht-kompromittierbare Zeitquelle bestätigt, hat dies einen hohen Beweiswert, wohingegen die Systemzeit des Computers als stets reproduzierbar und daher als wenig aussagekräftig angesehen wurde. Die Simulationsstudie hat vor allem gezeigt, dass der Beweiswert

[121] Begründung zum Gesetzesentwurf zu § 7 EGovG, BT-Drs. 17/11473, S. 31.

erhöht wird, wenn die Empfehlungen der TR-RESISCAN eingehalten und dies durch Zertifizierung oder Transfervermerk[122] nachgewiesen werden kann [RoNe14a, S. 41 ff.], [RoNe14b, S. 891].

[122] *VG Wiesbaden*, Urteil vom 26.9.2014, Az. 6 K 691/14.WI.A, Rn. 19: Der signierte Transfervermerk „dient als Nachweis für einen ordnungsgemäßen Scanvorganmg".

Glossar

Authentifizierung	Bei der „Authentifizierung“ wird eine „Behauptung“ über eine elektronische Identität geprüft. Hierbei besteht eine „Behauptung“ aus mindestens einem Identitätsattribut (z. B. dem Namen des Kommunikationspartners).
Authentizität	Unter der „Authentizität“ von Daten versteht man, dass die Quelle der Daten eindeutig bestimmbar ist.
Bildliche Übereinstimmung	Von einer „bildlichen Übereinstimmung“ zwischen einem Scanprodukt und einem Original spricht man, wenn das Scanprodukt ein im Rahmen der gewählten Auflösung identisches Abbild des Originals ist.
Ersetzendes Scannen	Wird nach dem „Scannen“ das papiergebundene Original vernichtet, so spricht man vom „ersetzenden Scannen“.
Inhaltliche Übereinstimmung	Von einer „inhaltlichen Übereinstimmung“ zwischen einem Scanprodukt und einem Original spricht man, wenn das Scanprodukt und das Original in den wesentlichen Inhaltsdaten übereinstimmen, nicht aber unbedingt in der visuellen Darstellung.
Integrität	„Integrität“ bedeutet, dass die Daten oder Systeme nicht verändert wurden. Bei einem wirksamen Integritätsschutz werden zudem zumindest Veränderungen erkannt.
IT-System	Der Begriff „IT-System“ beschreibt ein aus Hardware und Software bestehendes System zur Informationsverarbeitung.
Lesbarkeit	Lesbarkeit bedeutet, dass die in den Daten enthaltenen Informationen erkannt werden können.[123]
Löschbarkeit	Unter Löschen von Daten ist das Unkenntlichmachen der gespeicherten Daten zu verstehen (§ 3 Abs. 4 Satz 2 Nr. 5 BDSG). Dies ist gegeben, wenn die Daten unwiderruflich so behandelt worden sind, dass eigene Informationen nicht aus gespeicherten Daten gewonnen werden können, wenn also der Rückgriff auf diese Daten nicht mehr möglich ist [Simi11, § 3 BDSG, Rn. 180].
Nachvollziehbarkeit	Unter der „Nachvollziehbarkeit“ eines Vorgangs versteht man, dass alle wesentlichen Schritte des

[123] Ein elektronisches Dokument ist nur dann lesbar, wenn die notwendige Hard- und Software die Daten verarbeiten, ihre Informationen interpretieren und dem menschlichen Betrachter in lesbarer Weise präsentieren kann.

	Vorgangs von einer unabhängigen Stelle nachgezeichnet werden können.
Scannen	„Scannen“ bezeichnet das elektronische Erfassen von Papierdokumenten mit dem Ziel der elektronischen Weiterverarbeitung und Aufbewahrung des hierbei entstehenden elektronischen Abbildes (Scanprodukt).
Sicherungsdaten	„Sicherungsdaten“ sind Datenobjekte, die dem Schutz der Integrität und ggf. Authentizität anderer Datenobjekte dienen. Dies umfasst insbesondere elektronische Signaturen, Zeitstempel, Zertifikate, Sperrinformationen und Evidence Records (vgl. „Credential“ in [BSI-TR03125]).
Sicherungsmittel	Unter dem Begriff „Sicherungsmittel“ werden in dieser Technischen Richtlinie Sicherungsdaten oder Sicherungssysteme verstanden.
Sicherungssysteme	„Sicherungssysteme“ sind IT-Systeme und/oder Anwendungen, die dem Schutz der Integrität und ggf. Authentizität anderer Datenobjekte dienen.
Transfervermerk	Darunter versteht man ein softwaretechnisches Hilfsmittel. Es beinhaltet Informationen zum Scanprozess und zum Original. Damit kann es die Beurteilung der Integrität und Authentizität des Originals durch den Betrachter unterstützen und den Beweiswert des Scanprodukts verbessern.
Verfügbarkeit	Die „Verfügbarkeit“ von Daten, Diensten, IT-Systemen, IT-Anwendungen oder IT-Netzen ist vorhanden, wenn diese den Benutzern innerhalb akzeptabler Wartezeiten in der benötigten Form zur Verfügung stehen.
Verkehrsfähigkeit	„Verkehrsfähigkeit“ bezeichnet die Möglichkeit, Dokumente und Akten von einem System zu einem anderen übertragen zu können, bei der die „Qualität“ des Dokuments sowie seine Integrität und Authentizität nachweisbar bleiben.[124]
Vertraulichkeit	„Vertraulichkeit“ ist die Verhinderung einer unbefugten Kenntnisnahme.
Vollständigkeit	„Vollständigkeit“ bedeutet, dass der gegenseitige Bezug mehrerer aufgrund eines inneren Zusammenhangs zusammengehörigen Datenobjekte sichergestellt ist.

Tabelle 14: Glossar

[124] Es sei angemerkt, dass die Verkehrsfähigkeit von kryptographisch gesicherten Daten nur bei Verwendung von allgemein anerkannten (z.B. internationalen) Standards und interoperablen Systemen gewährleistet werden kann.

Literaturverzeichnis

[ADBV16] ADV- Arbeitsgemeinschaft, Bundesversicherungsamt (Hrsg.), *Leitfaden Elektronische Kommunikation und Langzeitspeicherung elektronischer Daten*, Version 4.1, Düsseldorf/Bonn, Stand 22.4.2016, https://www.bundesversicherungsamt.de/fileadmin/redaktion/PDK/2016-04-22_Leitfaden_Version4.1.pdf.

[AgElVa11] Arbeitsgruppe Elektronische Verwaltungsakte: *Anforderungen der Verwaltungsgerichtsbarkeit an die Führung elektronischer Verwaltungsakten – eine Orientierungshilfe*, JurPC Web-Dok. 66/2011.

[AWV16] Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V., Muster-Verfahrensdokumentation zur Belegablage, Version 1.0 vom 19.10.2015, http://www.awv-net.de/upload/pdf/Belegablage_V1_20151026.pdf .

[BSDS14] Bundessteuerberaterkammer, Deutscher Steuerberaterverband e.V., Muster Verfahrensdokumentation zur Digitalisierung und elektronischen Aufbewahrung von Belegen inkl. Vernichtung der Papierbelege, Stand März 2014, http://www.dstv.de/download/gemeinsame-verfahrensbeschreibung .

[BaHo18] A. Baumbach, K. J. Hopt, *Handelsgesetzbuch, Kommentar*, 38. Auflage, München 2018.

[BaRo12] J. Bader, M. Ronellenfisch, *Verwaltungsverfahrensgesetz*, *Beck'scher Online-Kommentar,* 17. Edition, München 2012.

[Bie12] M. Biewald, *Externe Dienstleister im Krankenhaus und ärztliche Schweigepflicht – eine rechtliche Unsicherheit*, Datenschutz und Datensicherheit (DuD) 2011, S. 867-869.

[BfDI22] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Tätigkeitsbericht zum Datenschutz für die Jahre 2007 und 2008 (22. Tätigkeitsbericht),* https://www.bfdi.bund.de/DE/Infothek/Taetigkeitsberichte/taetigkeitsberichte-node.html .

[BfDI23] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Tätigkeitsbericht zum Datenschutz für die Jahre 2009 und 2010 (23. Tätigkeitsbericht),* https://www.bfdi.bund.de/DE/Infothek/Taetigkeitsberichte/taetigkeitsberichte-node.html .

[BHR+14] R. Bauer, D. Heckmann, K. Ruge, M. Schallbruch, S. Schulz, Verwaltungsverfahrensgesetz und E-Government, 2. Auflage, Wiesbaden 2014.

[BLAH12] A. Baumbach, W. Lauterbach, J. Albers, P. Hartmann, Zivilprozessordnung, Kommentar, 70. Auflage, München 2012.

[BSI-Glossar] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Glossar und Begriffsdefinitionen*, https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/ElektronischeSignatur/Glossar/glossar_node.html

[BSI-GSK] Bundesamt für Sicherheit in der Informationstechnik (BSI): *IT-Grundschutz- Kataloge*, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html.

[BSI-TR03125] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR)*, Technische Richtlinie (TR) des BSI Nr. 03125, Version 1.2.1, 2018, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_V1_2_1.pdf?__blob=publicationFile&v=2

[BSI-TR03138] Bundesamt für Sicherheit in der Informationstechnik (BSI), *RESISCAN – Ersetzendes Scannen*, Technische Richtlinie (TR) des BSI Nr. 03138, Version 1.4.1, 2020.

[BSI-TR03107-1] Bundesamts für Sicherheit in der Informationstechnik (BSI), *Elektronische Identitäten und Vertrauensdienste*, Technische Richtlinie (TR) des BSI Nr. -03107-1, Version 1.1, 31.10.2016.

[BT-Drs.] Bundestagsdrucksachen, abrufbar unter http://www.bundestag.de/dokumente/drucksachen/index.html

[BR-Drs.] Bundesratsdrucksachen, abrufbar unter https://www.bundesrat.de/DE/dokumente/dokumente-node.html.

[Bund16] Bundesregierung, *Bericht zur Verzichtbarkeit der Anordnungen der Schriftform und des persönlichen Erscheinens im Verwaltungsrecht des Bundes*, BT-Drs. 18/9177.

[CCCE10] Competence Center für die Elektronische Signatur im Gesundheitswesen e.V. (Hrsg.), Empfehlungen für den Einsatz elektronischer Signaturen und Zeitstempel in Versorgungseinrichtungen des Gesundheitswesens (Berichte aus der Medizinischen Informatik und Bioinformatik), Herzogenrath 2010.

[DiSc08] M. Diller, F. Schuster, *Rechtsfragen der elektronischen Personalakte*, in: Der Betrieb (DB) 2008, S. 928-932.

[EBJS14] C. T. Ebenroth, K. Boujong, D. Joost, L. Strohn, *Handelsgesetzbuch, Kommentar*, 3. Auflage, München 2014.

[Fisc06] S. Fischer-Dieskau, *Das elektronisch signierte Dokument als Mittel zur Beweissicherung, Anforderungen an seine langfristige Aufbewahrung*, Baden-Baden 2006.

[Fisc17] T. Fischer, *Strafgesetzbuch, Kommentar, 64*. Auflage, München 2017.

[GUKK12] K. Gohl, U. Ungerer, C.-G. Kalbfell, G. Krauskopf, *Landeskrankenhausgesetz Baden-Württemberg, Kommentar*, Loseblatt, Januar 2012, Wiesbaden.

[HaBi93] V. Hammer, J. Bizer, *Beweiswert elektronisch signierter Dokumente,* in: Datenschutz und Datensicherheit (DuD) 1993, S. 689-693.

[HuKa17] S. Huster, M. Kaltenborn, Krankenhausrecht, 2. Auflage, München 2017.

[IDW RS FAIT 3] Institut der Wirtschaftsprüfer, *Stellungnahme zur Rechnungslegung: Grundsätze ordnungsgemäßer Buchführung beim Einsatz elektronischer Archivierungsverfahren*, 11.7.2006.

[IT-P15] IT-Planungsrat, *Handreichung mit Empfehlungen des IT-Planungsrats für die Zuordnung von Vertrauensniveaus in der Kommunikation zwischen Verwaltung und Bürgerinnen und Bürgern bzw. der Wirtschaft*, Berlin 13. März 2015.

[Jand15] S. Jandt, *Beweissicherheit im elektronischen Rechtsverkehr*, Neue Juristische Wochenschrift (NJW) 2015, S. 1205-1211.

[JaMD15] S. Jandt, T. Michalek, K. Dietrich, *Wie hoch ist der (Beweis-)Wert digitaler Dokumente*?, Datenschutz und Datensicherheit (DuD) 2015, 687-692.

[JaRo11] S. Jandt, A. Roßnagel, *Qualitätssicherung im Krankenhaus*, in: Medizinrecht (MedR) 2011, 140-145.

[JaRW11a] S. Jandt, A. Roßnagel, D. Wilke, *Krankenhausinformationssysteme im Gesundheitskonzern*, in: Recht der Datenverarbeitung (RDV) 2011, 222-228.

[JaRW11b] S. Jandt, A. Roßnagel, D. Wilke, *Outsourcing der Verarbeitung von Patientendaten – Fragen des Daten- und Geheimnisschutzes*, in: Neue Zeitschrift für Sozialrecht (NZS) 2011, 641-646.

[JaWi09] S. Jandt, D. Wilke, *Gesetzliche Anforderungen an das ersetzende Scannen von Papierdokumenten*, Kommunikation und Recht (K&R) 2009, 96-100.

[KGSt17] Landkreis Breisgau-Hochschwarzwald, KGSt, VITAKO (Hrsg.), *Leitlinie zum ersetzenden Scannen in Kommunen nach TR RESISCAN*, Stand April 2017,

https://www.vitako.de/Publikationen/Leitlinie%20zum%20ersetzenden%20Scannen%20in%20Kommunen%20nach%20TR%20RESISCAN.pdf .

[KoRa16] F. Kopp, M. Ramsauer, *Verwaltungsverfahrensgesetz, Kommentar,* 17. Auflage, München 2016.

[KoKR17] I. Koller, P. Kindler, W. H. Roth, W. Morck, *Handelsgesetzbuch, Kommentar,* 8. Auflage, München 2017.

[Klei16] F. Klein, *Abgabenordnung, Kommentar,* 13. Auflage, München 2016.

[KüBu17] J. Kühling, B. Buchner (Hrsg.), *Datenschutz-Grundverordnung-Kommentar*, München 2017.

[LaKe10] A. Laufs, B.-R. Kern, *Handbuch des Arztrechts*, 4. Auflage, München 2010.

[LaKü14] K. Lackner, K. Kühl, *Strafgesetzbuch, Kommentar,* 28. Auflage, München 2014.

[LüSp17] H. Lüthge, N. Springer, *Vollständige Digitalisierung von Personalakten: Rechtslage, Risiken und Sicherheitsvorkehrungen bei der Vernichtung von Unterlagen mit Schriftformerfordernis*, Betriebsberater (BB) 2017,S. 1397 – 1404.

[Musi17] H. J. Musielak, *Zivilprozessordnung, Kommentar*, 14. Auflage, München 2017.

[MüKo16] M. Henssler, W. Krüger (Hrsg.), *Münchener Kommentar zum Bürgerlichen Gesetzbuch*, Band 4, Schuldrecht – Besonderer Teil, 7. Auflage, München 2016.

[PaHo16] N. Paland, J. Holland, Das Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen , NZS 2016, 247

[PaKo14] A. Pahlke, U. Koenig, *Abgabeordnung, Kommentar,* 3. Auflage, München 2014.

[PoWo12] H. Posser, H. A. Wolff, *Verwaltungsgerichtsordnung, Beck'scher Online-Kommentar*, 23. Edition, München 2012.

[QuZu14] M. Quaas, R. Zuck, Clemens, T., *Medizinrecht*, 3. Auflage, München 2014.

[RWWO09] R. Richardi, H. Wißmann, O. Wlotzke, H. Oetker, *Münchener Handbuch zum Arbeitsrecht*, 3. Auflage, München 2009.

[RoFJ07] A. Roßnagel, S. Fischer-Dieskau, S. Jandt, *Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente*. Herausgegeben im Auftrag des Bundesministeriums für Wirtschaft und Technologie, Nr. 564, Berlin August 2007.

[RoJa08] A. Roßnagel, S. Jandt, *Handlungsleitfaden zum Scannen von Papierdokumenten.* Herausgegeben im Auftrag des Bundesministeriums für Wirtschaft und Technologie, Nr. 571, Berlin April 2008.

[RoPf03] A. Roßnagel, A. Pfitzmann, *Der Beweiswert von E-Mail,* in: Neue Juristische Wochenschrift (NJW) 2003, S. 1209-1214.

[Roßn03] A. Roßnagel: *Handbuch Datenschutzrecht – Die neuen Grundlagen für Wirtschaft und Verwaltung*, Beck 2003.

[Roßn03a] A. Roßnagel, *Die fortgeschrittene elektronische Signatur*, in: Multimedia und Recht (MMR) 2003, S. 164-170.

[Roßn11] A. Roßnagel, *Rechtsverbindliche Telekooperation*, in: Schulte/Schröder (Hrsg.), Handbuch des Technikrechts, 2. Auflage, Berlin Heidelberg 2011.

[Roßn13a] A. Roßnagel, *Recht der Telemediendienste, Kommentar,* München 2013.

[Roßn13b] A. Roßnagel, *Auf dem Weg zur elektronischen Verwaltung – das E-Government-Gesetz*, in: Neue Juristische Wochenschrift (NJW) 2013, S. 2710-2716.

[Roßn14] A. Roßnagel, *Neue Regeln für sichere elektronische Transaktionen – Die EU- Verordnung über elektronische Identifizierung und Vertrauensdienste*, Neue Juristische Wochenschrift (NJW) 2014, S. 3686-3692.

[Roßn15] A. Roßnagel, *Der Anwendungsvorrang der eIDAS-Verordnung. Welche Regelungen des deutschen Rechts sind weiterhin für elektronische Signaturen anwendbar?*, in: Multimedia und Recht (MMR) 2015, S. 359-364.

[Roßn16a] A. Roßnagel, *Das Recht der Vertrauensdienste – Die eIDAS-Verordnung in der deutschen Rechtsordnung*, Baden-Baden 2016.

[Roßn16b] A. Roßnagel, *Beweiswirkungen elektronischer Vertrauensdienste*. Neue Regelungen durch die eIDAS-Verordnung der Europäischen Union, in: Multimedia und Recht (MMR) 2016, S. 647-652.

[Roßn18] A. Roßnagel (Hrsg.), *Europäisches Datenschutzrecht. Die Datenschutz-Grundverordnung und das angepasste deutsche Datenschutzrecht*, Baden-Baden 2018.

[RoNe14a] A. Roßnagel, M. Nebel, *Simulationsstudie „Ersetzendes Scannen" - Ergebnisse,* Nürnberg 2014.

[RoNe14b] A. Roßnagel, *Beweisführung mittels ersetzend gescannter Dokumente*, in: Neue Juristische Wochenschrift (NJW) 2014, S. 886-891.

[RoSc06] A. Roßnagel/P. Schmücker (Hrsg.), *Beweiskräftige elektronische Archivierung – Bieten elektronische Signaturen Rechtssicherheit?*, Bonn 2006.

[RoSW09] A. Roßnagel/A. U. Schmidt/D. Wilke (Hrsg.), *Rechtssichere Transformation signierter Dokumente – Anforderungen, Konzepte und Umsetzung*, Baden-Baden 2009.

[RoWi06] A. Roßnagel, D. Wilke, *Die rechtliche Bedeutung gescannter Dokumente,* in: Neue Juristische Wochenschrift (NJW) 2006, S. 2145-2150.

[RFJK07] A. Roßnagel, S. Fischer-Dieskau, S. Jandt, M. Knopp, *Langfristige Aufbewahrung elektronischer Dokumente, Anforderungen und Trends*, Baden-Baden 2007.

[RFJW08] A. Roßnagel, S. Fischer-Dieskau, S. Jandt, D. Wilke, *Scannen von Papierdokumenten – Anforderungen, Trends und Empfehlungen*, Baden-Baden 2008.

[Schu14] R. Schulze u. a., *Bürgerliches Gesetzbuch, Kommentar,* 8. Auflage, Baden-Baden 2014.

[ScSc14] A. Schönke, H. Schröder, *Strafgesetzbuch, Kommentar,* 29. Auflage, München 2014.

[Simi14] S. Simitis, *Bundesdatenschutzgesetz, Kommentar*, 8. Auflage, Baden-Baden 2014.

[StBS14] P. Stelkens, H. J. Bonk, M. Sachs, *Verwaltungsverfahrensgesetz, Kommentar*, 8. Auflage, München 2014.

[Wilk11] D. Wilke, *Die rechtssichere Transformation von Dokumenten – Rechtliche Anforderungen an die Technikgestaltung und rechtlicher Anpassungsbedarf*, Baden-Baden 2011.

[Zöll16] R. Zöller, *Zivilprozessordnung, Kommentar,* 31. Auflage, Köln 2016.