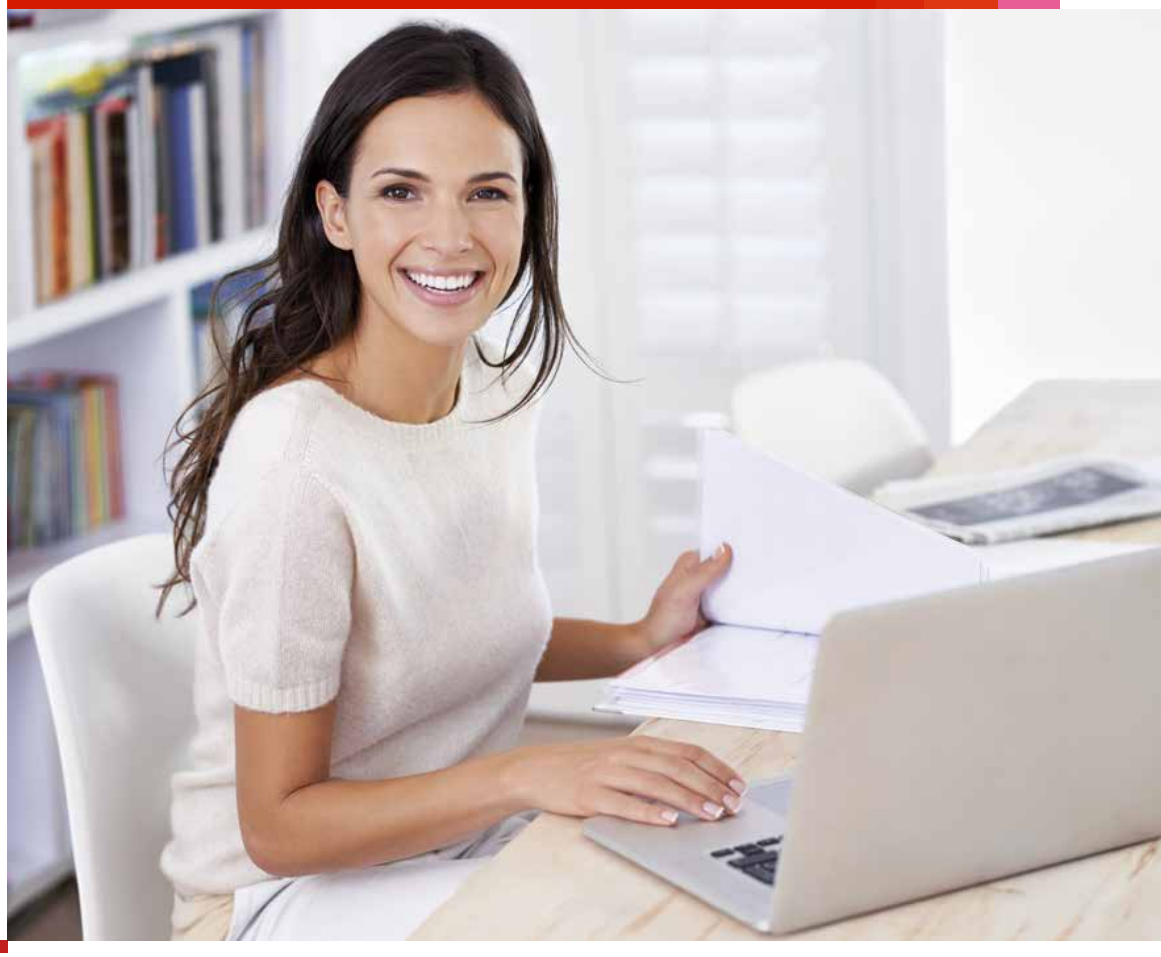
TR RESISCAN: Beschleuniger oder Bremse für E-Government?

Positionspapier zur BSI TR 03138 „TR-RESISCAN 1.0“



Zöller & Partner

pwc

Inhaltsverzeichnis

A Einleitung

Die Digitalisierung schreitet im modernen Wirtschaftsleben, in der Gesellschaft und in der Verwaltung in hohem Tempo voran. Arbeitsabläufe, Kommunikationsformen und ganze Geschäftsmodelle unterliegen derzeit einem fundamentalen Wandel.

Die öffentliche Seite versucht mit einer Vielzahl von Initiativen und Maßnahmen sowie infrastrukturellen Programmen, diese Entwicklungen zu begleiten und zu befördern. Dazu gehört, den regulatorischen Rahmen zeitgemäß anzupassen sowie um neue, richtungsgebende Aspekte zu erweitern. Als Beispiel sei das Grundsatzpapier *Digitale Agenda* der gegenwärtigen Bundesregierung genannt. Die öffentliche Verwaltung muss sich aber auch selbst den neuen Herausforderungen stellen und viele tradierte, häufig standort- und papiergebundene Arbeitsformen überdenken. Bei der Digitalisierung der eigenen Organisation steht sie, betrachtet man die Umsetzung in vielen Behörden, nicht an der Spitze der Entwicklung. Dies liegt nicht zuletzt an besonderen rechtlichen Bestimmungen, denen ihr Handeln unterworfen ist. Viele Behördenleiterinnen und Behördenleiter sind unsicher, ob die ganzheitliche Umstellung vom papiergebundenen auf das elektronische Arbeiten ausreichend rechtlich fundiert ist. Zugleich spielen Finanzierungsfragen und organisatorische Beharrungskräfte sowie Ungewissheiten bezüglich der technischen Umsetzbarkeit neuer Arbeitsweisen vielerorts eine wichtige Rolle.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat vor diesem Hintergrund Handlungsbedarf erkannt und sich einem Aspekt gewidmet, den es als eine Hürde auf dem Weg zu vermehrtem elektronischem Arbeiten sieht: das Scannen. Die hierzu eigens vom BSI erstellte und 2013 veröffentlichte *Technische Richtlinie 03138 Ersetzendes Scannen* (kurz: TR RESISCAN oder BSI TR 03138) erhebt den Anspruch, „Anwendern in Justiz, Verwaltung, Wirtschaft und Gesundheitswesen als Handlungsleitfaden und Entscheidungshilfe zu dienen, wenn es darum geht, Papierdokumente nicht nur einzuscannen, sondern nach Erstellung des Scanproduktes auch zu vernichten“[1]. Auch für den Fall, dass Post noch in Papierform eingeht, soll also eine Brücke zu elektronischen Arbeitsprozessen geschlagen werden. Gleiches gilt für die Digitalisierung bereits vorhandenen papierbasierten Schriftguts.

Diese Absicht entspricht dem Ziel, möglichst auf eine ineffiziente Hybridaktenführung zu verzichten und das Scannen sowie vor allem das Vernichten der gescannten Papierunterlagen rechtlich abzusichern.

[1] BSI TR 03138, S. 6.

Obwohl die Richtlinie selbst einen „lediglich empfehlenden Charakter“ besitzt, beabsichtigt das BSI selbstverständlich durchaus, mit ihr eine „Referenz“ vorzulegen, die wiederum von rechtlichen Vorgaben aufgegriffen werden kann, sodass auch die TR RESISCAN rechtliche Bindekraft erhielte.[2] Inzwischen hat der Bund mit dem sogenannten E-Government-Gesetz (EGovG) einen rechtlichen Rahmen geschaffen, um in den Bundesbehörden elektronische Aktenführung flächendeckend einzuführen. Viele Bundesländer ziehen nach oder haben bereits analoge E-Government-Gesetze. Bis 2020 soll die „E-Akte“ jedenfalls beim Bund Wirklichkeit werden. Vorgesehen sind in diesem Zusammenhang das Übertragen von Papierdokumenten in ein elektronisches Format und die Vernichtung der Originale. In der 2014 vom Bundesministerium des Innern (BMI) vorgelegten Kommentierung des Gesetzes wird dabei explizit auf die TR RESISCAN verwiesen. Sie sei ein Beispiel dafür, wie sich Dokumente „nach dem Stand der Technik“ sicher scannen ließen, also im Ergebnis das Scanprodukt dem Original entspreche.[3]

Da die TR RESISCAN zukünftig also möglicherweise nicht mehr nur ein bloßer Handlungsleitfaden oder eine Entscheidungshilfe sein wird und stärkere normative Wirkung entfalten könnte, lohnt sich der erneute Blick auf die Richtlinie. Gelingt es mit ihr, die rechtlichen Unsicherheiten aus dem Weg zu räumen? Verhilft sie der E-Akte und elektronischem Arbeiten ohne Hybridakten zum Durchbruch?

In unserem Positionspapier kommen wir mit Blick auf zahlreiche Facetten der TR RESISCAN leider zu dem Schluss, dass die Richtlinie ihren eigenen Anspruch nicht einlöst und in der gegenwärtigen Form auch nicht einlösen kann. Entscheidend sind folgende Punkte:

- Die TR RESISCAN besitzt nicht den Normencharakter, der es erlauben würde, Rechtssicherheit herzustellen (Kapitel C 1). Implizit erhebt sie zwar diesen Anspruch, aber sie kann keine grundsätzliche Klärung auf einer höheren Stufe der Normenpyramide ersetzen. Insofern vergrößert sie als weiteres Element den Kreis einschlägiger Gesetze, Erlasse, Ordnungen, Handreichungen usw., setzt aber keine andere außer Kraft. Da die TR RESISCAN zudem auf einer Synopsis bestehender Vorgaben in unterschiedlichen Anwendungsbereichen (Justiz, Verwaltung, Gesundheit, „Personalakten“ usw.) aufbaut und daraus den Kanon der eigenen „Empfehlungen“ schafft, importiert sie im Ergebnis Vorgaben in Bereiche, in deren Rechtskreis diese heute rechtlich gar nicht notwendig sind und die auf bewährten Erfassungs- und Aufbewahrungsverfahren beruhen (z. B. Ordnungsmäßigkeit nach den Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme [GoBS] bzw. nach den Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff [GoBD]). Besonders deutlich wird dies etwa beim Einsatz kryptografischer Elemente, der in der TR RESISCAN insgesamt eine wichtige Rolle spielt. Jedoch schaffen selbst diese Elemente keine Rechtssicherheit, da sie den Charakter der Scandokumente als „Augenscheinobjekte“ vor Gericht nicht zwangsläufig ändern und die richterliche Unabhängigkeit bei der Beweisaufnahme nicht schmälern.

[2] Vgl. BSI TR 03138, S. 6.
[3] Vgl. BMI, Minikommentar zum E-Government-Gesetz, Erläuterungen zu EGovG Bund § 7 Satz 2, S. 25.

- Die TR RESISCAN legt ihren Fokus allein auf das Herstellen eines Scanprodukts und darauf, dass dieses dem Original entspricht (Kapitel C 2.1). Sie beleuchtet hierzu den Scanprozess in vielerlei Hinsicht: technisch, organisatorisch und personell bis hin zu Qualifikationserfordernissen der Menschen am Scanner. Mit Blick auf die Rechtssicherheit bleiben dabei indes der Übertragungsweg (Versand/Posteingang) und Fragen der Aufbewahrung, des Zugriffs usw. sowie der entsprechenden technischen Umsetzung ausgeklammert. Im Streitfall erscheint dies im Vergleich zum Scanprozess selbst ein ungleich höheres Risiko zu bergen. Auch wenn das Scannen umfassend behandelt wird, bleibt die TR RESISCAN aus Sicht der Anwender zwangsläufig inkrementell.
- Als weiterer Aspekt kommt hinzu, dass die TR RESISCAN den Anspruch der Praxistauglichkeit aus Anwendersicht kaum einlöst (Kapitel C 2). Die Richtlinie selbst ist komplex aufgebaut und teilweise schwer verständlich, und sie beschreibt das Scannen in sehr differenzierten, bisweilen kleinteiligen und dann auch wieder an vielen Stellen generischen Gliederungspunkten. Dieser hohe Detaillierungsgrad überfordert sicherlich viele Anwender, die für die Einrichtung des Scanverfahrens keine zusätzliche Expertise in Anspruch nehmen können, insbesondere mittelständische und kleine Unternehmen bzw. mittlere und kleine Körperschaften des öffentlichen Rechts. Auch in technischer Hinsicht steigt die TR RESISCAN bisweilen auf ein äußerst detailliertes Niveau hinab (Kapitel C 3), wie zum Beispiel bei den Ausführungen zur Manipulationssicherheit des Scan-Cache. Im Ergebnis könnte eine unbeabsichtigte Wirkung der Richtlinie sogar darin liegen, dass Anwender sie weniger als Hilfe erkennen, sondern vielmehr abgeschreckt werden und entweder einen professionellen Dienstleister beauftragen – oder eben doch bei der Hybridaktenführung bleiben.
- Für den letztgenannten Punkt gibt es auch Gründe, die im Ansatz der Richtlinie und ihrer Handhabbarkeit liegen (Kapitel C 3). Eine entscheidende Rolle spielen trotz aller Hilfestellungen, die auch an dieser Stelle recht komplex ausfallen, die eigenen Einschätzungen des Schutzbedarfs der zu scannenden Dokumente. Da es mithin weder eine verlässliche Negativ- noch eine Positivliste gibt, bleiben Einordnungen zwangsläufig im Vagen, sodass die Anwender doch wieder in direkter Verantwortung stehen, mit Rechtsrisiken umgehen zu müssen. Vergrößert werden diese dadurch, dass die aufgezeigten Klassifizierungen derart komplex sind, dass sie in vielen Organisationen nicht nur das Scanpersonal überfordern dürften.

Wir nehmen die TR RESISCAN aus diesen Gründen zum Anlass, für eine übergeordnete Regelung des ersetzenden Scannens zu plädieren. Diese wäre indes Teil eines grundsätzlicheren Konzepts für die Ordnungsmäßigkeit elektronischer Aktenführung entlang des gesamten Dokumentenlebenszyklus, nicht nur des Scannens – und zugleich deutlich schlanker (Kapitel C 4).

Bis dahin läuft die TR RESISCAN angesichts der vorgestellten Merkmale Gefahr, im besten Falle rein deklaratorisch von Herstellern und Scandienstleistern genutzt zu werden bzw. einen eigenen Markt für Konformitätsprüfungen entlang ihrer Taxonomien zu schaffen. Bei den Anwendern jedoch, bei denen sie eigentlich für den Durchbruch moderner Arbeitsformen sorgen sollte, riskiert sie in der jetzigen Form, ignoriert zu werden oder sogar zu verhindern, dass elektronische und Papierakten nicht mehr parallel aufbewahrt werden. Angesichts der Komplexität in der Umsetzung, der ungeklärten inhaltlichen Bewertungen von Dokumenten und der schlicht weiterhin ungeklärten rechtlichen Situation dürften viele Organisationen ein ersetzendes Scannen zunächst aufschieben.

B Aktuelle Situation

Die Vorteile elektronischer Workflows mit Dokumentenmanagement- und Vorgangsbearbeitungssystemen (DMS/VBS) gegenüber tradiertem, papierbasiertem Arbeiten liegen auf der Hand: Arbeiten können standortunabhängig verteilt und erledigt werden, Vorgänge und ganze Bestände lassen sich mit Stichwortsuchen und Indizierungen erschließen, eine einfache „Veraktung" aus Fachanwendungen ist ohne Weiteres möglich und durch die Integration von Telefonie und Applikationen (CTI) sind DMS und VBS multikanalfähig. Hinzu kommt, dass elektronische Dokumente Papierakten auch in puncto Verfügbarkeit und Platzbedarf eindeutig überlegen sind – also zwei wesentlichen Kostentreibern der herkömmlichen Schriftgutverwaltung. Elektronische Lösungen erlauben es ferner, übergreifende Informations- und Wissensstrukturen innerhalb einer Organisation aufzubauen. Dies ist gerade in der öffentlichen Verwaltung schon mit Blick auf die demografische Situation und die Sicherung von Wissen ganzer nun zur Pensionierung anstehender Alterskohorten von außerordentlicher Bedeutung.

Ihr volles Potenzial entfaltet die elektronische Akte mit der konsequenten Ablösung der Papierakte. Dazu gehört, dass man vorliegende Papierdokumente scannt, in die elektronische Akte überführt und das Original vernichtet (soweit möglich), ohne Defizite bei der Beweiskraft bzw. der Gerichtsfestigkeit dieser Akten befürchten zu müssen. Folglich bedarf es Regelungen für das ordnungsgemäße Führen der elektronischen Akte.

Im privatwirtschaftlichen Bereich sind die Regelungen zur ordnungsgemäßen Speicherung von Daten national wie international sehr zahlreich. Für den Betrieb eines ordnungsgemäßen DMS gelten in Deutschland vor allem Regeln des kaufmännischen Rechts, das dem Privatrecht zuzuordnen ist. Insbesondere sind dies die Rechtsnormen des Handelsgesetzbuchs (HGB), der Abgabenordnung (AO) und der daraus abgeleiteten GoBS/GoBD. Bei diesen Rechtsnormen handelt es sich zwar um Regeln für den kaufmännischen bzw. steuerrechtlichen Bereich, jedoch gelten sie unmittelbar auch für DMS. Hier sind also die Voraussetzungen für einen ordnungsgemäßen Betrieb von Dokumentenmanagementlösungen sowie für die Datenspeicherung beschrieben. Daraus wurden vom Institut der Wirtschaftsprüfer in Deutschland (IDW) mit der IDW RS FAIT 3 sowie vom Verband Organisations- und Informationssysteme e. V. (VOI) mit den PK DML[4] Kriterienkataloge entwickelt, die aus den rechtlichen Vorgaben konkrete Prüfkriterien ableiten. Diese Kataloge präzisieren die Anforderungen an eine ordnungsgemäße elektronische Aktenführung im privatwirtschaftlichen Bereich. Hinzu treten spezifische Regelungen für besondere Dokumentarten (u. a. Urkunden) bzw. Anwendungsbereiche (z. B. Gesundheitswesen).

[4] Prüfkriterien für Dokumentenmanagementlösungen.

Für die öffentliche Verwaltung ist, wie bereits erwähnt, der 1. August 2013 ein besonderes Datum, da an diesem Tag das EGovG des Bundes in Kraft getreten ist, das unter anderem die Grundsätze der elektronischen Aktenführung und Regelungen zum ersetzenden Scannen im Geltungsbereich der Bundesverwaltung beinhaltet. Die Bundesbehörden werden weitgehend verpflichtet, die elektronische Akte bis 2020 als „führende" und alleinige Akte einzusetzen (§ 7 Abs. 2 EGovG). Schleswig-Holstein hatte als erstes Bundesland ein vergleichbares E-Government-Gesetz, das noch vor dem EGovG Bund in Kraft trat. Inzwischen sind weitere Länder gefolgt (z. B. Sachsen, Berlin), haben ein E-Government-Gesetz in Vorbereitung (u. a. Nordrhein-Westfalen, Saarland, Bayern) bzw. passen das jeweilige Verwaltungsverfahrensgesetz an (z. B. Brandenburg, Hessen, Mecklenburg-Vorpommern).

Eine offene Flanke bei diesen gesetzlichen Regelungen bleibt, was eine ordnungsgemäße elektronische Aktenführung beinhaltet. Explizit gefordert wird sie zum Beispiel im EGovG Bund, doch wird dort nicht konkretisiert, was mit dem Begriff gemeint ist. Grundsätzlich lässt sich zwar aus bekannten einschlägigen Normen, vom Grundgesetz bis hin zum Verwaltungsverfahrensgesetz, eine Reihe von Kriterien ableiten, die auch für Papierakten gelten. Doch eine konkrete materielle Definition, wie sie im privatwirtschaftlichen Bereich auch durch Wirtschaftsprüfungen zugrunde gelegt wird, gibt es noch nicht. Der vom BSI beschrittene Weg ist insofern grundsätzlich nachvollziehbar: Anforderungen (Sicherstellung der Integrität, Authentizität etc.) formulieren und sie in die digitale Welt übertragen. In der Art der Ausgestaltung können diese indes nicht den Anspruch erheben, die einzige Umsetzungsform darzustellen.

In den Behörden wiederum führt die Situation verständlicherweise zu Unsicherheiten und im Zweifel dazu, die Papierakte als führende Akte beizubehalten, ergänzt um die elektronische Akte. Durch redundante Ablagestrukturen bedingte Ineffizienzen bewirken vielerorts sogar, dass die Beschäftigten die Einführung der E-Akte ablehnen.

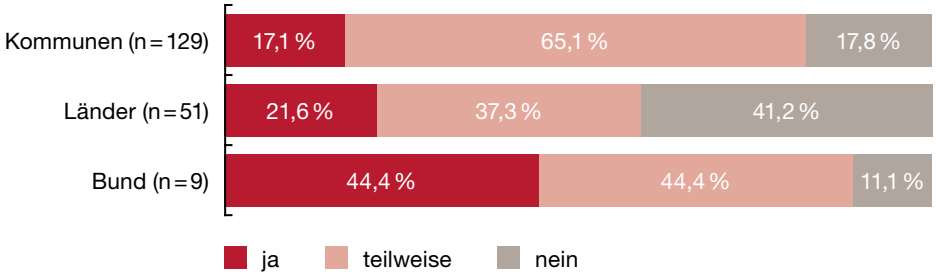
Bei der Einführung der E-Akte in der öffentlichen Verwaltung gibt es nach wie vor klaren Nachholbedarf. Rund 75 Prozent der Behörden (37 Prozent beim Bund, 81 Prozent in den Ländern, 79 Prozent in den Kommunen) geben an, bereits E-Akten zumindest in Teilbereichen einzusetzen.[5] Ein ersetzendes Scannen ist damit allerdings überwiegend nicht verbunden. In mehr als 80 Prozent der Verwaltungen, die die E-Akte bereits einsetzen, werden die Papierdokumente nach dem Scannen nicht oder nur zum Teil vernichtet und bleibt die Papierakte zumeist die führende Akte. Dies dürfte primär den Zweifeln hinsichtlich der Rechtmäßigkeit einer Vernichtung der Originale geschuldet sein.

Der vom BSI entdeckte Handlungsbedarf beim ersetzenden Scannen erscheint folglich mit Blick auf das Ziel einer weiteren Verbreitung der E-Akte dringend. Zweifel bleiben allerdings, ob die TR RESISCAN das geeignete Mittel ist.

[5] Vgl. Studie „E-Akte 2015 – Folgestudie von PwC und IMTB zur elektronischen Aktenführung in der öffentlichen Verwaltung – Einführungsstand, Ordnungsmäßigkeit und Handlungsempfehlungen", PwC und IMTB, 2015.

Folgende Abbildung verdeutlicht die aktuelle Situation in der öffentlichen Verwaltung:[5]

Werden die eingescannten, aktenrelevanten Papierdokumente vernichtet, nachdem sie der E-Akte zugeordnet wurden (ersetzendes Scannen)?



Verbindliche Fristen zur Aufbewahrung der Papieroriginale sind nur in 50 % der Behörden definiert, die ersetzend scannen.

Diese Aufbewahrungsfristen schwanken zwischen einer Woche und fünf Jahren.

In mehr als 80 % der Verwaltungen, die die Papierdokumente nach dem Scannen nicht vernichten, bleibt die Papierakte die führende Akte!

[5] Vgl. Studie „E-Akte 2015 – Folgestudie von PwC und IMTB zur elektronischen Aktenführung in der öffentlichen Verwaltung – Einführungsstand, Ordnungsmäßigkeit und Handlungsempfehlungen“, PwC und IMTB, 2015.

C Kritische Würdigung der TR RESISCAN

1 Anspruch der Rechtssicherheit

Schon der Titel der Richtlinie bringt ihre zentrale Zielsetzung zum Ausdruck: Die TR RESISCAN (**Re**chts**si**cheres **Scan**nen) soll „eine Steigerung der Rechtssicherheit im Bereich des ersetzenden Scannens“ herbeiführen. Sie richtet sich nicht nur an Bundesbehörden, sondern generell an alle „Anwender in Justiz, Verwaltung, Wirtschaft und Gesundheitswesen“.[6]

Der Anspruch, für Hersteller und Anwender die Rechtssicherheit zu erhöhen, zieht sich wie ein roter Faden durch die Richtlinie. Im Einzelnen lässt sich der gewählte Ansatz wie folgt zusammenfassen:

- Die TR RESISCAN wird als ein unterstützender Handlungsleitfaden verstanden, der empfehlenden, aber keinen bindenden Charakter hat. Entsprechend will die Richtlinie zwar die Rechtssicherheit erhöhen, kann aber nicht versprechen, sie wirklich zu geben.[7]
- Die TR RESISCAN ist gleichwohl eindeutig normativ aufgebaut. Sie stellt verschiedene Forderungen auf, unterteilt in KANN-, SOLL-, MUSS-Forderungen usw. Damit will sie deutlich machen, in welchen Fällen die Rechtssicherheit erhöht werden kann, und Handlungsanweisungen geben. Es geht darum, die Rechtsrisiken in einem umfangreichen Spektrum zu minimieren.
- Die Forderungen selbst leitet sie ab aus einer Zusammenschau einschlägiger allgemeiner Vorgaben zum rechtssicheren Dokumentenmanagement und benennt zugleich „beispielhaft“ besondere Vorgaben verschiedener Anwendungsbereiche (Gerichtsakten, Verwaltungsunterlagen, Sozialversicherungsunterlagen, medizinische Dokumentation, kaufmännische Buchführungsunterlagen, Besteuerungsunterlagen und Personalakten) sowie weitere Anforderungen.[8] Durch die Ableitung von Umsetzungserfordernissen zur Gewährleistung der ihrerseits abgeleiteten Kriterien einer ordnungsgemäßen Aktenführung (Integrität, Authentizität etc.) erstellt sie somit einen allgemeinen Kanon.[9] Aus der Klassifikation bestimmter Schutzbedarfe für Datenobjekte, IT-Systeme und Anwendungen sowie Kommunikationswege, die sich ihrerseits aus den fachlichen rechtlichen Anforderungen ergeben, resultiert gemäß Richtlinie eine ganze Liste von Anforderungen. Diese werden einer Bedrohungsanalyse gegenübergestellt und bedingen Sicherheitsmaßnahmen. Deutlich wird: Der Klassifikationsraum und die empfohlenen Maßnahmen sind sehr dezidiert und umfassend hergeleitet und gegliedert. In ihrer Mittelbarkeit entfernen sie sich indes von konkret einschlägigen Normen.[10] Der fachliche Schutzbedarf „MUSS […] von jedem Anwender der TR vor dem ersetzenden Scannen anhand der konkret verarbeiteten Dokumente individuell bestimmt werden“[11].

---

6 Vgl. BSI TR 03138, S. 6.
7 Vgl. BSI TR 03138, S. 6 f.
8 Vgl. BSI TR 03138 Anlage R: Unverbindliche rechtliche Hinweise und BSI TR 03138 Anlage A Ergebnis der Risikoanalyse, S. 15 ff.
9 Die TR RESISCAN leitet bestimmte „Sicherheitsziele“ ab (Integrität, Authentizität, Vollständigkeit, Nachvollziehbarkeit, Verfügbarkeit, Lesbarkeit, Verkehrsfähigkeit, Vertraulichkeit und Löschbarkeit).
10 Vgl. BSI TR 03138 Anlage A: Ergebnis der Risikoanalyse.
11 BSI TR 03138 Anlage A: Ergebnis der Risikoanalyse, S. 17.

- Die TR RESISCAN befasst sich überdies ausschließlich mit dem Teilprozess des elektronischen Erfassens von Dokumenten. Darüber hinausgehende Teile des Gesamtprozesses zur elektronischen Dokumentenverwaltung werden ausgeklammert.

Aus den hier formulierten Ansprüchen der TR RESISCAN ergeben sich auch die zentralen Problemfelder hinsichtlich des Nutzens im Hinblick auf die Rechtssicherheit.

- Fehlende Verbindlichkeit und daraus resultierende Notwendigkeit der rechtlichen Verankerung: Die TR RESISCAN sorgt nicht dafür, dass entsprechend gestaltete Verfahren zu einer Beweiskraft führen, die vergleichbar mit der Beweiskraft eines in Papierform aufbewahrten Dokuments ist. Dies wäre aber von zentraler Bedeutung für die größere Akzeptanz einer solchen Richtlinie. Somit bleibt die TR RESISCAN stets darauf angewiesen, dass andere (regelungsfähige) Gesetze, Verordnungen und Vorschriften sie als zulässigen abschließenden Qualitätsmaßstab für die Rechtssicherheit heranziehen. Daher ist davon auszugehen, dass sie allenfalls in bestimmten Regelungsbereichen verbindlich sein wird und somit das bestehende Mosaik spezifischer Anforderungen in verschiedenen Rechtsbereichen um einen weiteren Stein ergänzt.
- Inwiefern sich Behördenleitungen angesichts der Komplexität und des Aufwands zur bloßen Minimierung rechtlicher Risiken dafür entscheiden, die TR RESISCAN zu berücksichtigen, bleibt abzuwarten. Unabhängig von der Frage des Verhältnisses von Aufwand und Nutzen gilt, dass die Verwaltung dem Legalitätsprinzip unterworfen ist. Sie muss also nach Recht und Gesetz handeln. Eine unternehmerische Risikoabwägung – etwa dahin gehend, den Grad der Gerichtsfestigkeit des eigenen Handelns abzuwägen – ist ihr im Grundsatz untersagt.
- Die hergeleitete Klassifikationslogik ist äußerst anspruchsvoll. Die getroffenen Entscheidungen zur Sicherstellung eines rechtmäßigen ersetzenden Scannens kann sie jedoch allenfalls dokumentieren und plausibilisieren. Auch damit bleiben die Anwender auf ihre Entscheidungen und ihre Verantwortung zurückgeworfen.
- Die TR RESISCAN leistet keine ganzheitliche Prozessbetrachtung. Vielmehr gibt es andere Richtlinien für verschiedene Teilprozesse, die jedoch in ihrem Zusammenwirken keinen ganzheitlichen Rahmen erzeugen.

Ein Advocatus Diaboli könnte sogar behaupten, dass die Übertragung von Anforderungen aus bestimmten Rechtskreisen in den Kanon der empfohlenen Maßnahmen auch in anderen Anwendungsgebieten die Rechtsunsicherheit erhöht. Wie die Anlage R der TR RESISCAN eindrücklich ausführt, ist zum Beispiel der Bereich der kaufmännischen Buchführung vergleichsweise einfach geregelt. Seit den Tagen der Mikrofiche-Verfilmung gibt es dort niederschwellige Lösungen für ersetzendes Scannen. Die Übertragung von Elementen anderer Rechtskreise wiederum stellt diese infrage und konfrontiert sie, je nach Analyseergebnis, mit Kryptografieanforderungen. Dieses Vorgehen, verbunden mit einem De-facto-Regelungsanspruch, dürfte nicht dazu beitragen, Unsicherheiten in der rechtlichen Bewertung eingescannter Dokumente abzubauen, weder bei den Anwendern noch vor Gericht.

2 Umsetzung der TR RESISCAN

Die folgenden Abschnitte erläutern einige grundsätzliche Probleme, die sich bei einer TR-RESISCAN-konformen Umsetzung ergeben. Aufgrund der Vielzahl der erkennbaren Probleme wurde die Darstellung auf bestimmte, besonders repräsentative Beispiele beschränkt; eine vollständige Diskussion wurde aus Platzgründen vermieden.

Einige der problematischen Aspekte sind grundsätzlicher Natur, wie beispielsweise der Anspruch der höheren Rechtssicherheit, der starke Fokus auf kryptografische Verfahren, der fehlende Praxisbezug zu üblichen Scanverfahren, die Unschärfe zentraler Begrifflichkeiten und der erhebliche Umfang der zu berücksichtigenden Unterlagen aufgrund der Vielzahl mehrstufig referenzierter mitgeltender Dokumente (BSI-Grundschutz, andere TRs, Common Criteria u. a.).

Andere Herausforderungen hingegen sind sehr konkret, etwa die zahlreichen Anforderungen, die sich im praktischen Alltag nur unter äußersten Schwierigkeiten oder gar nicht umsetzen lassen, sowie fachliche und redaktionelle Fehler, die das Verständnis der Richtlinie erheblich erschweren.

2.1 Enge Fokussierung auf Scanprozess

Eine Grundidee der TR RESISCAN besteht darin, die Integrität des gescannten Bildes sowie weiterer im Scanprozess entstandener Daten zu sichern und diese Integritätssicherung als Bestandteil des Scanprozesses zu betrachten. Dieser Gedanke kommt unter anderem in folgenden Aussagen zum Ausdruck:

- „Um eine unerkannte nachträgliche Manipulation der während des Scanprozesses entstehenden Datenobjekte […] zu vermeiden, MÜSSEN geeignete Mechanismen … eingesetzt werden“[12].
- „Hinsichtlich der Entscheidung, ob ein eingesetzter Sicherheitsmechanismus ausreichende Widerstandsfähigkeit besitzt, kann bei Bedarf auf das im Rahmen der Common Criteria […] formalisierte Angriffspotenzial eines Angreifers zurückgegriffen werden“[13].

Die implizierte Prämisse, dass es mittels technischer Maßnahmen unbedingt möglich sei, von Menschen verursachte Fehler festzustellen, ist in diesem Zusammenhang als unzutreffend und nicht zielführend zu bewerten. Darüber hinaus ist festzuhalten, dass die Integritätssicherung nicht allein im Prozess des Scannens verortet werden darf, sondern als Handlungsmaxime den gesamten Dokumentenlebenszyklus begleiten muss. Vor diesem Hintergrund fällt in der TR RESISCAN besonders auf, dass der in der Scanpraxis übliche Integritätsschutz, nämlich die Prüfung des Scanergebnisses durch einen sachverständigen Mitarbeiter, völlig unberücksichtigt bleibt.

[12] BSI TR 03138, S. 26.
[13] BSI TR 03138, S. 26.

Besonderes Augenmerk wird allerdings auf den Schutzbedarf der Datenobjekte, also des eingescannten Dokuments (Digitalisats), dessen Attribute und anderer Aspekte, gelegt. Selbst auf kryptografische Verfahren wird dabei ausführlich eingegangen. Allerdings ist auch hier darauf hinzuweisen, dass ein technischer Algorithmus nicht in der Lage sein kann zu überprüfen, ob ein einzuscannendes Dokument identisch mit dem Schriftstück ist, das einige Tage zuvor postalisch verschickt bzw. empfangen wurde. Dieser Sachverhalt tritt besonders deutlich beim durchaus üblichen Verfahren des sogenannten späten Scannens hervor, wenn also ein Schriftstück bereits von mehreren Instanzen bearbeitet, klassifiziert, weitergeleitet und möglicherweise verändert wurde, bevor es Tage oder sogar Wochen später zum Scannen vorgelegt wird.

Zusammenfassend soll also darauf hingewiesen werden, dass der Integritätsschutz eines Dokuments immer Teil eines homogenen Gesamtverfahrens sein muss und eben nicht nur im technischen Prozess des Scannens beheimatet sein kann. Beispielhaft sei an dieser Stelle noch die gängige Verfahrenspraxis aus der DMS-Branche erwähnt, die seit über 25 Jahren diesen ganzheitlichen Verfahrensansatz berücksichtigt.

Es stellt sich angesichts der starken Fokussierung auf den Scanprozess auch die Frage, in welchem Umfang denn eine übergreifende Erörterung rechtssicherer elektronischer Vorgangsbearbeitung abzubilden wäre. Die TR RESISCAN ist mit den mitgeltenden Anlagen nämlich ein äußerst umfangreiches, kaum handhabbares Dokument. In dem 160-seitigen oft sehr komplexen, mitunter widersprüchlichen Text werden zusätzlich mehrere Hundert Seiten aus dem BSI-Grundschutz zur Berücksichtigung empfohlen oder sogar gefordert. Gleichzeitig ist der Prozess des Scannens der geringste Teil einer ordnungsgemäßen VBS-/DMS-Lösung. Genauso kritisch für eine zuverlässige, ordnungsgemäße digitale Lösung der Dokumentenverwahrung ist das vorgelagerte Bearbeitungs- und nachgelagerte Aufbewahrungsverfahren. Diese Themen haben beispielsweise die GoBS/GoBD in deutlich komprimierterer Form in einer einzigen Richtlinie vereint. Allerdings muss einschränkend hinzugefügt werden, dass sich die GoBS/GoBD ausschließlich auf die Aufbewahrung handelsrechtlich und steuerrechtlich relevanter Daten und Dokumente in elektronischer Form beziehen und somit weder für alle Dokumentenklassen noch für alle Wirtschaftsteilnehmer (z. B. öffentliche Verwaltung) Anwendung finden.

2.2 Praxistauglichkeit einzelner Anforderungen

Im Folgenden werden einige Anforderungen der TR RESISCAN exemplarisch aufgegriffen, die aus organisatorischer und funktionaler Sicht eine Praxistauglichkeit vermissen lassen:

1. **Schutzbedarfsanalyse:** Für den praktischen Alltag besonders unhandlich ist zweifelsohne die in der TR RESISCAN geforderte Schutzbedarfsanalyse. Sie ist verpflichtender Bestandteil des Gesamtvorgangs. Die Anwender sollen für jede Dokumentart sechs verschiedene Datenobjekte (Papieroriginal, Scandokument, Attribute, Transfervermerk, Sicherungsdaten und Protokolldaten) auf neun Sicherheitsziele (Integrität, Authentizität, Vollständigkeit, Nachvollziehbarkeit, Verfügbarkeit, Lesbarkeit, Verkehrsfähigkeit, Vertraulichkeit, Löschbarkeit) hin bewerten und hierbei jeweils den Schutzklassen „Normal", „Hoch", oder „Sehr hoch" zuordnen. Dabei gilt, dass die TR RESISCAN den Einsatz kryptografischer Verfahren zwingend fordert, sobald eine Dokumentart der Schutzklasse „Hoch" oder „Sehr hoch" zugeordnet wird. Im Übrigen bleibt auch hier das nachgelagerte DMS bzw. Archiv unberücksichtigt.

   Die Schutzklasse „Hoch" ist in der TR RESISCAN dann wie folgt definiert: „Die Schadensauswirkungen sind in der Regel beträchtlich. Ein solcher Schaden führt im Regelfall zu beträchtlichen Konsequenzen für die am Geschäftsvorfall beteiligten Personen und Institutionen."[14] Es liegt letztlich also im Ermessen des zuständigen Anwenders zu beurteilen, ob die Schadensauswirkung oder die Konsequenzen „beträchtlich" sind. Den Anwender zu dieser subjektiven Bewertung zu zwingen ist allerdings nicht als zielführend für einen angestrebten reibungslosen und zuverlässigen Gesamtablauf zu sehen.

2. **Kommunikationsverbindungen**: Die TR RESISCAN beschränkt sich auf der einen Seite auf den Scanvorgang und lässt den Gesamtvorgang des Dokumentenumgangs unberücksichtigt. Daher wird der Leser überrascht, wenn er an anderer Stelle bemerkt, dass Anwender die sieben wesentlichen Kommunikationsverbindungen einer Scanstation analysieren sollen. Die der TR RESISCAN zugrunde liegende Annahme, dass ein Dokument durch externes Eingreifen während des Scanvorgangs in Echtzeit unbemerkt manipuliert werden könnte, erscheint nicht nur sehr abwegig, sondern verlangt vom Anwender ein kaum zu erfüllendes Maß an technischem Expertenwissen und vermengt zusätzlich die eigentliche Zielsetzung dieser TR (d. h. die Gewähr, dass ein Scanprodukt dem Original entspricht) mit der Frage IT-sicherheitsbezogener bzw. datenschutzrechtlicher Abhörsicherungen. Eine im Alltag umzusetzende TR RESISCAN muss aus unserer Sicht vor allem praxistauglich sein, andernfalls wird sie nicht ordnungsgemäß angewendet. Dieser Anspruch wird hier aber nicht erfüllt.

[14] BSI TR 03138 Anlage A, S. 15.

3. **Duplizierung der Digitalisate**: Anlage R empfiehlt, bei Anwendung von Bildverbesserungsalgorithmen (z. B. Kontrastverstärkung, lotrechte Ausrichtung etc.), „das in Frage stehende Original doppelt zu verarbeiten“[15]. Daraus ergibt sich als Konsequenz schlichtweg, dass jedes Digitalisat dupliziert werden muss: erstens zur Verarbeitung der unveränderten Rohdaten und zweitens zur zusätzlichen Verarbeitung der Version, die durch die Bildverbesserungsalgorithmen erzeugt wurde. Dass auf diese Weise eine beträchtliche Datenmenge entstünde, ist offensichtlich. Bei Roh-Bitmaps muss man je DIN-A4-Seite, abhängig von Auflösung und Farbtiefe, mit circa 10–20 MB rechnen. Der Beitrag zur Sicherstellung einer Übereinstimmung des Originaldokuments mit dem Digitalisat bleibt dabei fraglich.

2.3 Technische Aspekte der TR RESISCAN

In dem Versuch, den Scanprozess in aller Tiefe zu durchleuchten, beschreibt die TR RESISCAN in der normativen Anlage A, Kapitel A.1.5, die **Schnittstelle K1 zwischen Scannerhardware und Software**. Dort wird kritisiert, dass weder TWAIN, ISIS noch SANE[16] einen Integritätsschutz als Bestandteil der Schnittstelle vorsehen. Für Anwender, die mit der Umsetzung der Richtlinie konfrontiert sind, stellt dieser Hinweis keinen informativen Mehrwert dar. Es sollte daher überlegt werden, ihn aus der Richtlinie zu entfernen.

Als zwingenden Bestandteil des Gesamtverfahrens fordert die Richtlinie, dass auch bei Wartungs- und Reparaturarbeiten **eventuelle Manipulationen am Gerät**, zum Beispiel am Scan-Cache, **verhindert werden**. Das von der TR RESISCAN unbedingt verfolgte Ziel, sämtliche vorstellbaren Wege zur Verfälschung eines Dokuments während des Scannens zu eliminieren, stellt Anwender hier eindeutig vor nahezu unlösbare Herausforderungen. Von wem und auf welche Weise kann zum Beispiel nach einer Wartung überprüft werden, ob der Scan-Cache manipuliert wurde?

Auch die vielen Empfehlungen zur Hardware des Scanners[17], beispielsweise bezüglich des „Durchsatzes“ (Prüfpunkt A.SC.1.a), der „ausreichenden Flexibilität der Konfiguration“ (Prüfpunkt A.SC.1.e), der „geeigneten Schnittstellen für die Übermittlung der Scanprodukte an andere Anwendungen“ (Prüfpunkt A.SC.1.h), der „Nutzung des internen Datenspeichers“ (Prüfpunkt A.SC.1.j), sind entbehrlich. Dass die Rechtssicherheit des Digitalisats von der jeweiligen marktüblichen Scannerhardware abhängt, ist für Experten nicht erkenntlich. Grundsätzlich sollte sich die Richtlinie auf die normative Formulierung des Kernanliegens konzentrieren und es der jeweiligen Behörde bzw. dem jeweiligen Unternehmen überbelassen, diesem Anliegen gerecht zu werden.

[15] BSI TR 03138 Anlage R, S. 37.
[16] Toolkit Without An Important Name (TWAIN), Image and Scanner Interface Specification (ISIS), Scanner Access Now Easy (SANE).
[17] Vgl. BSI TR 03138, S. 21 f., bzw. BSI TR 03138 Anlage P, S. 12 f.

Die Richtlinie sollte dahin gehend überprüft werden, ob die Einhaltung auch kleinen und mittelständischen Unternehmen bzw. Verwaltungen gelingen kann. Kategorische Forderungen nach Anwendung des Vieraugenprinzips oder der Sicherung alter Konfigurationen und nach Protokollierung der Änderungen werden gerade kleinere Organisationen nur schwer umsetzen können. Ebenfalls sollten Ausführungen zur Nutzung des Scanners, die keinen direkten Zusammenhang zum Kernanliegen (der Sicherstellung der Übereinstimmung des Originals mit dem Digitalisat) aufweisen, überdacht, abgeändert oder gegebenenfalls aus der Richtlinie entfernt werden.

Grundsätzlich sollten die Umsetzungshürden so niedrig wie möglich gehalten werden. Ohne praktische Umsetzbarkeit wird die Richtlinie auf nur sehr begrenzte Akzeptanz stoßen.

Eine wesentliche Anforderung der TR RESISCAN sind **umfassende kryptografische Maßnahmen**, insbesondere Signaturen. Dies gilt, wenn mindestens eine Dokumentart der Schutzklasse „Hoch" bezüglich des Grundwerts Integrität zugeordnet ist. Und je nach Perspektive wird „Hoch" bereits auf einfache kaufmännische Dokumente zutreffen, bei denen Anwender oder deren Berater ein „erhebliches" Schadensrisiko sehen. Sobald mindestens eine Dokumentart mit „Hoch" bewertet ist, sind die Anforderungen der Richtlinie sehr kategorisch: „Darüber hinaus MÜSSEN die spezifischen Maßnahmen in den Abschnitten 4.3.2–4.3.7 umgesetzt werden, wenn der Schutzbedarf bezüglich des entsprechenden Grundwertes (Integrität (gw = IN), Vertraulichkeit (gw = VT) oder Verfügbarkeit (gw = VF)) ‚hoch' (A.AM.gw.H.x) oder ‚sehr hoch' ist."[18]

Die Richtlinie verlangt: Einsatz kryptografischer Mechanismen zum Integritätsschutz, geeignetes Schlüsselmanagement und Berücksichtigung der „einschlägigen Empfehlungen aus [BSI-M 2.46], [NIST-800-57-1/2] und [NIST-800-133]", Auswahl eines geeigneten kryptografischen Verfahrens (gemäß BSI TR 02102 oder BSI TR 03116) und Produkts, Verwendung sicherer Signaturerstellungseinheiten, Nachsignatur mit Empfehlung für TR 03125 (TR ESOR), langfristige Datensicherung bei Einsatz kryptografischer Verfahren, Verhinderung ungesicherter Netzzugänge usw.[19]

Wer diese Anforderungen ohne den Einsatz der vom BSI empfohlenen Signaturverfahren erfüllen möchte, darf dies nur tun, wenn er einen schriftlichen Nachweis über die vergleichbare „ausreichende Widerstandsfähigkeit" des alternativen Verfahrens erbringt.[20] Das dürfte Anwendern in der Regel nicht möglich sein – schon deshalb nicht, weil sie nicht wissen können, nach welchen Kriterien das BSI „ausreichende Widerstandsfähigkeit" bemisst und wie man das praktisch feststellen soll.

[18] BSI TR 03138 Anlage R, S. 26.
[19] Vgl. BSI TR 03138, S. 27–30.
[20] Vgl. BSI TR 03138, S. 29.

Der Einsatz von Signaturverfahren hat für Anwender jedoch gravierende Folgen: Die Einrichtungskosten der Lösungen erhöhen sich deutlich, da mehr Lizenzprodukte erworben und komplexe Hard- und Softwarekomponenten integriert werden müssen. Standardgesamtlösungen sind derzeit auf dem Markt kaum erhältlich und weder bei den meisten deutschen noch bei den großen internationalen Anbietern von Scanlösungen ist erkennbar, dass sie die auf den deutschen Markt beschränkten Anforderungen der TR RESISCAN in ihren Produktstandard aufnehmen. Ferner müssten aufgrund fehlender Standardlösungen auch die bestehenden Archiv-/DMS-Lösungen bei jedem Anwender projektseitig erweitert werden, um die spezifischen Datenobjekte der TR RESISCAN ordnungsgemäß aufzunehmen und zu verwalten. Nicht zuletzt müssten die Archiv-/DMS-Lösungen, in denen die gemäß TR-RESISCAN-Anforderung signierten Unterlagen verwaltet werden, mit einer Nachsignierungsfunktion ausgestattet werden, damit die Dokumente bei Bedarf nachträglich signiert werden könnten.

Zusätzliche Anforderungen entstehen, wenn nicht nur der Grundwert Integrität, sondern auch andere Grundwerte wie Verfügbarkeit oder Vertraulichkeit mit „Hoch“ kategorisiert werden, sodass insgesamt ein äußerst umfangreiches Bündel an Kryptografie- und sonstigen Hochsicherheitsmaßnahmen zu berücksichtigen und zu implementieren ist. Viele dieser Maßnahmen sind als MUSS-, manche als SOLL-, einige als KANN-Anforderung klassifiziert. Einer pragmatischen Anwendung der Richtlinie wird dabei ein Riegel vorgeschoben. Dem Kryptografie- und Signaturzwang kann man nicht dadurch entkommen, dass man einfach nur die MUSS-Anforderungen abdeckt und darauf hofft, dass die SOLL-Anforderungen nicht abgefragt werden. Die Richtlinie definiert hier: „SOLL beschreibt eine nachdrückliche Empfehlung. Abweichungen zu diesen Festlegungen sind nur in wohlbegründeten Ausnahmefällen möglich.“[21] Jeder Prüfer, der diese Definition ernst nimmt, wird das Zertifikat verweigern müssen, wenn ein Anwender nur die MUSS-Anforderungen umsetzt.

Was vielen Lesern bzw. Anwendern ohne sehr aufmerksames Studium der TR RESISCAN und aller ihrer Anlagen vielleicht nicht sofort als Konsequenz auffällt: Dokumente der Schutzklasse „Hoch“ können auch nicht mehr an beliebigen Scanstationen, Multifunktionsgeräten oder per Eingangsfax (eine nach wie vor sehr häufige Zugangsart) digitalisiert werden. Diese Gerätegattungen können zahlreiche MUSS- oder SOLL-Anforderungen gar nicht erfüllen (z. B. keine Zugangskontrollen, keine prüfbaren Scan-Caches, keine verschlüsselbaren internen Kommunikationswege etc.). Der Prüfer, der einem eigentlich normalen Erfassungsprozess ein TR-RESISCAN-Zertifikat erteilen möchte, muss hier gegen die Intention der Richtlinie zertifizieren.

[21] BSI TR 03138, S. 9.

2.4 Normative Rolle

Mit ihrem Anspruch, die Rechtssicherheit zu erhöhen, betritt die TR RESISCAN kein völlig unbearbeitetes Terrain. In der Privatwirtschaft gibt es Kriterien für rechtssicheres Scannen, die seit Jahren angewendet werden und den GoBS bzw. GoBD entnommen werden können. Diese beziehen sich allerdings auf den gesamten Dokumentenlebenszyklus.

Vor allem im Vergleich zu den weit weniger umfangreichen GoBS von 1995 (seit 1. Januar 2015 abgelöst durch die GoBD), die einschließlich eines Begleitschreibens des Bundesministeriums der Finanzen (BMF) nur 17 Seiten umfassen und dabei auch die ordnungsgemäße elektronische Aufbewahrung thematisieren, erscheint die TR RESISCAN als unhandlich und schwerfällig. Gerade zum Zwecke der korrekten und ordnungsgemäßen Umsetzung sollten dem Anwender das Verständnis und der Umgang mit einer Richtlinie nicht unnötig erschwert werden. Es wäre daher sehr empfehlenswert, die Richtlinie als ein geschlossenes Dokument zu präsentieren, das sich, dem Vorbild der GoBD/GoBS folgend, dem Gesamtverfahren des Dokumentenlebenszyklus widmet. Durch Konzentration auf die Nutzerperspektive ergibt sich außerdem erhebliches Kürzungspotenzial. Als „Klammerdokument“, das einschlägige Regelungen zusammenbringen möchte und für alle Anwendungsbereiche – vom Malereibetrieb über eine Bundesbehörde bis hin zu einer Krankenkasse – einen Gesamtregelungsrahmen schafft, wird die TR RESISCAN in der gegenwärtigen Form gerade in Sektoren, die bislang auf deutlich nutzerfreundlichere Regelwerke (wie die GoBD) zurückgreifen konnten, auf wenig Verständnis treffen – zumal die TR RESISCAN die GoBD auch nicht ersetzt, sondern neben sie tritt.

3 Aufwand und Nutzen

Aufgrund des hohen Anspruchs, den die Verfasser an die TR RESISCAN stellen, ist die Umsetzung für alle Anwender sehr aufwendig. An der einen oder anderen Stelle schießen die Anforderungen sogar über das Ziel hinaus. Einige dieser Punkte sind in den vorangegangenen Abschnitten bereits aufgegriffen worden.

In diesem Abschnitt stellen wir eine Reihe von Aufwandstreibern vor und hinterfragen sie. Es geht uns nicht darum, die Anforderungen und damit den Aufwand pauschal auf ein Minimum zu beschränken. Das wäre zu einfach und ginge im Zweifelsfall auch zulasten der Rechtssicherheit. Vielmehr werden wir illustrativ auf Punkte eingehen, bei denen der voraussichtliche Aufwand nicht in einem angemessenen Verhältnis zum Mehr an Rechtssicherheit steht und die verdeutlichen, dass die TR RESISCAN diesbezüglich zu überarbeiten ist.

Generell ist es bei Einführung einer Lösung zum rechtssicheren Scannen und Aufbewahren wichtig, folgende Grundsätze zu beachten:

- Die Einführung von Digitalisierungslösungen ist ein Projekt und kein Vorhaben, das quasi aufwandslos im Tagesbetrieb realisiert werden kann.
- Die sorgfältige Planung und Grundlagenanalyse des Umfelds, in dem die Digitalisierung eingeführt werden soll, verursachen zwar Aufwand, sind aber die Voraussetzung für die effektive und effiziente Umsetzung.

3.1 Strukturanalyse und Schutzbedarfsfeststellung

Die TR RESISCAN (einschließlich der Anhänge und mitgeltenden Dokumente) enthält detaillierte Vorgaben zur Methodik. Diese umfasst zu Beginn eine Struktur- und Schutzbedarfsanalyse.

Vorgehensweise und Inhalt der Strukturanalyse und Schutzbedarfsfeststellung sind sehr umfangreich und detailliert beschrieben. Es darf allerdings bezweifelt werden, ob die konkrete Ausgestaltung praxistauglich ist.

Beispielsweise dürfte es – abhängig vom Einzelfall – nicht immer zwingend erforderlich sein, sämtliche Netze und Datenobjekte in die Bewertung einzubeziehen. Darüber hinaus ist die dedizierte Betrachtung aller in der TR RESISCAN aufgeführten Sicherheitsziele häufig mit einem Aufwand verbunden, der sich unter Verhältnismäßigkeitsgesichtspunkten schwer rechtfertigen lässt.

Unabhängig davon ist der hinter dieser Methodik steckende Grundgedanke, sich im Vorfeld der Gestaltung und Einführung einer Digitalisierungslösung mit den zu digitalisierenden Dokumenten, den daraus resultierenden Anforderungen und den eingesetzten Systemen auseinanderzusetzen, positiv hervorzuheben. In der Praxis kommt dies häufig zu kurz und führt zu ineffizienten oder unzureichenden Lösungen.

Der methodische Ansatz einer Strukturanalyse und Schutzbedarfsfeststellung enthält aus unserer Sicht also eine gute Grundidee. Unglücklicherweise lässt sich dieses Vorgehen aufgrund des hohen Detaillierungsgrads kaum mit vertretbarem Aufwand umsetzen.

3.2 Einschränkung von Wahlmöglichkeiten bei Sicherheitsmaßnahmen

Bei der Ausgestaltung der Sicherheitsmaßnahmen für einen rechtssicheren Scanprozess wird in der TR RESISCAN nicht ausschließlich auf abstrakte Ziele abgestellt. Vielmehr werden konkrete Anforderungen definiert, die auf der Schutzbedarfs- und Risikoanalyse basieren und eine wirkliche Hilfestellung bei der Ausgestaltung der Digitalisierungslösung darstellen können.

Leider hat bei der Definition der Anforderungen an einigen Stellen eine zu starke Fokussierung bzw. Festlegung stattgefunden, sodass Maßnahmen, die eigentlich nur Gestaltungsalternativen darstellen, eher verbindlich zu verstehen sind. Dies kann bei der Umsetzung zu unnötig hohem Aufwand führen.

Ein Beispiel für derartige Einschränkungen und Fokussierungen ist die prominente Empfehlung des Einsatzes qualifizierter elektronischer Signaturen bei erhöhtem Schutzbedarf bezüglich der Integrität. Aufgrund der Aussage, dass eine Abweichung nur in begründeten Ausnahmefällen möglich sei, entsteht der Eindruck, dass solche Signaturen das bevorzugte Mittel sind. Tatsächlich stellen qualifizierte elektronische Signaturen aber nur eine von mehreren Möglichkeiten dar, um das Schutzziel zu erreichen. Welche dieser Möglichkeiten unter Aufwands- bzw. Nutzengesichtspunkten am besten geeignet ist, sollte (auch im Sinne der Technologieneutralität) der Anwender entscheiden.

3.3 Mangelnde Fokussierung auf die Zielsetzung Rechtssicherheit

Bei dem Versuch, eine umfassende Liste von Anforderungen aufzustellen, sind in die TR RESISCAN auch Anforderungen aufgenommen worden, die mit dem primären Zweck nur am Rande etwas zu tun haben. Der Fokus sollte doch auf der Beweiskraft gescannter Dokumente liegen.

Ein Beispiel hierfür stellt die Anforderung A.NB.5 (Barrierefreiheit) der TR RESISCAN dar.[22] Danach sind – zumindest in Behörden und sonstigen öffentlichen Stellen – geeignete Maßnahmen zur Förderung der Barrierefreiheit zwingend erforderlich. Unabhängig von der Tatsache, dass dies gesetzlich vorgeschrieben ist, steht diese Anforderung in keinem Zusammenhang mit der Beweiskraft der gescannten Dokumente. Der für diese Maßnahmen entstehende Aufwand sollte also getrennt betrachtet werden.

Zusätzlich wird bei der Umsetzbarkeit der Schutzmaßnahmen zu wenig differenziert, inwiefern sie einen tatsächlichen Beitrag zur Risikoreduktion leisten.

Diesen Effekt illustriert die A.AM.G.2 der TR RESISCAN.[23] Danach ist eine zwingende Protokollierung beim Scannen erforderlich, sofern Dokumente mit einem Schutzbedarf von mindestens „Hoch“ bezüglich Integrität, Vertraulichkeit oder Verfügbarkeit verarbeitet werden. Eine solche Protokollierung kann sowohl in der Einrichtung als auch im Betrieb deutlichen Aufwand verursachen. Gleichzeitig leistet sie keinen direkten Beitrag zur Erreichung der oben dargestellten Schutzziele.

Die oben dargestellten Mängel in der Differenzierung dürften in der Umsetzung dazu führen, dass für Verfahren, die sich vollständig an der TR RESISCAN ausrichten wollen, Aufwand entsteht, der keinen Beitrag zur Rechtssicherheit bzw. Beweiskraft leistet. Dadurch werden die Anwendbarkeit und die Akzeptanz der TR RESISCAN deutlich beeinträchtigt.

3.4 Zusammenfassung

Die TR RESISCAN versucht im Vergleich zu anderen Vorschriften im Umfeld der Digitalisierung konkrete Vorgaben zu definieren. Allerdings dürfte eine buchstabengetreue Umsetzung der aktuellen TR RESISCAN kaum zu rechtfertigen sein.

Dies liegt vor allem in dem hohen Aufwand begründet, der für die Vorbereitung und Analyse, aber auch für die Ausgestaltung und Implementierung der Maßnahmen anfällt. In einem mittelständischen Unternehmen können allein die Strukturanalyse und Schutzbedarfsfeststellung mehrere Personenwochen in Anspruch nehmen. Für die Planung, Umsetzung und Dokumentation der Maßnahmen ist zusätzliche Zeit einzuplanen. Der Arbeitsaufwand in Personentagen kann also schnell im oberen zweistelligen Bereich liegen. Mit zunehmender Komplexität und Größe des Unternehmens erhöht sich somit auch der Analyse- und Umsetzungsaufwand.

[22] Vgl. BSI TR 03138 Anlage P, S. 18.
[23] Vgl. BSI TR 03138 Anlage P, S. 20.

Hinzu kommen die Kosten für die entsprechenden technischen Mittel (über die eigentlichen Scanvorrichtungen hinaus) zur Umsetzung der Vorkehrungen und Schutzmaßnahmen, sodass der finanzielle Aufwand, der für die wortgetreue Umsetzung der TR RESISCAN zu betreiben ist, in diesem Szenario gut einen sechsstelligen Betrag annehmen kann – eine Größenordnung, bei der Unternehmen es sich unter Effizienzgesichtspunkten genau überlegen, ob die Einführung der Digitalisierung bzw. die Vernichtung von Papierdokumenten diesen Aufwand rechtfertigt.

Um die Vorteile der TR RESISCAN als Werkzeug ergänzend zu anderen rechtlichen Vorschriften (z. B. den GoBD) nutzen zu können, ist aus unserer Sicht daher eine pragmatischere Ausgestaltung erforderlich. Dabei sind folgende Faktoren essenziell:

- Vereinfachung der Methodik zur Strukturanalyse und Schutzbedarfsfeststellung
- Öffnung der Anforderungsdefinition für geeignete Gestaltungsalternativen (einschließlich einer Neutralität hinsichtlich der möglichen Lösungen)
- Fokussierung der eigentlichen Anforderungen auf das für den Einsatzzweck der TR RESISCAN Notwendige (gegebenenfalls mit einer Ergänzung um zusätzliche Empfehlungen)

4 Fokuswahl zur Gewährleistung der Ordnungsmäßigkeit

Unabhängig von der mangelnden Praxistauglichkeit der TR RESISCAN in ihrer jetzigen Form bleibt als weiterer „Knackpunkt“ ihr sehr enger Fokus auf den Scanprozess. Hier besteht aus Anwendersicht noch Handlungsbedarf. Wir empfehlen dringend, die TR RESISCAN so zu überarbeiten, dass das Thema Ordnungsmäßigkeit auf allen relevanten Ebenen betrachtet wird. Wesentliche Punkte werden im Folgenden ausgeführt.

Die TR RESISCAN beschreibt aufgrund ihres Ziels, Rechtssicherheit beim ersetzenden Scannen herzustellen, lediglich Anforderungen an eine Phase innerhalb des Dokumentenlebenszyklus (die Dokumenterzeugung) sowie hierbei nur an einen Typus von Dokumenten (digitalisierte Papierdokumente). Weder im Hinblick auf die Gerichtsverwertbarkeit elektronischer Akten noch auf die Bereitschaft der öffentlichen Verwaltung, die elektronische Akte vollständig und ohne redundante Papierakten einzuführen, reicht diese segmentierte Betrachtung jedoch aus. Hierfür ist nach § 6 EGovG durch geeignete technisch-organisatorische Maßnahmen nach dem Stand der Technik sicherzustellen, dass die Grundsätze ordnungsgemäßer Aktenführung eingehalten werden. Der Begriff der Ordnungsmäßigkeit der Aktenführung ist zwar nicht abschließend geregelt und so bleiben auch für die elektronische Aktenführung noch Prüfkriterien zu spezifizieren. Es ist jedoch klar, dass dafür nicht allein der Blick auf den Scanprozess genügt.

Die TR RESISCAN verwendet wiederum bezogen auf den Prozess der Digitalisierung den Begriff der Ordnungsmäßigkeit und nennt wesentliche Kriterien (auch wenn diese, wie oben beschrieben, nicht immer zweckmäßig erscheinen). Als grundlegende Anforderung an das ersetzende Scannen wird eine Verfahrensdokumentation mit definierten Inhalten (u. a. Qualifizierungsmaßnahmen der Beschäftigten, Abläufe im Scanprozess, IT-Systeme, Sicherheitsanforderungen) formuliert.

Vergleichbare Anforderungen, bezogen auf den gesamten Dokumentenlebenszyklus von der Erzeugung bis zur Aussonderung bzw. Vernichtung, fehlen bislang für die öffentliche Verwaltung. Ohne anerkannte Kriterien kann auch nicht die Ordnungsmäßigkeit der elektronischen Aktenführung nachgewiesen oder durch einen Dritten festgestellt werden. Eine gesamtheitliche Betrachtung der Anforderungen an die Ordnungsmäßigkeit, wie es im Übrigen die IDW RS FAIT 3 oder die PK DML für den Bereich der Privatwirtschaft bereits exemplarisch aufzeigen, wäre aus Sicht der Verwaltungen zwingend notwendig.

Daher scheint allein das Grundkonzept der TR RESISCAN nicht zu greifen. Eine derart stark segmentierte Betrachtungsweise ist für Anwender wenig zielführend. Vielmehr sind Anforderungen an das ersetzende Scannen in ein Gesamtkonzept zur ordnungsgemäßen elektronischen Aktenführung zu integrieren. Dabei wird dann gegebenenfalls auch ersichtlich, dass an die ersetzend gescannten Dokumente grundsätzlich die gleichen Anforderungen wie an elektronisch geborene Dokumente gestellt werden sollten. Hier wird die qualifizierte elektronische Signatur nur bei Schriftformerfordernis eingesetzt, obwohl auch Dokumente ohne Schriftformerfordernis, die zum Beispiel den Verwaltungsakt dokumentieren, vor Gericht Anerkennung finden müssen.

Aus unserer Sicht umfasst daher ein solcher zu entwickelnder Kriterienkatalog, in dem die TR RESISCAN in einer Fortentwicklung aufgehen kann, folgende Phasen bzw. Aspekte des gesamten Dokumentenlebenszyklus:

- die Entgegennahme (Posteingang)/Erfassung/Erzeugung von Dokumenten und Daten
- die Speicherung und Verknüpfung von Dokumenten und Daten
- die Bearbeitung und Veränderung von Dokumenten und Daten
- den Zugriff und die Reproduktion von Dokumenten und Daten
- die Langzeitspeicherung von Dokumenten und Daten
- die Vernichtung und Aussonderung (inkl. Fristenmanagement) von Dokumenten und Daten

Diese Aspekte gilt es in einer ganzheitlicheren Betrachtung, die die Dimensionen Organisation, Dokumentation, Mensch und Technik umfasst, zu beschreiben.

Die genannten vier Dimensionen durchziehen auch die TR RESISCAN, allerdings mit starker Fokussierung auf die Themen Technik und Kryptografie. Es ist durchaus positiv hervorzuheben, dass beispielsweise Anforderungen an das Scanpersonal entwickelt werden. Zugleich hat die TR RESISCAN sich auf einen Aspekt, nämlich den Scanprozess, zu sehr verengt und diesen zu komplex und anspruchsvoll geregelt, sodass das primäre Ziel, die Rechtssicherheit zu erhöhen, in der Praxis derzeit kaum zu erreichen ist.

Eine überarbeite Version 2.0 könnte indes sehr wohl einen Beitrag leisten und zudem in ein umfassenderes und zugleich praxistauglicheres Regelwerk zur Definition und Gewährleistung der Ordnungsmäßigkeit elektronischer Aktenführung eingebettet werden.

D Fazit

Unser Fazit kann nur lauten, dass wir eine grundlegende Überarbeitung der TR RESISCAN empfehlen. Gerade mit Blick auf ihre Grundintention, Anwendern eine Hilfestellung zu geben, erweist sie sich als wenig praxisgeeignet. In vielen Punkten tendiert sie zur Überregulierung.

Eine deutlich überarbeitete Version, integriert in eine umfassende Klärung der Ordnungsmäßigkeit elektronischer Aktenführung, hätte indes das Potenzial, einen großen Beitrag zur weiteren Verbreitung der E-Akte und moderner, digitaler Arbeitsformen zu leisten.

Wir freuen uns auf eine Version 2.0.

Ihre Ansprechpartner

Dr. Wolfgang Zink
Partner
Tel.: +49 69 9585-3012
wolfgang.zink@de.pwc.com

Carsten Crantz
Senior Manager
Tel.: +49 40 6378-1836
carsten.crantz@de.pwc.com

Wigand Grabner
Senior Manager
Tel.: +49 30 2636-1492
wigand.grabner@de.pwc.com

PwC

Über uns

Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expertennetzwerks in 157 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

PwC. 9.400 engagierte Menschen an 29 Standorten. 1,55 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.

Bernhard Zöller
Tel.: +49 6196 999-09-0
bzoeller@zoeller.de

Volker Halstenbach
Tel.: +49 6196 999-09-0
vhalstenbach@zoeller.de

Zöller & Partner

Über uns
Zöller & Partner ist eine strikt anbieter- und produktneutrale Organisations- und Technologieberatung, fokussiert auf Enterprise-Content-Management (ECM).
Dazu gehören die Themen:

- Optimierung Content-basierter Abläufe und Geschäftsprozesse (Workflow)
- Dokumentenmanagement
- elektronische Archivierung
- Collaboration
- Outputmanagement
- Web-Content-Management