Der Beauftragte der Bundesregierung für Informationstechnik

Dienstekonsolidierung

Leitfaden: E-Scannen für Bundesbehörden

Ersetzendes Scannen gemäß EGovG und TR-RESISCAN

Anlage (V): Muster Verfahrensanweisung für Bundesbehörden

Inhaltsverzeichnis

1 Einleitung

Hinweis: Das vorliegende Dokument enthält Textbausteine für eine exemplarische Verfahrensanweisung für Bundesbehörden und zielt darauf ab, die Einführung und/oder Durchführung eines ordnungsgemäßen Scanprozesses gemäß der Technischen Richtlinie „Ersetzendes Scannen (RESISCAN)“

[BSI-TR03138] des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bei Bundesbehörden zu unterstützen. Sie stellt eine Hilfestellung bei der anwendungsbezogenen Umsetzung der durchzuführenden Maßnahmen entsprechend dem im konkreten Anwendungsbereich ermittelten Schutzbedarf dar. Um die Umsetzung zu erleichtern, ist das Dokument wie eine Dokumentenvorlage mit Platzhaltern für die jeweilige Institution/Organisation erstellt worden. Abweichungen sind möglich, jedoch wird empfohlen, insbesondere auf Vollständigkeit der Maßnahmen und zu treffenden Regelungen zu achten.

Als Organisation ist die Behörde zu verstehen. Typischerweise wird die Verfahrensbeschreibung durch die Behördenleitung freigegeben. Die Pflege der Verfahrensbeschreibung kann auch in der für Organisationsfragen zuständigen Organisationseinheit angesiedelt sein. Der Freigabe- und Pflegeprozess ist behördenspezifisch festzulegen.

Die vorliegende Musterverfahrensbeschreibung wurde auf Basis von

[BSI-TR03138-V] entwickelt und geht von einem Ersetzenden Scannen bei der Behörde selbst aus. Sofern ein Scandienstleister eingesetzt wird, so sind die für „Outsourcing“ einschlägigen Bausteine (OPS.2.1) des BSI-Grundschutz-Kompendiums [BSI-GSK] zu beachten und von der Behörde nur die Schnittstellen zum Dienstleister zu beschreiben, die übrigen Aspekte des Ersetzenden Scannen müssen in der Verfahrensdokumentation des Scandienstleisters selbst enthalten sein.

Das vorliegende Dokument ist die Verfahrensweisung für das ersetzende Scannen bei [Organisation] gemäß TR-RESISCAN.

Nur die Leitung der Organisation ist berechtigt Ausführungen und Änderungen der Verfahrensanweisung zu genehmigen, namentlich [Leiter der Organisation].

Diese Verfahrensanweisung wurde von der Leitung der Organisation am [Datum] von [Name] freigegeben, trägt die Versionsbezeichnung [Versionsbezeichnung] und gilt ab [Datum] bis zu einer Überarbeitung.

Die vorliegende Verfahrensanweisung ersetzt die bis dahin geltende Verfahrensanweisung [vorherige Versionsbezeichnung].

Diese Verfahrensanweisung dokumentiert die Maßnahmen und Verfahrensschritte, die für den Scanprozess inkl. der Vernichtung der originären Papierbelege in der [Organisation] gelten.

Die beschriebenen Maßnahmen und Verfahren sind von allen beteiligten Personen, die an den einzelnen Prozess-Schritten beteiligt sind sowie für diese unterwiesen und autorisiert wurden, zu befolgen.

2 Überblick

2.1 Organisatorisches Umfeld

Hinweis: Hier erfolgt die Beschreibung der Behörde (Aufgaben, Struktur, Standorte incl. Adressen etc.) sowie der mit dem ersetzenden Scannen und Aufbewahrung betrauten Organisationseinheiten

unter Angabe der Aufgabe im Scanprozess. Dies umfasst insbesondere alle behördlichen Scan- und Aufbewahrungsorte für die Originalunterlagen (bis zur Vernichtung). Darüber hinaus wird der Anwendungsfall (Scannen von Posteingängen, Scannen von Bestandsakten) etc. einschließlich der Scanperioden (täglich / wöchentlich / monatlich) etc.

Die Angaben sollten möglichst detailliert und lückenlos erfolgen. Unterstützt wird die Darstellung beispielsweise durch Organisationspläne und geeignete Grafiken, die als Anlage zur Verfahrensanweisung beigefügt werden können.

[Kurze Beschreibung der Organisation: Name, Sitz, rechtliche Verankerung, Ressort, Geschäftszweck.]

[Kurze Erläuterung von Besonderheiten der Organisation bzgl. der Verarbeitung und Aufbewahrung von Dokumenten.]

Hinweis: Bei ressortbezogenen/anwendungsfallbezogenen Besonderheiten handelt es sich um spezielle Vorgaben zur Digitalisierung oder Aufbewahrung von Papieroriginalen, z.B. Formerfordernisse, Verpflichtungen zur Aufbewahrung der Papieroriginale durch Spezialgesetze etc.

[Soweit dies bei der Größe der Organisation sinnvoll ist, erfolgt eine kurze Beschreibung der für das ersetzende Scannen relevanten Organisationseinheiten.]

- [Organisationseinheit:] [Prozess-Schritt, z. B. Bearbeitung der Eingangspost]
- […]

Die Digitalisierung findet an nachfolgend beschriebenen Orten statt:

- [ggf. Adresse, Raum].
- […]

Die Ablage der Originaldokumente bis zur Vernichtung erfolgt an folgenden Orten:

- [ggf. Adresse, Raum].

Die Digitalisierung erfolgt [fallweise/in [täglichen/wöchentlichen/monatlichen] Digitalisierungsläufen].

2.2 Rechtliche Rahmenbedingungen

Für das ersetzende Scannen bei [Organisation] sind die folgenden rechtlichen und organisatorischen Rahmenbedingungen zu berücksichtigen:

Hinweis: Hier werden die für die Behörde oder den Anwendungsfall relevanten Rechtsgrundlage aufgelistet z.B.:

- eIDAS-Verordnung
- [eIDAS-VO]
- Datenschutzgrundverordnung
- [DSGVO]

- E-Government-Gesetz [EGovG]
- Minikommentar zum EGovG [EGovG-MK]
- Bundesdatenschutzgesetz [BDSG]
- Gemeinsame Geschäftsordnung der Bundesministerien
- [GGO]
- Einschlägige Regularien zur Personalaktenführung bei den Bundesbehörden, wie z.B. **Fehler! Ungültiger Eigenverweis auf Textmarke.** und [BDG]
- Registraturrichtlinie
- [RegR]
- BSI TR-RESISCAN
- [BSI-TR03138]
- BSI TR-ESOR [BSI-TR03125]
- spezialgesetzliche Vorgaben und behördenspezifische Richtlinien[1]

2.3 Verarbeitete Dokumente

Hinweis: Hier werden die tatsächlich in die Digitalisierung einbezogenen Dokumente aufgelistet und dabei insbesondere auch benannt, welche Dokumente ersetzend und welche kopierend gescannt werden. Sofern die Unterlagen den am Scanprozess beteiligten Personen zugänglich sind, kann auch auf weiterführende und mitgeltende Dokumente, wie z.B. die Schutzbedarfsanalyse oder eine Negativliste zum Scannen, die dann eine verbindliche Anlage zur Verfahrensanweisung darstellt, verwiesen werden.

Digitalisiert werden originär in Papierform vorliegende bzw. eingehende Dokumente, die absehbar aktenrelevant sind und einer Dokumentations- und Aufbewahrungspflicht unterliegen.
Dies umfasst insbesondere:

- […]

2.4 Nicht verarbeitete Dokumente (Negativliste)

Hinweis: Hier werden die Dokumente aufgelistet, die entweder nicht gescannt werden (z.B. aufgrund Format, Beschaffenheit etc.) oder nicht ersetzend gescannt werden (z.B. Dokumente, die aufgrund gesetzlicher Vorgaben nicht ausschließlich elektronisch geführt werden dürfen). Es wird empfohlen, diese Dokumente in einer Negativliste aufzulisten und diese als verbindliche Anlage der Verfahrensbeschreibung beizufügen. Ebenso ist im Sinne einer vollständigen elektronischen Akte anzugeben, wo die Papieroriginale aufbewahrt werden z.B.: Aktenlagerraum 3, Regel 4, Fach 5, Box 24. Diese Angabe muss selbstverständlich der korrespondierenden elektronischen Akte ebenso hinzugefügt werden.

Explizit von der Verarbeitung und vor allem von der Vernichtung ausgeschlossen sind Dokumente, denen aufgrund ihrer Form gesetzlicher Bestimmung im Original besondere Bedeutung zukommt, wie z. B. [notarielle Urkunden, Testate unter Siegelverwendung, Eröffnungsbilanzen und Abschlüsse, Wertpapiere, Zollpapiere mit fluoreszierendem Original-Stempel, …].

[1] Behördenspezifische Regelungen z.B.BSI-Gesetz, Bauartzulassung etc.

Diese werden explizit von der [Erfassung und/oder] Vernichtung ausgenommen. Dafür werden sie [im Rahmen der Dokumentenvorbereitung/bei einer Durchsicht vor der Vernichtung] ausgesondert und geordnet archiviert. Für diese Dokumente erfolgt eine papierbasierte Aufbewahrung des Originaldokuments nach den entsprechenden Regelungen [der Organisation]. In Zweifelsfällen holt der für die Zuordnung der Dokumente zum Scannen zuständige Mitarbeiter[2] Auskunft bei der zuständigen Führungskraft ein.

2.5 Der Scanprozess

Hinweis: Die Verfahrensbeschreibung fokussiert auf den kompletten Scanprozess inklusive der Übergabe von Scanprodukt und Transfervermerk an das Zielsystem. Bei einer möglichen Zertifizierung werden nur die Schritte ab Dokumentenvorbereitung bis einschließlich der Integritätssicherung betrachtet. Die vorliegende Beispielbeschreibung geht von einem Ersetzenden Scannen in der Behörde selbst aus. Sofern die Digitalisierung durch einen Scandienstleister erfolgt, werden durch die Behörde nur die Schnittstellen, also bis zur Übergabe der Papieroriginale an den Scandienstleister und die Übernahme vom Scandienstleister beschriebe. Die übrigen Teile sind vom Digitalisierungsdienstleister in dessen Verfahrensbeschreibung festzuhalten und von der Behörde auf Konformität gegenüber der TR-RESISCAN zu prüfen.

Der Prozess für das ersetzende Scannen bei [Organisation] umfasst folgende Schritte:

- Eingang des Dokuments
- Dokumentenvorbereitung
- Scannen
- Nachverarbeitung
- Integritätssicherung
- Aufbewahrung bzw. Zwischenspeicherung [bis zur Übergabe an Langzeitspeicher]
- Vernichtung des Originals

Hinweis: Beim Eingang des Papierdokuments (siehe auch Abschnitt 0) und der Übergabe der elektronischen Dokumente an den Langzeitspeicher zur Aufbewahrung (siehe Abschnitt 2.5.6) wird in der Verfahrensdokumentation nur die Schnittstelle zu den angrenzenden Systemen betrachtet, wie z.B. die E-Akte oder das Digitale Zwischenarchiv des Bundes (DZAB). Die Aufbewahrung selbst ist Teil eines Archivkonzepts, das zusätzlich zum Scankonzept notwendig ist.

2.5.1 Eingang des Dokumentes

Der Scanprozess beginnt mit dem Eingang des papiergebundenen Dokumentes [an Ort] oder dem Vorliegen der Bestandsakten am Scanort.

2.5.2 Dokumentenvorbereitung

Hinweis: Die Maßnahmen in der Dokumentenvorbereitung entsprechen im Wesentlichen der Behandlung des papiernen Posteingangs und dessen Vorbereitung zum Scannen. Details können z.B. dem Baustein Scanprozess des Organisationskonzepts elektronische Verwaltungsarbeit

[2] Im Rahmen der vorliegenden Verfahrensanweisung sind unter dem Begriff „Mitarbeiter“ sowohl weibliche als auch männliche Mitarbeiter umfasst.

[OK-eVA-SP] entnommen werden.

2.5.2.1 Vorsortierung mit Prüfung auf Echtheit

Der Posteingang wird unter Beachtung der Vollständigkeit (kein Verlust von eingegangenen Sendungen, keine ungeprüfte Vernichtung) vom zuständigen Mitarbeiter geöffnet, gesichtet und nach den organisationsinternen Vorgaben [mit einem Posteingangsstempel versehen,] vorsortiert und [an Ort] abgelegt.

Bei der Sichtung erfolgt eine Prüfung auf Echtheit und Unversehrtheit der Eingangspost. Liegen Zweifel vor (z. B. fehlender Stempel auf Original; fehlende Unterschriften; fehlende Form; Beschädigungen, z. B. Risse; fehlende Seiten, z. B. erkennbar an durchbrochener fortlaufender Nummerierung), wird das Verfahren bzgl. der betroffenen Dokumente beendet und von einer weiteren Bearbeitung vorläufig abgesehen. Es erfolgt eine Rücksprache mit der zuständigen Führungskraft und bei Bedarf dem Absender des Dokuments.

2.5.2.2 Identifikation der zu scannenden Dokumente (rechtliche bzw. faktische Prüfung)

Hinweis: Die Identifikation der zu scannenden bzw. scanbaren Dokumente erfolgt beispielsweise anhand der Positivliste (vgl. Abschnitt 2.3) und der Negativliste (vgl. Abschnitt 2.4), die die nicht scanfähigen Dokumente enthält. Die nicht scanbaren Dokumente werden geeignet separiert und am definierten Aufbewahrungsort verwahrt (vgl. Abschnitt 2.4).

Die geöffnete [gestempelte] und vorsortierte Eingangspost/Bestandsakten wird hinsichtlich der Scanfähigkeit der einzelnen Dokumente vom zuständigen Mitarbeiter geprüft. Dabei werden alle gemäß Abschnitt 2.3 zu erfassenden Dokumente für die anschließende Digitalisierung identifiziert und an [Ort] abgelegt. Der dem Schutzbedarf angemessene Zugriffsschutz wird durch […] gewährleistet.
Hat der zuständige Mitarbeiter Zweifel an der Scanfähigkeit eines Dokuments, so holt er beim zuständigen Fachbereich oder der zuständigen Führungskraft eine entsprechende Auskunft ein.

2.5.2.3 Vorbereitung der zu digitalisierenden Dokumente (technische Prüfung)

Hinweis: Die Vorbereitung der zu scannenden Dokumente enthält alle Schritte bis zum praktischen Auflegen des Scanstapels auf dem Scangerät und der eigentlichen technischen Durchführung der Digitalisierung. Hier gilt es bspw. festzulegen:

- Art und Aufbau der Scanstapel
- Ggf. vorherige Erfassung von i.d.R. einem minimalen Metadatensatz je Dokument
- Ausgabe der Metadaten auf Bar-/QR-Code zur Stapeltrennung

Alle für eine Digitalisierung identifizierten Belege werden durch den Scanmitarbeiter daraufhin geprüft, ob eine Verarbeitung durch das Digitalisierungsgerät technisch möglich ist und ein originalgetreues Abbild erzeugt werden kann.
Es wird im Einzelnen geprüft, ob für einen erfolgreichen Scanvorgang vorherige Maßnahmen am Dokument erforderlich sind. Als solche kommen beispielhaft in Frage:

- Lösen von Klammerungen
- Sorgfältiges Sortieren, um die Reihenfolge zu gewährleisten

- Ordnungsgemäßes Einlegen von Trennblättern
- Entfernen von Notiz- und Klebezetteln
- Anbringung von Barcodes/QR-Codes
- Bildung von Scanstapeln

2.5.3 Scannen

Hinweis: Die Maßnahmen zum Scannen beschreiben insbesondere wie die (ersetzende) Digitalisierung ausgestaltet ist, ggf. auch in Unterscheidung der Digitalisierung in einer zentralen Scanstelle und dem möglichen Scannen am Multifunktionsgerät etc. Hierzu gehören im Wesentlichen:

- Angaben zu den verwendeten Scannern und Scansoftware incl. Zugriffskontrollen und Außerbetriebnahme, IT-Sicherheit z.B.:
  - Vorgaben zur Nutzung der Scanner incl. Passwörter
  - Ausreichender Durchsatz
  - Geeignete Dateiformate, typischerweise PDF/A oder TIFF
  - Unterstützung Dokumententrennung und Seiteneinzug
  - Schnittstellen und Zusammenspiel mit Zielsystemen
- Angaben zur Nutzung der Scanhardware und –Software, der Scaneinstellungen und verwendeter Bildkompressionsverfahren
  - Geeignete Scaneinstellungen beziehen sich u.a. auf einseitiger/doppelseitiger Scan, Format, Auflösung etc.
- Metadatenerfassung
  - Texterkennung und Indexierung
- Qualitätssicherung
  - Prüfung der Scanqualität, je nach Schutzbedarf kann dies in Stichproben oder kompletter Sichtkontrolle erfolgen
- Protokollierung des Scannens

Der Digitalisierungsvorgangs wird durch das Auflegen auf das Scangerät bzw. durch das Einlegen in den Einzug durch den zuständigen Mitarbeiter eingeleitet.
Der Digitalisierungsvorgang endet mit der Ausgabe des digitalen Mediums und der Speicherung [auf dem Export-Datenpfad/...]. Darüber hinaus sind folgende Details zu berücksichtigen:

- [...]

Vor der Digitalisierung prüft der zuständige Mitarbeiter, ob alle erforderlichen Hard- und Softwarekomponenten betriebsbereit sind und die vorgegebenen Grundeinstellungen am Digitalisierungsgerät eingestellt sind.
Es wird sichergestellt, dass keine unzulässigen Kompressionsverfahren (siehe Anforderung A.SC.12 in [BSI TR-03138]) eingesetzt werden.
Die Grundeinstellungen für die Digitalisierung sind folgendermaßen definiert:

- [...]
- Zielformat: [z.B. PDF-A/TIFF/...]
- Auflösung: [X] dpi
- [Farbscan/Graustufenscan/Schwarz-Weiß-Scan] mit [Einstellung]
- Kontrast: [Einstellungen zu Kontrast]
- [Automatischer/manueller] und [einseitiger/beidseitiger] Einzug
- […]

Durch […] ist sichergestellt, dass keine unzulässigen Kompressionsverfahren[3] eingesetzt werden.

Hinweis: Sofern die papierne Vorlage relevante farbliche Markierungen enthält, so ist zur Gewährleistung der bildlichen und inhaltlichen Übereinstimmung auch ein Farbscan notwendig. Als typische Auflösung lassen sich bspw. 300 dpi angeben, als Formate haben sich bspw. PDF/A und TIFF bewährt.

Der Umgang mit Vorder-/Rückseite ist wie folgt geregelt:

- [Es wird immer Vor- und Rückseite gescannt]
- [Die Rückseite wird nur dann nicht gescannt, wenn sie leer ist]
- […]

Die Zwischenablage und Benennung der erzeugten Scandateien ist wie folgt geregelt:

- Ablageort/Verzeichnis: [...]
- Namenskonvention: [...]
- […]

Nach dem Scanvorgang werden die Papieroriginale vollständig und in unveränderter Ordnung zum Zweck der Kontrolle und der weiteren Behandlung an folgendem, gegen unbefugten Zugriff gesicherten [an Ort], abgelegt. Der Zugriffsschutz zu diesen Räumlichkeiten wird realisiert durch […].

Die zuständige Person stellt unmittelbar im Anschluss an die Digitalisierung sicher, dass jeder Papierbeleg genau einmal gescannt wurde (Vollständigkeit und Existenz der digitalisierten Kopie). Dies ist insbesondere bei mehrseitigen Originaldokumenten von Bedeutung, wobei auch auf die fortlaufende Nummerierung der Seiten geachtet wird. Fehlende digitale Dokumente werden erneut der Digitalisierung zugeführt, Mehrfachdigitalisierungen werden bis auf eine Kopie gelöscht oder entsprechend als Kopie gekennzeichnet und von einer doppelten Weiterverarbeitung ausgeschlossen.
Die zuständige Person überprüft zudem auf bildlich und inhaltlich korrekte Übertragung des Inhalts des papierbasierten zum digitalen Dokument, um einem Informationsverlust oder Informationsveränderungen vorzubeugen (Lesbarkeits- und Plausibilitätskontrolle).

Fehlerhafte digitale Dokumente werden erneut der Digitalisierung zugeführt, Mehrfachdigitalisierungen werden bis auf eine Ausfertigung gelöscht oder entsprechend als Kopie gekennzeichnet, um von einer doppelten Weiterverarbeitung ausgeschlossen zu werden. Die Prüfung der bildlichen und inhaltlichen Übereinstimmung erfolgt für [Anzahl Dokumente/Stichprobe/vollständige Sichtkontrolle].

2.5.4 Nachverarbeitung

Hinweis: Die Nachverarbeitung dient bspw. der Bearbeitung des Scanprodukts, um die Lesbarkeit zu erhöhen, selbstverständlich ohne Verfälschung der Inhalte. Darüber hinaus umfasst die Nachverarbeitung die Qualitätssicherung der nachbearbeiteten Scanprodukte und die Vollständigkeitsprüfung (z.B. durch Prüfung Anzahl gescannter Seiten vs. Seiten des Originals). Ein wesentlicher Punkt der Nachverarbeitung ist die Erstellung des Transfervermerks. Dieser

[3] Unzulässig wären insbesondere Bildkompressionsverfahren auf Basis von „Pattern Matching & Substitution“ oder „Soft Pattern Matching“, wie sie beispielsweise beim JBIG2 Format gemäß ISO/IEC 14492 genutzt werden.

dokumentiert den korrekten Ablauf des Scannens und ist zum Nachweis des ersetzenden Scannens nach TR-RESISCAN entscheidend. Als Angaben haben sich vor allem bewährt:

- Ersteller des Scanproduktes,
- etwaige Auffälligkeiten während des Scanprozesses
- Zeitpunkt der Erfassung
- Ergebnis der Qualitätssicherung und
- Bestätigung der bildlichen und inhaltlichen Übereinstimmung sowie ggf. Angaben zum technischen und organisatorischen Umfeld des Erfassungsvorganges (sofern nicht aus der Verfahrensbeschreibung ersichtlich).

Technisch wird der Transfervermerk von marktüblicher Scansoftware i.d.R. als XML-Datei ausgegeben und gemeinsam mit dem Scanprodukt dem Zielsystem übergeben werden. Als logische Verknüpfung bietet sich bspw. die Ablage des Transfervermerks als Metadatum im PDF/A (XMP) an.

Nach dem Scanvorgang werden die Papieroriginale vollständig und in unveränderter Ordnung zum Zwecke der Kontrolle und der weiteren Behandlung in einer gegen unbefugten Zugriff geschützten Weise [an Ort] abgelegt.

Die zuständige Person stellt unmittelbar im Anschluss an die Digitalisierung sicher, dass jeder Papierbeleg genau einmal gescannt wurde (Vollständigkeit und Existenz der digitalisierten Kopie). Dies ist insbesondere bei mehrseitigen Originaldokumenten von Bedeutung, wobei auch auf die fortlaufende Nummerierung der Seiten geachtet wird. Fehlende digitale Dokumente werden erneut der Digitalisierung zugeführt, Mehrfachdigitalisierungen werden bis auf eine Kopie gelöscht oder entsprechend als Kopie gekennzeichnet und von einer doppelten Weiterverarbeitung ausgeschlossen.
Die zuständige Person überprüft zudem auf bildlich und inhaltlich korrekte Übertragung des Inhalts des papierbasierten zum digitalen Dokument, um einem Informationsverlust oder Informationsveränderungen vorzubeugen (Lesbarkeits- und Plausibilitätskontrolle).

Hierbei erfolgt eine [vollständige/stichprobenartige] Sichtkontrolle [, die mindestens x % der verarbeiteten Dokumente umfasst].

Als Maßnahmen zur Verbesserung der Lesbarkeit des Scanprodukts sind zugelassen: […]
Fehlerhafte digitale Dokumente werden erneut der Digitalisierung zugeführt, Mehrfachdigitalisierungen werden bis auf eine Ausfertigung gelöscht oder entsprechend als Kopie gekennzeichnet und von einer doppelten Weiterverarbeitung ausgeschlossen.

Eine unautorisierte manuelle Veränderung des Scanproduktes ist ausgeschlossen, da […].
Das Scanergebnis in Form des digitalisierten Belegs wird im Zuge der Nachverarbeitung um folgende Index- und Metadaten angereichert:

- […]

2.5.5 Integritätssicherung

Hinweis: Die Maßnahmen zur Integritätssicherung des Scanprodukts müssen mit denjenigen des Transfervermerks übereinstimmen. Mit dem (qualifizierten) elektronischen Siegel gem. eIDAS-Verordnung, das auf Organisationszertifikaten beruht, wurde der Aufwand für kryptographische Sicherungsmittel erheblich reduziert, bei gleichzeitiger Gewährleistung der Verkehrsfähigkeit und hohem Beweiswert der gesiegelten Scanprodukte und Transfervermerke. In der Praxis wird aus diesem Grund häufig, auch unabhängig vom konkreten Schutzbedarf, das (qualifizierte) elektronische Siegel verwendet. Dieses lässt sich zudem auch für weitere Zwecke, wie z.B. digitale Bescheide

verwenden. Insofern sollte die Integritätssicherung in der Behörde im Gesamtkontext der Digitalisierung der behördlichen Prozesse betrachtet werden.

Die Integrität der digitalen Beleg-Kopie mit dem Papieroriginal wird durch Anwendung folgender technischer und organisatorischer Maßnahmen abgesichert:
[…]

Die Verkehrsfähigkeit der digitalen Beleg-Kopien ist durch […] gewährleistet.

2.5.6 Aufbewahrung bzw. Zwischenspeicherung [bis zur Übergabe an Geschäftsanwendung oder Langzeitspeicher]

Hinweis: Die Übergabe an die Geschäftsanwendung[4] in der das Scanprodukt und Transfervermerk weiterverarbeitet wird kann direkt nach dem Scannen oder asynchron zu einem dezidierten Zeitpunkt erfolgen. Bis zur Übergabe sind Integrität, Vertraulichkeit und Verfügbarkeit durch das Scansystem zu gewährleisten. Als Zielsystem kommen z.B. die E-Akte Bund oder das DZAB resp. die jeweilige Geschäftsanwendung in Frage. Je nach Dauer der Aufbewahrung bis zur Übergabe an Zielsystem sind ggf. Maßnahmen zur Beweiswert- und Informationserhaltung von Scanprodukt und Transfervermerk zu treffen. Grundsätzlich sollten die gescannten Dokumente zeitnah nach dem Scannen ans Zielsystem übergeben werden, um eine korrekte Veraktung und Aufbewahrung zu gewährleisten. Aus Gründen der Nachweisfähigkeit empfiehlt sich aus Praxissicht eine zeitnahe Übergabe an ein zur Beweiswerterhaltung geeignetes Verfahren.

Die Scanprodukte werden einschließlich der zugehörigen Transfervermerke an folgendes System/Ablageort […] übergeben und dort [bis zur Übergabe an die Geschäftsanwendung/ den Langzeitspeicher] (vgl. Abschnitt 2.2) aufbewahrt. Die Verfügbarkeit, Auffindbarkeit und Lesbarkeit wird durch folgende Maßnahmen sichergestellt:

- […].

2.5.7 Vernichtung des Originals

Die Vernichtung der digitalisierten Papierbelege erfolgt in einem zeitlich festgelegten Turnus, und zwar [täglich/wöchentlich/monatlich/...] für alle Papierbelege mit einem Alter von mehr als [einem Tag/einer Woche/einem Monat]. Sie wird vom zuständigen Mitarbeiter […] autorisiert und vom zuständigen Mitarbeiter […] durchgeführt.

In keinem Falle erfolgt eine Vernichtung vor dem Durchlaufen aller in der vorliegenden Verfahrensdokumentation dargestellten Schritte inkl. mindestens eines durchgeführten Backup-Laufes.
Bei der Vernichtung werden datenschutzrechtliche Aspekte berücksichtigt, indem [alle Belege/alle Belege mit Personenbezug] vollständig nach den Empfehlungen des Datenschutzes je nach Vertraulichkeitsstufe geschreddert werden.

2.6 Das Scansystem

Das Scansystem umfasst die nachfolgend aufgeführten Hardware- und Softwarekomponenten zur Digitalisierung, Integritätssicherung und Aufbewahrung.

[4] Hierunter werden in IT-Systeme oder –Verfahren resp. Fachverfahren in den Behörden verstanden (z.B. E-Akte, Langzeitspeicher, Bafög-System, ERP-System u.ä.)

2.6.1 Digitalisierung

Für die Digitalisierung kommt folgende Hardware zum Einsatz:

- [...]

Weitere Angaben über die eingesetzte Hardware der Digitalisierung sind [...] zu entnehmen.
Für die Digitalisierung kommt folgende Software zum Einsatz:

- [...]

Weitere Angaben über die eingesetzte Software der Digitalisierung sind [...] zu entnehmen.

2.6.2 Integritätssicherung

Die Integrität des Scanproduktes wird durch Anwendung der folgenden technischen und organisatorischen Maßnahmen abgesichert:

- [...]

Für die Integritätssicherung der Scanprodukte kommt folgende Hardware zum Einsatz:

- [...]

Weitere Angaben über die eingesetzte Hardware zur Integritätssicherung sind [...] zu entnehmen.
Für die Integritätssicherung der Scanprodukte kommt folgende Software zum Einsatz:

- [...]

Weitere Angaben über die eingesetzte Software zur Integritätssicherung sind [...] zu entnehmen.
Für den Schutz der Integrität der in den Scanprozess involvierten Systeme sind die in Abschnitt 3.3.2 näher erläuterten Maßnahmen vorgesehen.

2.6.3 Aufbewahrung [bis zur Übergabe an die Geschäftsanwendung/den Langzeitspeicher]

Für die Aufbewahrung der digitalisierten Belege [bis zur Übergabe an die Geschäftsanwendung/ den Langzeitspeicher] kommt folgende Hardware zum Einsatz:

- [...]

Weitere Angaben über die für die Aufbewahrung der digitalisierten Belege eingesetzte Hardware sind [...] zu entnehmen.
Für die Aufbewahrung der digitalisierten Belege kommt folgende Software zum Einsatz:

- [...]

Weitere Angaben über die für die Aufbewahrung der digitalisierten Belege eingesetzte Software sind [...] zu entnehmen.

Details zum Speichermedium für die digitalisierten Belege sowie deren Ablage sind [...] zu entnehmen.

Hinweis: Sofern im Rahmen der vorliegenden Verfahrensdokumentation die zuverlässige, langfristige Aufbewahrung berücksichtigt wird, müssen beispielsweise auch entsprechende Festlegungen zu Backups getroffen werden.

Die gespeicherten Dokumente werden durch folgende Verfahren einem systematischen Backup- Prozess unterzogen, damit im Falle eines Ausfalls des Speichermediums jederzeit eine vollständige und verlustfreie Wiederherstellung der Daten erreicht werden kann:

- [technische Verfahren der Absicherung, z. B. tägliche Spiegelung]
- [Backup-Verfahren; Turnus und Logik der Backups]

Sowohl bei Ersteinrichtung als auch turnusmäßig ([monatlich/halbjährlich/jährlich]) erfolgt ein Funktionsfähigkeitstest des Backup- und Wiederherstellungsverfahrens.
Sowohl bei Ersteinrichtung als auch turnusmäßig ([wöchentlich/monatlich]) erfolgt ein stichprobenartiger Test der Integrität und Lesbarkeit der Scanprodukte und zugehörigen Daten.
[Durch folgende Maßnahmen/Aus folgenden Gründen] ist sichergestellt, dass die Zuverlässigkeit der Speicherung im Hinblick auf den Schutzbedarf der Datenobjekte angemessen ist:

- [...]

2.6.4 Umgebung

Die Software für die Digitalisierung, Integritätssicherung und Speicherung der Scanprodukte und zugehörigen Transfervermerke läuft in folgender Systemumgebung:

- [...]

Weitere Angaben über die Umgebung der eingesetzten Software sind [...] zu entnehmen.
Für die eingesetzten Hard- und Software-Komponenten liegen folgende Softwarebescheinigungen oder Zertifikate vor, die auch Teil des Auswahlprozesses dieser Komponenten waren:

- [...]

Angaben über die notwendige Einsatzumgebung der eingesetzten Software sind [...] zu entnehmen.

3 Maßnahmen

3.1 Organisatorische Maßnahmen

3.1.1 Verantwortlichkeiten und Regelungen

Hinweis: Hier gilt es alle das Scannen betreffenden respektive hiermit korrespondierenden Regelungen aufzulisten, die beim ersetzenden Scannen zu beachten sind. Hierzu können, neben der Verfahrensanweisung beispielsweise gehören:

- Aktenordnung/Registraturrichtlinie etc.
- Richtlinie zum Umgang mit Postein- und -ausgängen
- Richtlinie zum Umgang mit (qualifizierten) elektronischen Signaturen, Siegeln und Zeitstempeln

Darüber hinaus sind alle Verantwortlichkeiten für jeden Schritt beim ersetzenden Scannen sowie die Qualitätskontrollen, die berührten IT-Systeme und Anwendungen oder eine Clearingstelle für Zweifelsfragen festzulegen. Dabei sind Interessenkonflikte zu vermeiden und besonderes Augenmerk auf typische Fehlerquellen zu legen.

Es gelten folgenden organisatorische Regelungen und Verantwortlichkeiten zum ersetzenden Scannen:

- [...]

Die nachfolgend aufgeführten Mitarbeiter sind zur Durchführung der einzelnen Verarbeitungsschritte eingewiesen und verantwortlich:

- [...]

3.1.1.1 Dokumentenvorbereitung

Die Dokumentenvorbereitung wird durchgeführt von:

- [Name, Vorname, ggf. Personalnummer oder Funktion in der Organisation]

3.1.1.2 Scannen

Der Digitalisierungsvorgang wird durchgeführt von:

- [Name, Vorname, ggf. Personalnummer oder Funktion in der Organisation]

3.1.1.3 Nachverarbeitung

Die Nachverarbeitung, die insbesondere die Vollständigkeits-/Lesbarkeits- und Plausibilitätskontrolle umfasst, wird durchgeführt von:

- [Name, Vorname, ggf. Personalnummer oder Funktion in der Organisation]

Hinweis: Sofern besonders schutzwürdige Dokumente verarbeitet werden und hierfür gesonderte Regelungen vorgesehen sind, sind die folgenden Passagen relevant.

Es ist nur folgenden Personen gestattet die Digitalisierung, Vollständigkeits-/Lesbarkeits- und Plausibilitätskontrolle sowie Nachverarbeitung und Aufbewahrung von Dokumenten mit Belegfunktion, die laut organisationsinterner Vorgaben als besonders schutzwürdig gelten, vorzunehmen:

- Name, Vorname, ggf. Personalnummer oder Funktion in der Organisation]

In diesen Fällen erfolgt die Ablage [auf einem gesonderten Export-Datenpfad welcher zur Sicherstellung dient/...], wobei der Zugang nur folgenden Personen gestattet ist:

- [...]

Hierbei ist der Zugriff durch folgende Maßnahmen geschützt:

- [...]

3.1.1.4 Integritätssicherung

Die Integritätssicherung wird durchgeführt von:

- [Name, Vorname, ggf. Personalnummer oder Funktion in der Organisation bzw. im System]

3.1.1.5 Geeignete Aufbewahrung [bis zur Übergabe an Langzeitspeicher]

Die Aufbewahrung der Dokumente [bis zur Übergabe an Langzeitspeicher] wird verantwortet von:

- [Name, Vorname, ggf. Personalnummer oder Funktion in der Organisation]

3.1.1.6 Vernichtung des Originals

Die Freigabe zur Vernichtung der Dokumente erfolgt durch

- [Name, Vorname, ggf. Personalnummer oder Funktion in der Organisation]

Die tatsächliche Vernichtung der originalen Dokumente erfolgt durch [Interne Stelle/Externen Dienstleister] und wird verantwortet von

- [Name, Vorname, ggf. Personalnummer oder Funktion in der Organisation]

Der externe Dienstleister ist von [Name] unter der Registrierungsnummer […] zertifiziert.
Die Freigabe zur Löschung der digitalen Archivbestände erfolgt in keinem Fall vor Ablauf der Aufbewahrungsfrist und durch:

- [Name, Vorname, gegebenenfalls Personalnummer oder Funktion in der Organisation]

Die tatsächliche Löschung der digitalen Archivbestände erfolgt durch

- [Name, Vorname, gegebenenfalls Personalnummer oder Funktion in der Organisation]

3.1.2 Regelungen für Wartungs- und Reparaturarbeiten

Die Wartung und die Reparatur der für den Scanvorgang eingesetzten IT-Systeme und Anwendungen ist folgendermaßen geregelt:

Die Festlegung der Verantwortlichkeiten für die Beauftragung, Durchführung und ggf. Kontrolle von Wartungs- und Reparaturaufgaben obliegt [Name, Vorname, gegebenenfalls Personalnummer oder Funktion in der Organisation].

Regelungen zur Authentisierung und zum Nachweis der Autorisierung des Wartungspersonals werden von Mitarbeitern [Name, Vorname, gegebenenfalls Personalnummer oder Funktion in der Organisation] überwacht.

Die Dokumentation von sicherheitsrelevanten Veränderungen an den involvierten IT-Systemen und Anwendungen erfolgen durch die Mitarbeiter [Name, Vorname, gegebenenfalls Personalnummer oder Funktion in der Organisation].

Die Dokumentation der erfolgreichen Durchführung der Maßnahmen zur Qualitätskontrolle und Freigabe vor der Wiederaufnahme des regulären Betriebs erfolgt durch die Mitarbeiter [Name, Vorname, gegebenenfalls Personalnummer oder Funktion in der Organisation].

3.1.3 Abnahme- und Freigabe-Verfahren für Hardware und Software

Durch die ordnungsmäßige und ununterbrochene Nutzung der in Abschnitt 2.6 aufgeführten Hard- und Software wird insbesondere sichergestellt, dass die in Abschnitt 2.2 aufgeführten rechtlichen Rahmenbedingungen eingehalten werden.

Gleichzeitig wird sichergestellt, dass die digitalisierten Daten bei Lesbarmachung mit den ursprünglichen papiergebundenen Unterlagen bildlich und inhaltlich übereinstimmen. Sie sind während der Dauer der Aufbewahrungsfrist verfügbar und können jederzeit innerhalb angemessener Frist lesbar gemacht werden.

Bei einer Änderung der digitalisierungs- und/oder archivierungsrelevanten Hardware und/oder Software wird neben der Dokumentation der Systemänderung sichergestellt, dass die Lesbarkeit der digitalisierten Dokumente gewährleistet bleibt.

3.1.4 Aufrechterhaltung der Informationssicherheit

Für die Informationssicherheit im Scanprozess ist [Name, Vorname, gegebenenfalls Personalnummer oder Funktion in der Organisation] verantwortlich.

In angemessenen zeitlichen Abständen erfolgt eine Überprüfung der Wirksamkeit und Vollständigkeit der für die Informationssicherheit beim Ersetzenden Scannen vorgesehenen Maßnahmen.
Die Audits werden regelmäßig alle [x Jahre/Monate] durchgeführt. [Beispielsweise wurde das letzte Audit von [Firma, Name] am [Datum] durchgeführt. Die fachliche Kompetenz und Unabhängigkeit für die qualifizierte Durchführung der Audits ist gewährleistet durch […].

Die Ergebnisse dieser Überprüfung werden [schriftlich/elektronisch] dokumentiert. Sofern Sicherheitslücken oder andere Probleme gefunden werden, werden entsprechende Korrekturmaßnahmen durchgeführt.

Für die Korrekturmaßnahmen wird ein Zeitplan mit verantwortlichen Mitarbeitern definiert. Detaillierte Festlegungen finden sich in […].

3.1.5 Anforderungen beim Outsourcing des Scanprozesses

Hinweis: Sofern der Scanprozess komplett oder teilweise von spezialisierten Scandienstleistern durchgeführt wird, sind die in

[BSI-TR03138] vorgesehenen Maßnahmen und die in den für „Outsourcing“ relevanten Bausteine (OPS.2.1 bzw. OPS.3.1) des IT-Grundschutz-Kompendiums [BSI-GSK] aufgeführten Maßnahmen zu berücksichtigen. Darüber hinaus ist zu beachten, dass bei einem Outsourcing des Scanprozesses nur die Schnittstellen in der Verfahrensbeschreibung der Behörde darzustellen sind, der eigentliche Scanprozess wird dann durch den Scandienstleister in dessen Verfahrensbeschreibung dokumentiert.

Die organisatorischen und technischen Schnittstellen zwischen Auftraggeber und Auftragnehmer (Übertragungswege, Datenablageorte, beteiligte Akteure, Rückfallverfahren etc.) sind folgendermaßen gegeben:

- […]

Der Auftragnehmer wird zur Einhaltung der vom Auftraggeber definierten Sicherheitsmaßnahmen verpflichtet. Dies umfasst insbesondere:

- […]

Die Analyse der durch die Aufgabenteilung zusätzlich entstehenden Risiken hat zu folgendem Ergebnis geführt:

- […]

Zusätzlich zur regelmäßigen Auditierung werden unangemeldete Stichprobenprüfungen durchgeführt. Verantwortlich für die Durchführung und Auswertung dieser Stichprobenprüfung ist

- [Name, Vorname, gegebenenfalls Personalnummer bzw. Funktion in der Organisation]

Darüber hinaus existieren folgende vertragliche Regelungen:

- […]

3.2 Personelle Maßnahmen

3.2.1 Grundlegende Anforderungen

An die in den Scanprozess eingebundenen Mitarbeiter werden die folgenden grundlegenden Anforderungen gestellt:

- [...]

3.2.1.1 Sensibilisierung der Mitarbeiter für Informationssicherheit

Zur Einweisung und Sensibilisierung der Mitarbeiter für die Informationssicherheit erfolgt für die in Abschnitt 3.1.1 genannten vorbereitenden, digitalisierenden, archivierenden, kontrollierenden, freigebenden und vernichtenden Mitarbeiter eine regelmäßige [jährliche/...] Unterweisung in den Digitalisierungs-, Archivierungs- und Vernichtungsprozess. Darüber wird ein Protokoll angefertigt und archiviert. Die beteiligten Mitarbeiter verpflichten sich in dieser Unterweisung explizit zur Einhaltung dieser Verfahrensanweisung.

Bei einem Wechsel der personellen Zuständigkeit erfolgt eine Unterweisung in den Digitalisierungs-, Archivierungs- und Vernichtungsprozess sowie eine Schulung zur ordnungsmäßigen Bedienung des Digitalisierungs- und Archivierungssystems durch die zuständige Führungskraft. Die unterwiesenen Mitarbeiter verpflichtet sich explizit zur Einhaltung dieser Verfahrensdokumentation.

3.2.2 Verpflichtung der Mitarbeiter

Die im Rahmen der fachlichen Schutzbedarfsanalyse identifizierten und in Abschnitt 0 aufgeführten rechtlichen Rahmenbedingungen werden den in den Scanprozess involvierten Mitarbeitern zur Kenntnis gebracht. Die Mitarbeiter werden, sofern dies nicht bereits geschehen ist, auf die Einhaltung der einschlägigen Gesetze, Vorschriften, Regelungen und der Verfahrensanweisung verpflichtet.

Dies erfolgt durch Mitarbeiter [Name, Vorname, gegebenenfalls Personalnummer bzw. Funktion in der Organisation].

3.2.3 Maßnahmen zur Qualifizierung und Sensibilisierung

3.2.3.1 Einweisung zur ordnungsgemäßen Bedienung des Scansystems

Die Mitarbeiter, die den Scanvorgang durchführen, werden von den verantwortlichen Mitarbeitern ([Name, Vorname, gegebenenfalls Personalnummer bzw. Funktion in der Organisation]) hinsichtlich der eingesetzten Geräte, Anwendungen und sonstigen Abläufe eingewiesen. Dies umfasst insbesondere:

- die grundsätzlichen Abläufe im Scanprozess einschließlich der Dokumentenvorbereitung, dem Scannen, der Indexierung, der zulässigen Nachbearbeitung und der Integritätssicherung,
- die geeignete Konfiguration und Nutzung des Scanners und der Scan-Workstation,
- Anforderungen hinsichtlich der Qualitätssicherung,
- die Abläufe und Anforderungen bei der Erstellung des Transfervermerks,
- die Konfiguration und Nutzung der Systeme zur Integritätssicherung und
- das Verhalten im Fehlerfall.

Hierfür werden die unter […] abgelegten Schulungsunterlagen genutzt.

3.2.3.2 Einweisung zu Sicherheitsmaßnahmen im Scanprozess

Zuständige Mitarbeiter, die den Scanvorgang durchführen oder verantworten, werden von [Name, Vorname, gegebenenfalls Personalnummer bzw. Funktion in der Organisation] in geeigneter Weise hinsichtlich der dabei umzusetzenden sowie der implementierten Sicherheitsmaßnahmen eingewiesen. Dies umfasst insbesondere:

- die grundsätzliche Sensibilisierung der Mitarbeiter für Informationssicherheit,
- personenbezogene Sicherheitsmaßnahmen im Scanprozess,
- systembezogene Sicherheitsmaßnahmen im Scansystem,
- Verhalten bei Auftreten von Schadsoftware,
- Bedeutung der Datensicherung und deren Durchführung,
- Umgang mit personenbezogenen und anderen sensiblen Daten und
- Einweisung in Notfallmaßnahmen.

Hierfür werden die unter […] abgelegten Schulungsunterlagen genutzt.

3.2.3.3 Schulung des Wartungs- und Administrationspersonals

Zuständige Mitarbeiter für Wartungs- und Administrationsaufgaben für die in den Scanprozess involvierten IT-Systeme und Anwendungen werden hinsichtlich der hierfür notwendigen Kenntnisse über die eingesetzten IT-Komponenten geschult.
Dies erfolgt durch [Name, Vorname, gegebenenfalls Personalnummer bzw. Funktion in der Organisation] [in regelmäßigen Abständen/zuletzt am ...] und umfasst insbesondere:

- Selbstständigkeit bei alltäglichen Administrationsaufgaben,
- selbstständige Fehlererkennung und -behebung,
- regelmäßige selbsttätige Durchführung von Datensicherungen,
- Nachvollziehbarkeit von Eingriffen externen Wartungspersonals, das Erkennen und Beheben von Manipulationsversuchen oder unbefugten Zugriffen auf die Systeme.

Hierfür werden die unter […] abgelegten Schulungsunterlagen genutzt.

3.3 Technische Maßnahmen

3.3.1 Grundlegende Sicherheitsmaßnahmen für IT-Systeme

Hinweis: Die grundlegenden Sicherheitsmaßnahmen sind abhängig vom konkreten Scansystem dessen Aufbau und Struktur in der Strukturanalyse beschrieben sind.

Für die in den Scanprozess involvierte IT-Systeme werden die hierfür im IT-Grundschutz-Kompendium [BSI-GSK] vorgesehenen Sicherheitsmaßnahmen umgesetzt. Die wirksame Umsetzung der Maßnahmen wurde geprüft durch [Name] am [Datum].

Gemäß des Sicherheitskonzeptes wurden hierbei insbesondere die folgenden IT-Grundschutz-Bausteine berücksichtigt:

- [...]

3.3.2 Zulässige Kommunikationsverbindungen

Da die für das Scannen eingesetzten IT-Systeme über ein Netzwerk verbunden sind, werden in diesem Netzwerk sowie auf den IT-Systemen selbst die zulässigen Kommunikationsverbindungen durch entsprechende Maßnahmen geschützt. Dies umfasst insbesondere

- [...]

Die verantwortlichen Mitarbeiter [Name] hat die Wirksamkeit der zum Schutz der IT-Infrastruktur vorgesehenen Sicherheitsmaßnahmen am [Datum] geprüft.

3.3.3 Schutz vor Schadprogrammen

Um einer Infektion durch Schadprogramme vorzubeugen werden die Maßnahmen des IT-Grundschutz-Bausteins OPS.1.1.4 (Schutz vor Schadprogrammen) berücksichtigt. Dies umfasst insbesondere:

- die Auswahl eines geeigneten Viren-Schutzprogramms, wie vom zuständigen Mitarbeiter [Name] am [Datum] festgelegt,
- die Meldung von Schadprogramm-Infektionen an die zuständigen Mitarbeiter ([Name]),
- die Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen (diese [erfolgt automatisch/wird von den zuständigen Mitarbeitern [Name] regelmäßig alle […] angestoßen]),
- eine regelmäßige Datensicherung, die regelmäßig und [automatisch/von den zuständigen Mitarbeitern [Name]] alle […] angestoßen wird.

3.3.4 Mitgeltende Unterlagen

Neben den vorstehend aufgeführten Regelungen gelten folgende Unterlagen:

- [...]
- [Anwenderhandbücher X, Y]
- [weitere Arbeits-/Organisationsanweisungen X, Y]
- [Berechtigungskonzept X, Y]
- [Bericht über Prüfung des Archivsystems, X]

- [Freigaberichtlinien X, Y]
- [IT-Sicherheitskonzept]
- [Organigramm]
- [Vereinbarung/Vertrag zwischen X und Y]

3.3.5 Zuverlässige Speicherung (TR-ESOR konforme Langzeitspeicherung)

Hinweis: Für die beweiswerterhaltende Aufbewahrung (Langzeitspeicherung) ist der Dienst DZAB für die Bundesbehörden verbindlich zu nutzen, sofern nicht eigene Komponenten nach dem Stand der Technik [BSI-TR03125] bereits vorhanden sind.

Die beweiswerterhaltende Aufbewahrung der Scanprodukte inkl. Transfervermerke und zugehörigen Metadaten wird wie folgt gewährleistet:

- […]

Literaturverzeichnis

[BBG] Bundesbeamtengesetz, https://www.gesetze-im-internet.de/bbg_2009/

[BDG] Bundesdisziplinargesetz, http://www.gesetze-im-internet.de/bdg/

[BDSG] Bundesdatenschutzgesetz, https://www.gesetze-im-internet.de/bdsg_2018/

[BSI-GSK] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kompendium, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

[BSI-TR03125] Bundesamt für Sicherheit in der Informationstechnik (BSI): Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR), BSI TR-03125 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html

[BSI-TR03138] Bundesamt für Sicherheit in der Informationstechnik (BSI): Ersetzendes Scannen (RESISCAN), BSI TR-03138 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03138/index_htm.html

[BSI-TR03138-V] Bundesamt für Sicherheit in der Informationstechnik (BSI): Ersetzendes Scannen – Anwendungshinweis V: Exemplarische Verfahrensanweisung, BSI TR-03138-V, Version 1.2, 2018

[DSGVO] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), http://data.europa.eu/eli/reg/2016/679/oj

[EGovG] Bundesministerium der Justiz und für Verbraucherschutz: Gesetz zur Förderung der elektronischen Verwaltung, https://www.gesetze-im-internet.de/egovg/

[EGovG-MK] Bundesministerium des Innern, für Bau und Heimat (Referat O2): Minikommentar zum Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften, https://www.verwaltung-innovativ.de/SharedDocs/Publikationen/Artikel/Minikommenta_EGov_Gesetz.pdf?__blob=publicationFile&v=1

[eIDAS-VO] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, http://data.europa.eu/eli/reg/2014/910/oj

[GGO] Bundesregierung: Gemeinsame Geschäftsordnung der Bundesministerien (GGO), https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/ministerium/ggo.pdf?__blob=publicationFile&v=2

[OK-eVA-SP] Bundesministerium des Innern, für Bau und Heimat: *Organisationskonzept elektronische Verwaltungsarbeit – Baustein Scanprozess*, https://www.verwaltung-innovativ.de/SharedDocs/Publikationen/Organisation/scanprozess.pdf

[RegR] Bundesministerium des Innern, für Bau und Heimat: Richtlinie für das Bearbeiten und Verwalten von Schriftgut (Akten und Dokumenten) in Bundesministerien (RegR), https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/ministerium/registraturrichtlinie.pdf

[ZPO] Bundesministerium der Justiz und für Verbraucherschutz: Zivilprozessordnung, https://www.gesetze-im-internet.de/zpo/BJNR005330950.html

Impressum

Herausgeber
Der Beauftragte der Bundesregierung für Informationstechnik, 10557 Berlin

Ansprechpartner
Programm Dienstekonsolidierung
Postanschrift: Alt-Moabit 140, 10557 Berlin
Hausanschrift: Englische Str. 30, 10587 Berlin
Referatspostfach: DGII1@bmi.bund.de
Internet: www.cio.bund.de

Stand
15.04.2020

Bildnachweis
James Brey/GettyImages

www.cio.bund.de