Ersetzendes Scannen

Verfahrensanweisung

Stand 22.11.2017

Herausgeber

Beauftragter der Landesregierung für
Informationstechnik (CIO)

Ministerium für Wirtschaft, Innovation, Digitalisierung
und Energie des Landes Nordrhein-Westfalen

Historie

Version	*Datum*	*Autor*	*Änderungen*	*Freigabe*	*Gültig ab*
1.0	*22.11.17*	*Markus Kahle*		*06.12.17*	*15.01.17*

1. Inhaltsverzeichnis

1. Einleitung

Das vorliegende Dokument ist die Verfahrensanweisung für das ersetzende Scannen bei der [Organisation] gemäß [BSI-TR03138 Version: 1.1] und der Verwaltungsvorschrift zu § 23 Abs. 2 Nr. 5 EGovG NRW.

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

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

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

Diese Verfahrensanweisung beinhaltet die Maßnahmen und Verfahrensschritte, die für den Scanprozess inkl. der Vernichtung der originären Papierbelege in der [Organisation] _____ gelten. Gegenstand dieser Verfahrensanweisung ist das Scannen sowohl der Eingangspost als auch der Bestandsakten.

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.

Diese Verfahrensanweisung ist beschränkt auf eine ordnungsgemäße Digitalisierung von Dokumenten mit dem Ziel der Aufrechterhaltung der Beweiskraft des Digitalisats im Vergleich zum Papieroriginal, unter Berücksichtigung der geltenden Ordnungsmäßigkeitsanforderungen. Sonstige im Vergleich zu Papierbelegen analoge Verfahren bleiben unangetastet und gelten weiterhin gemäß der in der [Organisation] _____getroffenen Regelungen.

2. Überblick

2.1 Organisatorisches Umfeld

[Kurze Beschreibung der Organisation: Name, Sitz]

Beispiel:
Als Mittelbehörde in der Landesverwaltung stellt die Bezirksregierung Detmold das Bindeglied zwischen Landesregierung und der Region Ostwestfalen-Lippe dar. Sie vereinigt die wichtigsten Fachaufgaben fast aller Landesministerien und bringt regionale Interessen sowie Besonderheiten ein.

Der Sitz der Bezirksregierung Detmold ist in der Leopoldstr. 15, 32756 Detmold

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

Beispiel:
Der Posteingang ist entsprechend der vielen unterschiedlichen Aufgaben, die in der Bezirksregierung wahrgenommen werden sehr heterogen. Ebenso existieren Bestandsakten unterschiedlichster Ausprägungen und Umfänge.

2.1.1 Eingangspost

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

Beispiel:
Die Eingangspost geht bei der zentralen Poststelle der Bezirksregierung in Detmold ein. Die Zentrale Poststelle ist Teil des Servicebereiches, der wiederum Teil des Dezernates 12 (Beauftragter für den Haushalt, Vergabe, Justitiariat, Innerer Dienst) ist.

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

Beispiel:
Dezernat 12 → Servicebereich → Posteingang

- Bearbeitung der Eingangspost
- Übergabe an den Scanbereich

Dezernat 12 → Servicebereich → Scanstelle

- Scanvorbereitung
- Digitalisieren
- Ablegen ins Zwischenarchiv

Die Digitalisierung findet an nachfolgend beschriebenen Orten statt:

Adresse und Raum:_____

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

[ggf. Adresse, Raum]: _____

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

2.1.2 Bestands-/Altakten (Akten)

Die zu digitalisierenden Akten werden von der aktenführenden Stelle in Zusammenarbeit mit der Scanstelle analysiert und die notwendigen Anforderungen für die Digitalisierung werden projektbezogen beschrieben.

Dies ist in einer Vereinbarung zu dokumentieren.

Folgende Festlegungen muss die Vereinbarung mindestens enthalten:

- Aufbereitung der Papierakten
- Schutzbedarfskategorien für die Schutzziele Integrität, Vertraulichkeit und Verfügbarkeit der Akten bzw. einzelner Akteninhalte
- Übergabeverzeichnis der Akten
- Ort des Scannens und ggflls. Transport der Akten zur Scanstelle
- Qualität (Auflösung, Farbe etc.) des Digitalisats
- Struktur und Übergabe des Digitalisats
- Aufbewahrungszeit und Aufbewahrungsort der Akten bis zur Vernichtung
- Freigabe/Qualitätssicherung/Entsorgung der Akten
- Zustimmung zur Vernichtung der Papierdokumente
- Ansprechpartner

Im Rahmen des Bestandsaktenscans ist projektbezogen die Entscheidung zu treffen, welche Dokumente ersetzend gescannt werden können und in welchen Fällen die Rücksendung der Papieroriginale erfolgen oder das Einverständnis zur Vernichtung eingeholt werden muss.

Sofern der Scanprozess komplett oder teilweise von externen Scandienstleistern durchgeführt wird, sind darüber hinaus die besonderen Anforderungen beim Outsourcing des Scanprozesses aus der TR-RESISCAN zu berücksichtigen.

2.2 Rechtliche Rahmenbedingungen

Für das Ersetzende Scannen bei [Organisation] _____ sind insbesondere die folgenden rechtlichen Rahmenbedingungen zu berücksichtigen:

Gesetz zur Förderung der elektronischen Verwaltung in Nordrhein-Westfalen –EGOVG NRW

Verordnung über elektronische Identifizierung und Vertrauensdienste – eIDAS

Vertrauensdienstegesetz - VDG

Verwaltungsvorschrift zum Ersetzenden Scannen nach dem E-Governmentgesetz NRW

Die jeweils geltende Aktenordnung

DIN 66399

Datenschutzgesetz NRW / Datenschutz-Grundverordnung EU

2.3 Eingangspost

Digitalisiert werden als Papierdokumente vorliegende bzw. eingehende Dokumente. Dies umfasst insbesondere schriftliche Posteingänge von Bürgern, Betrieben und Behörden.

2.3.1 Nicht zu scannende Dokumente

Dem Ausschluss der elektronischen Form unterliegen alle Objekte, die beispielsweise wegen ihrer dreidimensionalen Form nicht scanbar sind (z.B. Gebiss-Modell, Kfz-Nummernschild).

Dokumente, bei denen durch eine Scanvorbereitung der Zustand verändert würde (z.B. gesiegelt und gekordelt), dürfen nicht verarbeitet werden. Dokumente mit einem Schutzbedarf größer hoch dürfen nicht in diesem beschriebenen Scanprozess digitalisiert werden.

Der Scanstelle ist eine Liste über nicht zu scannende Dokumentklassen vorzugeben. Diese Dokumentklassen werden dem Empfänger auf herkömmlichen Weg zugeleitet.

2.3.2 Nach dem Scannen nicht zu vernichtende Dokumente (Ergänzendes Scannen)

Gem. Nr. 7 .1a) - e) Verwaltungsvorschrift Ersetzendes Scannen dürfen dort genannte Dokumentklassen nach dem Scannen nicht vernichtet werden.

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 Auskunft bei seiner zuständigen Führungskraft ein.

2.4 Der Scanprozess der Eingangspost

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

- Eingang des Dokumentes
- Vorbereitung der zu digitalisierenden Dokumente
- Scannen
- Zwischenlagerung der Papierdokumente
- Integritätssicherung des Digitalisats
- Nachverarbeitung des Digitalisats
- Aufbewahrung der Scanprodukte
- Re-Scan fehlerhafter Dokumente
- Vernichtung des Papieroriginals

2.4.1 Eingang des Dokumentes

Der Scanprozess beginnt mit dem Eingang des papiergebundenen Dokumentes [Ort]

2.4.2 Dokumentenvorbereitung

2.4.2.1 Vorsortierung mit Prüfung auf Vollständigkeit, Echtheit und Unversehrtheit

Die Eingänge sind auf Vollständigkeit, Echtheit und Unversehrtheit zu prüfen.

Beispiel:

Zunächst werden die nicht zu öffnenden Eingänge aussortiert.

Anschließend wird der Posteingang unter Beachtung der Vollständigkeit (kein Verlust von eingegangenen Sendungen, keine ungeprüfte Vernichtung) vom zuständigen Mitarbeiter geöffnet, gesichtet und mit einem Posteingangsstempel versehen. Der Stempel erfolgt direkt auf der ersten Seite des eingegangenen Schriftstückes.

Bei der Sichtung erfolgt eine Prüfung auf Unversehrtheit der Eingangspost. Liegen Zweifel vor (z.B. fehlender Stempel auf Original, fehlende Unterschriften, ungewöhnliche Form, Beschädigungen, z.B. Risse, fehlende Anlagen, fehlende Seiten, z. B. erkennbar an durchbrochener fortlaufender Nummerierung), muss dies in einem Vermerk, der dem Dokument beigefügt wird, aufgenommen werden. Gegebenenfalls kann dieser Vermerk ein Foto des z.B. beschädigten Briefes beinhalten. Liegt der Verdacht vor, dass es sich bei dem vorliegenden Dokument um eine Manipulation handelt, so ist das Papieroriginal dem zuständigen Sachbearbeiter vorzulegen.

2.4.2.2 Identifikation der zu scannenden Belege

Grundsätzlich werden alle Dokumente mit für Schutzbedarf "hoch" (Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit) vorgeschriebenen Maßnahmen nach TR RESISCAN behandelt.

[Beschreibung der Prüfung der eingegangenen Dokumente; Ablage; Raum/ Schutzbedarfsanalyse]

Beispiel:

Die eingegangenen Dokumente werden nach Organisationseinheiten sortiert in Stapeln abgelegt. Alle gemäß Abschnitt 2.3 zu bearbeitenden Dokumente werden für die anschließende Digitalisierung identifiziert und im Raum ___ abgelegt. Der dem Schutzbedarf angemessene Zugriffsschutz wird dadurch gewährleistet, dass der Raum nur von Berechtigten zu öffnen ist. Zusätzlich erfolgt während der Stapelbildung eine Sichtkontrolle auf Anhaltspunkte, die bei der Vertraulichkeit den Schutzbedarf "sehr hoch" haben könnte (z.B. Vermerk "streng vertraulich"). In diesem Falle ist das Schriftstück aus dem Stapel zu nehmen und der Leitung der Poststelle vorzulegen. Die Leitung prüft erneut, ob der Schutzbedarf tatsächlich „sehr hoch“ sein könnte. Ist dies der Fall, ist das Dokument vom Poststellenleiter persönlich der Leiter der zuständigen Organisationseinheit zu übergeben. Es wird nicht gescannt.

Gescannt werden Dokumente mit normalem oder hohem Schutzbedarf.

Sofern die entsprechenden Dokumente wegen ihrer Belegfunktion bereits digitalisiert wurden und in ihrer originalen Papierversion (vor allem bei Dokumenten gemäß Abschnitt 2.4.2) nach der Digitalisierung noch weitere Informationen (z.B. Notizen/Vermerke) auf diesen angebracht werden, die ebenfalls Belegcharakter haben, so werden diese Dokumente nochmals digitalisiert und als weitere Version des ursprünglichen Originalbelegs aufbewahrt. Der Zusammenhang zwischen den verschiedenen Versionen des Belegs wird durch die Ablage im selben Vorgang des Dokumentenmanagementsystems und als Hinweis in einem Metadatenfeld gewährleistet.

Hat der zuständige Mitarbeiter Zweifel am Belegcharakter eines Dokuments, so holt er bei der zuständigen Führungskraft eine entsprechende Auskunft ein.

2.4.2.3 Vorbereitung der zu digitalisierenden Dokumente

Im Vorfeld ist für den Scanbereich eine Anleitung je Organisationseinheit zu erstellen, aus der hervorgeht, welche Dokumentenklassen aus technischen, organisatorischen oder rechtlichen Gründen nicht gescannt werden sollen.

Anhand dieser Anleitungen werden die Stapel in zu scannende und in nicht zu scannende

Eingänge aufgeteilt.

Die nicht zu scannenden Stapel werden als Papierpost der betreffenden Organisationseinheit zugeleitet. Dort ist zu prüfen, ob bei diesen Dokumenten ein Scannen und Importieren in die elektronische Akte tatsächlich unterbleiben kann. Gegebenenfalls muss das entsprechende Dokument der Scanstelle zum Nachscannen zugeleitet werden.

Es wird im Einzelnen geprüft, ob für einen erfolgreichen Scanvorgang Maßnahmen am Dokument erforderlich sind. Als solche kommen beispielhaft in Frage:

- Entheften
- Entklammern
- Glätten

Damit beim Scannen nach Dokumenten und Vorgängen unterschieden werden kann, erfolgt eine Trennung z.B. durch Patchblätter oder Barcodeaufkleber. Als Vorgangstrenner erfolgt z.B. ein Patch-T-Blatt, für die Dokumententrennung ein Patch-2-Blatt. Zudem untersucht der Mitarbeiter, ob z.B. wegen Bildern in Graustufen eine spezielle Einstellung des Scangeräts erforderlich ist (z.B. Helligkeit, Kontrast etc.). Für Dokumente, die nicht gescannt werden, z.B. CDs, USB-Sticks und Belege, die für den Scanner in den Abmaßen zu groß sind, wird ein Beiblatt mit Angaben über die nicht gescannten Objekte anstelle dieser Objekte eingefügt und mitgescannt. Papierdokumente, die wegen des Schutzbedarfes sehr hoch gem. 2.3.1 nicht gescannt werden dürfen, werden entsprechend den Regelungen der jeweiligen Postordnung / Geschäftsordnung in den Geschäftsgang gegeben.

2.4.3 Scannen

Der zuständige Mitarbeiter meldet sich mit seiner personenbezogenen Kennung ohne Administratorrechte an dem Scancomputer an und startet die Scansoftware _____. Der Mitarbeiter darf keine Profileinstellungen oder Voreinstellungen in der Scansoftware ändern können.

Vor der Digitalisierung prüft der zuständige Mitarbeiter, ob alle erforderlichen Hard- und Softwarekomponenten betriebsbereit sind und die vorgegebenen Grundeinstellungen am Digitalisierungsgerät eingestellt sind.

Vorab ist die geeignete Farbeinstellung zu wählen. Die Farbeinstellung scharz-weiß ist nur zulässig, wenn auf den Papieroriginalen keine Informationwerte durch Farben enthalten sind (wie z.B. bei unterschiedlich farbig gestalteten Plänen). Ein farbiges Logo dürfte dagegen in der Regel im Schwarz-Weiß-Modus gescannt werden.

Der Beginn des Digitalisierungsvorgangs besteht im Auflegen des Papierstapels auf das Digitalisierungsgerät.

Die Grundeinstellungen für die Digitalisierung sind in der Anlage Scansystem definiert.

[Beschreibung des Scanablaufs]

Beispiel:

Während des Scanvorgangs öffnet sich ein Fenster. Dort sind die Postart und das Dezernat auszuwählen. Bei Postart wird unterschieden in „Ministerpost“ und „Normal“. Bei der Ministerpost wird anschließend kein Dezernat ausgewählt. Beim Feld Dezernat muss im Folgefeld das dem Belegstapel entsprechende Dezernat ausgewählt werden.

Bereits während des Scanvorgangs werden die gescannten Dokumente auf dem Bildschirm angezeigt. Hierbei erfolgt die erste Sichtkontrolle auf Auffälligkeiten (z.B. schwarze Seiten).

Werden Maßnahmen getroffen, die auf Erhöhung der Lesbarkeit zielen, zB. Veränderung des Kontrastes/der Helligkeit, Farbreduktionen, Beschneiden, Rauschunterdrückung etc., sind diese zu protokollieren.

Es muss sichergestellt werden, dass nur Leerseiten gelöscht werden. Nicht als Leerseiten erkannte Leerseiten müssen manuell gelöscht werden können. Dabei dürfen Seiten ohne Text aber mit einer Seitennummerierung nicht als Leerseite gelöscht werden.

Beispiel:

Nachdem der Scanvorgang abgeschlossen ist, wird als zweiter Kontrollschritt die automatische Leerseitenerkennung überprüft. Hierbei gibt es die Möglichkeit, die Löschmarkierung für nicht erkannte Leerseiten zu setzen oder die Löschmarkierung bei fälschlich als Leerseiten erkannten Dokumente zu entfernen.

Nicht gut lesbare Seiten (z.B. Graustufen-Fotos, die im Schwarz-Weiß-Modus gescannt wurden) können mit der Funktion "Ersetze Blatt" mit dem Scanverfahren Farbe (b) ersetzt werden.

Etwaige Auffälligkeiten während des Scanprozesses können für jedes Dokument getrennt in einer Infozeile eingetragen werden. Diese Infozeile wird später in das Transferprotokoll übertragen.

Mit der Funktion "Fertig stellen" werden die zum Löschen markierten Seiten und die erkannten Trennblätter entfernt und ins PDF-Format konvertiert.

Abschließend erfolgt die Qualitätssicherung. Der Mitarbeiter überprüft mindestens 3 % der eingescannten Belege auf bildliche und inhaltliche Übereinstimmung des Digitalisats mit dem Papierdokument. Die Prüfquote wird systemseitig eingestellt.

Sofern die Qualitätsüberprüfung ohne Beanstandungen erfolgt ist, wird automatisiert ein Transfervermerk erstellt. Dieser beinhaltet mindestens die unter 2.4.6 aufgeführten Merkmale.

Sofern eine Abweichung bei der Überprüfung auf bildliche und inhaltliche Übereinstimmung festgestellt wird, muss diese Abweichung dokumentiert und an eine unter 3.2.3.1 aufgeführte

Person gemeldet werden, damit eine Fehlersuche begonnen werden kann. Solange der Grund für die Abweichung nicht gefunden und für die Zukunft ausgeschlossen wurde, muss eine 100%-Prüfung auf bildliche und inhaltliche Übereinstimmung des Digitalisats mit dem Papierdokument erfolgen.

Vor dem automatisierten Import in das nachgelagerte System müssen die gescannten Dokumente jeweils mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz oder mit einem Behördensiegel nach der EIDAS-Verordnung versehen werden.

Der Import erfolgt anschließend automatisch.

Nach erfolgreichem Import werden die Digitalisate auf dem Scan-PC sowie der Cache des Scanners gelöscht.

2.4.4 Zwischenlagerung der Papierdokumente

Nach dem Scanvorgang werden die Papieroriginale vollständig und in unveränderter Ordnung zum Zwecke der Kontrolle und der weiteren Behandlung im Raum ____ gegen unbefugten Zugriff gesichert abgelegt. Dies erfolgt in einem festgelegten, nachvollziehbaren Ordnungssystem. Dieses stellt eine jederzeitige Auffindbarkeit des Belegs sicher.

> Beispiel:
>
> Als Indexsystem wird dabei ein numerisches System verwendet. Die Nummer besteht immer aus dem Tagesdatum, Name des Scanners und der Stapelnummer und wird beim Scanvorgang direkt auf die Rückseite gedruckt.

Sofern ein zwischengelagerter Papierbeleg von der bearbeitenden Stelle angefordert wird, wird dieser Papierbeleg gegen ein Platzhalterblatt mit der Aufschrift des Imprints und der Person, die den Beleg angefordert hat, getauscht und das Original der anfordernden Person zugeleitet.

2.4.5 Nachbearbeitung der Scanprodukte

Durch systemseitige Einstellungen zur weiteren Verwendung des Digitalisats wird sichergestellt, dass nur zulässige Kompressionsverfahren im Importprozess verwendet werden (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).

2.4.6 Integritätssicherung

Die Integrität der digitalen Beleg-Kopie mit dem Papieroriginal wird durch das Erstellen eines Transferprotokolls mit der Dokumentation folgender Merkmale sichergestellt:

- Ersteller des Scanproduktes,
- technisches und organisatorisches Umfeld des Erfassungsvorganges,

- etwaige Auffälligkeiten während des Scanprozesses,
- Zeitpunkt der Erfassung
- Ergebnis der Qualitätssicherung
- der Bestätigung der bildlichen und inhaltlichen Übereinstimmung mit dem Papieroriginal

Das Transferprotokoll wird in das PDF/A-Dokument eingebettet und anschließend mittels qualifizierter elektronischer Signatur bzw. Behördensiegel gegen Manipulation gesichert.

2.4.7 Aufbewahrung der Scanprodukte

Die digitalisierten Belege werden unter Verwendung der in Abschnitt 2.5 beschriebenen Systeme bis [zum Ende der Aufbewahrungszeit] aufbewahrt. Die Verfügbarkeit, Auffindbarkeit und Lesbarkeit wird durch folgende Maßnahmen sichergestellt:

- Die elektronischen Dokumente werden zum Abschluss des Scanablaufes mit einer qualifizierten elektronischen Signatur oder einem Behördensiegel versehen und anschließend automatisiert in das nachgelagerte System importiert. Im Rahmen der Posteingangsbearbeitung muss eine Zuordnung der Eingangsdokumente zu dem korrekten Vorgang vorgenommen werden. Dabei müssen beschreibende Metadaten zum Dokument vergeben werden.
- Die Dokumente können dann über das katalogweise Durchsuchen des Aktenbestandsverzeichnisses oder über die in der Elektronischen Akte integrierte Dokumentensuche anhand eine Volltextrecherche und / oder eine Metadatensuche aufgefunden werden.
- Innerhalb der Elektronischen Akte werden Änderungen eines Dokumentes (soweit möglich) immer als neue Dokumentenversion abgespeichert. Es ist somit immer gewährleistet, auf die ursprüngliche signierte Version zugreifen zu können.

2.4.8 Re-Scan fehlerhafte Dokumente

Bei der Bearbeitung der elektronischen Posteingangsdokumente in den Organisationseinheiten könnten Dokumente als fehlerhaft erkannt werden, die ein Re-Scan des Originaldokuments erforderlich machen. Da zu jedem elektronischem Dokument eine Nummer als Indexsystem in den Metadaten mitgeführt wird, ist die Recherche des Papieroriginals mit wenig Aufwand möglich. Wurde das Papieroriginal ausnahmsweise bereits an die Organisationseinheit weitergeleitet, muss auch das Papieroriginal zusätzlich an den Scanbereich gegeben werden.

Die Mitarbeiter des Scanbereichs können anhand des Imprints die chronologisch abgelegten Originaldokumente durchsuchen und das Dokument erneut einscannen.

2.4.9 Vernichtung des Papieroriginals

Unter Beachtung der Mindestaufbewahrungsfristen gem. Nr. 6 der Verwaltungsvorschrift Ersetzendes Scannen erfolgt die Vernichtung der digitalisierten Papieroriginale (außer der unter 2.3.2 genannten Papierbelege) in regelmäßigen Abständen.

Beispiel:

> Die Vernichtung der digitalisierten Papieroriginale erfolgt monatlich für alle Papierbelege mit einem Alter von über drei Monaten.

In keinem Falle erfolgt eine Vernichtung vor dem Durchlaufen aller in 2.4.1 bis 2.4.7 dargestellten Verfahrensschritte.

Bei der Vernichtung werden datenschutzrechtliche Aspekte berücksichtigt, indem alle Belege unter Beachtung der Mindeststandards der DIN66399, Schutzklasse 2, mindestens Sicherheitsstufe 3 zerstört werden, damit der Originalzustand nicht mehr hergestellt werden kann. Sie wird vom zuständigen Mitarbeiter autorisiert und überwacht oder selbst durchgeführt.

Werden Unterlagen durch externe Dritte als "Datenverarbeitung im Auftrag" vernichtet, ist die gesamte Handhabung und Sicherung der Unterlagen zwischen der Übergabe und dem Abschluss der Vernichtung vertraglich festzulegen. Dabei sind die Mindeststandards der DIN66399, Schutzklasse 2, mindestens Sicherheitsstufe 3 einzuhalten. Es müssen der Transport, eine eventuell erforderliche Zwischenlagerung, der Vernichtungsort und der höchstzulässige Zeitraum zwischen der Übergabe der Unterlagen sowie dem Abschluss der Vernichtung geregelt sein. Weiter ist schriftlich festzulegen, in welchem Zustand sich die Unterlagen zu befinden haben, um als vernichtet gelten zu können. Durch den Auftragnehmer ist zu gewährleisten, dass Unbefugte keine Kenntnis der in den Unterlagen gespeicherten Daten erhalten können. Die Übergabe von Unterlagen an das Auftragsunternehmen sollte quittiert werden und die Durchführung jeder Vernichtungsaktion sollte schriftlich bestätigt werden. Die Erteilung von Unterauftragsverhältnissen ist auszuschließen.

2.5 Das Scansystem

2.5.1 Anlage Scansystem

Das Scansystem umfasst die in der Anlage Scansystem aufgeführten Hardware- und Softwarekomponenten zur Digitalisierung und Integritätssicherung. Die Anlage Scansystem ist zu versionieren und ständig zu aktualisieren.

2.5.2 Aufbewahrung der Digitalisate

Die Digitalisate werden dem nachgelagerten System übergeben. Die ordnungsgemäße Aufbewahrung bis zur Aussonderung, also bis zur Archivierung oder Vernichtung wird über technische, rechtliche und organisatorische Regelungen zum Betrieb der Elektronischen Akte sicher gestellt.

3. Maßnahmen

Die in der Anlage Verantwortlichkeiten aufgeführten Personen sind zur Durchführung der folgenden Verarbeitungsschritte eingewiesen und verantwortlich.

3.1 Organisatorische Maßnahmen

3.1.1 Verantwortlichkeiten und Regelungen

3.1.1.1 Dokumentenvorbereitung

3.1.1.2 Scannen

3.1.1.3 Nachverarbeitung

Die Nachverarbeitung umfasst insbesondere die Vollständigkeits-/Lesbarkeits- und Plausibilitätskontrolle.

3.1.1.4 Integritätssicherung

3.1.1.5 Geeignete Aufbewahrung der Digitalisate

3.1.1.6 Vernichtung des Papieroriginals

Die Freigabe zur Vernichtung der Papieroriginale erfolgt durch Zeitablauf.

Die Löschung der Digitalisate nach Ablauf der Aufbewahrungsfrist wird in den nachgelagerten Systemen geregelt.

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:

3.1.2.1 Die Festlegung der Verantwortlichkeiten

Die Festlegung der Verantwortlichkeiten für die Beauftragung, Durchführung und ggf. Kontrolle von Wartungs- und Reparaturaufgaben obliegt der für den IT-Betrieb zuständigen Organisationseinheit.

3.1.2.2 Regelungen zur Authentisierung

Regelungen zur Authentisierung und zum Nachweis der Autorisierung des Wartungspersonals werden von Mitarbeitern der für den IT-Betrieb zuständigen Organisationseinheit.

3.1.2.3 Die Dokumentation von sicherheitsrelevanten Veränderungen

Die Dokumentation von sicherheitsrelevanten Veränderungen an den involvierten IT-Systemen und Anwendungen erfolgen durch die für den IT-Betrieb zuständige Organisationseinheit.

3.1.2.4 Dokumentation der Qualitätskontrolle

Die Dokumentation der erfolgreichen Durchführung der Maßnahmen zur Qualitätskontrolle

und Freigabe vor der Wiederaufnahme des regulären Betriebs erfolgt durch Mitarbeiter der für den IT-Betrieb zuständigen Organisationseinheit.

3.1.3 Abnahme- und Freigabe-Verfahren für Hardware und Software

Durch die ordnungsmäßige und ununterbrochene Nutzung der in Abschnitt 2.5 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

Zuständig für die Einhaltung der Informationssicherheit im Scanprozess ist die für den ~~IT-~~ Betrieb zuständige Organisationseinheit.

In angemessenen zeitlichen Abständen (mind. jährlich) erfolgt eine Überprüfung der Wirksamkeit und Vollständigkeit der für die Informationssicherheit beim ersetzenden Scannen vorgesehenen Maßnahmen durch den Informationssicherheitsbeauftragten.

Die Audits werden mindestens alle 4 Jahre durchgeführt. Beim Audit wird die Umsetzung der verschiedenen Maßnahmen der BSI TR-03138 durch einen vom BSI anerkannten Auditor geprüft und in einem Prüfbericht dokumentiert. Die fachliche Kompetenz und Unabhängigkeit für die qualifizierte Durchführung der Audits ist gewährleistet durch Vergabe des Auftrags nach dem Vergaberecht NRW.

Die Ergebnisse dieser Überprüfung werden dokumentiert. Sofern Sicherheitslücken oder andere Probleme gefunden werden, werden entsprechende Korrekturmaßnahmen durchgeführt.

Für die Korrekturmaßnahmen wird ein Zeitplan mit verantwortlichen Mitarbeitern definiert. Die Korrekturmaßnahmen und deren Ergebnisse werden ebenfalls protokolliert.

3.1.5 Aufrechterhaltung des Datenschutzes

Entsprechend den Regelungen des Datenschutzgesetzes NRW hat der behördliche Datenschutzbauftragte die Einhaltung der datenschutzrechtlichen Vorschriften zu überwachen, die mit der Verarbeitung personenbezogener Daten befassten Personen mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen und die Vorabkontrolle durchzuführen.

3.2 Personelle Maßnahmen

3.2.1 Grundlegende Anforderungen

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

Erklärung über Zuverlässigkeit und Verschwiegenheit bei Kenntnisnahme von allen im Scanprozess zur Kenntnis genommenen Angelegenheiten gem. Anlage Verschwiegenheitserklärung.

3.2.2 Verpflichtung der Mitarbeiter

Die im Rahmen der fachlichen Schutzbedarfsanalyse identifizierten und in Abschnitt 2.2 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 die für den IT-Betrieb zuständige Organisationseinheit.

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 der für den IT-Betrieb zuständigen Organisationseinheit 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 _____ gespeicherten Schulungsunterlagen genutzt.

3.2.3.2 Schulung zu Sicherheitsmaßnahmen im Scanprozess

Zuständige Mitarbeiter, die den Scanvorgang durchführen oder verantworten, werden von der für den IT-Betrieb zuständigen Organisationseinheit in geeigneter Weise hinsichtlich der dabei umzusetzenden sowie der implementierten Sicherheitsmaßnahmen geschult. 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 _____ gespeicherten 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 die für den IT-Betrieb zuständige Organisationseinheit [in regelmäßigen Abständen/zuletzt am ...] und umfasst insbesondere:

- Selbständigkeit 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 _____ gespeicherten Schulungsunterlagen genutzt.

3.2.3.4 Sensibilisierung der Mitarbeiter für Informationssicherheit

Zur Einweisung und Sensibilisierung der Mitarbeiter bezüglich der Regelungen zur Informationssicherheit erfolgt für die in Abschnitt 3.1.1 genannten vorbereitenden, digitalisierenden, archivierenden, kontrollierenden, freigebenden und vernichtenden Mitarbeiter eine jährliche Unterweisung in den Digitalisierungs-, Archivierungs- und Vernichtungsprozess. Dies wird in einem Protokoll dokumentiert. 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. Der unterwiesene Mitarbeiter verpflichtet sich explizit zur Einhaltung dieser Verfahrensanweisung.

3.3 Technische Maßnahmen

3.3.1 Grundlegende Sicherheitsmaßnahmen für IT-Systeme

Für die in den Scanprozess involvierten IT-Systeme werden die hierfür im IT-Grundschutz-Kompendium [BSI-GSK] vorgesehenen Sicherheitsmaßnahmen umgesetzt. Die wirksame Umsetzung der Maßnahmen wurde geprüft durch die für den IT-Betrieb zuständige Organisationseinheit.

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 den Betrieb des Scanner-PC in Minimalinstallation ohne Email-Programme oder Internetzugang.

Bei Änderungen in der Infrastruktur muss die Prüfung wiederholt werden. Die Prüfung und das Ergebnis müssen protokolliert werden.

3.3.3 Schutz vor Schadprogrammen

Um einer Infektion durch Schadprogramme vorzubeugen werden die Maßnahmen des IT-Grundschutz-Bausteins B 1.6 (Schutz vor Schadprogrammen) [BSI-B 1.6] berücksichtigt. Dies umfasst insbesondere

- die Auswahl eines geeigneten Viren-Schutzprogramms,
- die Meldung von Schadprogramm-Infektionen,
- die Aktualisierung der eingesetzten Viren-Schutzprogramme und Signaturen
- eine regelmäßige Datensicherung, die regelmäßig und automatisch angestoßen wird.

Sollte trotz dieser Schutzmaßnahmen ein Verdacht auf Schadsoftware bestehen, ist sofort die für den IT-Betrieb zuständige Organisationseinheit zu verständigen.

Anlage Verantwortlichkeiten:

- Die Dokumentenvorbereitung nach 3.1.1.1 wird durchgeführt von: [Name]
- Der Scanvorgang nach 3.1.1.2 wird durchgeführt von: [Name]
- Die Nachverarbeitung nach 3.1.1.3 wird durchgeführt von: [Name]
- Die Integritätssicherung nach 3.1.1.4 wird durchgeführt von: [Name]
- Die Aufbewahrung der Digitalisate nach 3.1.1.5 wird verantwortet von: [Name]
    - Technische Verantwortung: IT.NRW
    - Organisatorische Verantwortung: [Fachorganisationseinheiten und für Organisationsfragen zuständige Einheit]
    - Inhaltliche Verantwortung: [Fachorganisationseinheiten]
- Die Freigabe zur Vernichtung der Papieroriginale nach 3.1.1.6 wird verantwortet von: [Name]
  [Der externe Dienstleister ist von [Name] unter der Registrierungsnummer […] zertifiziert].
- Die Festlegung der Verantwortlichkeiten nach 3.1.2.1 wird verantwortet von [Name]
- Regelungen zur Authentisierung und zum Nachweis der Autorisierung des Wartungspersonals nach 3.1.2.2 wird verantwortet von [Name].
- Die Dokumentation von sicherheitsrelevanten Veränderungen an den involvierten IT-Systemen und Anwendungen nach 3.1.2.3 wird verantwortet von [Name].
- Die Dokumentation der erfolgreichen Durchführung der Maßnahmen zur Qualitätskontrolle und Freigabe vor der Wiederaufnahme des regulären Betriebs nach 3.1.2.4 wird verantwortet von [Name].
- Die Einhaltung der Informationssicherheit im Scanprozess nach 3.1.4 wird verantwortet von [Name].
- Die Verpflichtung der Mitarbeiter nach 3.2.2 wird verantwortet von [Name].
- Die Einweisung zur ordnungsgemäßen Bedienung des Scansystems nach 3.2.3.1 wird verantwortet von [Name].
- Die Schulung zu Sicherheitsmaßnahmen im Scanprozess nach 3.2.3.2 wird veranwortet von [Name].
- Die Schulung des Wartungs- und Administrationspersonals nach 3.2.3.3 wird verantwortet von [Name].
- Die Sicherheitsmaßnahmen nach 3.3.1 werden verantwortet [Name] und wurden zuletzt am [Datum] geprüft.
- Die nach 3.3.2 notwendigen Maßnahmen werden verantwortet [Name] und wurden zuletzt am [Datum] geprüft.
- Die Maßnahmen nach 3.3.3 werden verantwortet von [Name].

Anlage Scansystem:

Beispiel:

1 Digitalisierung

Für die Digitalisierung kommt folgende Hardware zum Einsatz:

- Arbeitsplatz-PC : Intel Core I7-6700 3,4 GHz, 8 GB RAM, Festplatte 256 MB SSD
- Monitor: 24 Zoll 16:9
- Scanner: Kodak i3200

Für die Digitalisierung kommt folgende Software zum Einsatz:

- Betriebssystem: Windows 7 – 64-Bit
- OCR-Software: Abbyy Fionereader OCR Modul 50 K
- Scannersoftware: Crosscap TR-Resiscan

  Grundeinstellungen:

  Zielformat: PDF/A

  Auflösung: 300 dpi

  Farbscan in 24-Bit Farbtiefe

  Automatischer Einzug mit grundsätzlich beidseitigem Scannen. Leerseiten sollen im Rahmen des Scannachbearbeitung entfernt werden.

  Durch systemseitige Einstellungen zur weiteren Verwendung des Digitalisats wird sichergestellt, dass nur zulässige Kompressionsverfahren im Importprozess verwendet werden (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).

2 Integritätssicherung

Direkt vor der Übergabe an die Importschnittstelle werden die digitalen Scanprodukte mit einer qualifizierten elektronischen Signatur oder einem Behördensiegel versehen. Die Integrität der Scanprodukte kann so überprüfbar gemacht werden.

Für die Integritätssicherung der Scanprodukte kommt folgende Hardware zum Einsatz:

Signaturkarten-Lesegerät: Cherry ST-2000
Multisignaturkarte

Anlage Verschwiegenheitserkärung nach 3.2

Bestätigung über die Teilnahme an der
Einweisung über den Datenschutz und die Datensicherheit
im Rahmen der Aufgabenwahrnehmung in der Scanstelle

Name:

Vorname:

Geb.-Datum:

Der/Die Unterzeichner/in bestätigt die Teilnahme an der Einweisung über den Datenschutz und die Datensicherheit im Rahmen der Aufgabenwahrnehmung in der Scanstelle der _____[Behörde] am _____[Datum]

Wesentliche Inhalte der Einweisung waren:

1. Rechtliche Grundlagen des Datenschutzes
2. Regelungen zum Datenschutz im Personalrecht
3. Sicherheitskonzept gem. § 10 Datenschutzgesetz mit Erläuterungen zum hohen Schutzbedarfs des Prozesses „Digitalisierung der Papiereingänge“
4. Verfahrensanweisung zum Ersetzenden Scannen

Der/Die Unterzeichner/in wurde darauf hingewiesen, dass die vorgenannten Regelungen von ihr/ihm anzuwenden sind. Sie/Er erklärt, nunmehr von dem Inhalt der genannten Bestimmungen unterrichtet zu sein. Die Erklärung wird zur Personalakte genommen.

[Ort]_____, den [Datum]_____

_____ _____

(Teilnehmer/-in) (Einweisende/r)

Anlage Spätes Scannen

Gem. Nr. 5 der Verwaltungsvorschrift Ersetzendes Scannen ist in folgenden Fällen ausnahmweise das späte Scannen zugelassen:

Beispiel:

Notifizierungen Dez. 52

Baustellenanzeigen Dez. 56

Glossar

Behördensiegel	Das sogenannte Behördensiegel ist ein EU-weit anerkanntes Signaturwerkzeug für Behörden und andere juristische Personen gemäß eIDAS-Verordnung und weist den Ursprung (*Authentizität*) und die Unversehrtheit (*Integrität*) von Dokumenten sicher nach.
Belegfunktion:	Dokument enthält Informationen, die einer Dokumentations- und Aufbewahrungsfrist unterliegen.
BSI-TR03138	(TR-RESISCAN) Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in der „BSI TR-03138 RESISCAN“ Vorgaben für das ersetzende Scannen festgeschrieben. Die technische Richtlinie bietet eine gute Orientierung für die Erstellung beweiskräftiger Digitalisate.
Digitalisat:	Das Endprodukt einer Digitalisierung besteht aus einer oder mehreren Dateien, die (in Anlehnung an Begriffsbildungen wie *Kondensat* oder *Korrelat*) Digitalisat genannt werden.
DIN 66399	Die DIN 66399 spezifiziert drei Schutzklassen, nach denen die Datenträger hinsichtlich ihrer Schutzbedürftigkeit bei der Datenträger-Vernichtung einzuordnen sind.
Dokumentenklassen	Eine Dokumentenklasse beschreibt im Dokumentenmanagement und bei der elektronischen Archivierung Gruppierungen von Dokumenten mit gleichen Attributen oder Inhalten. Typische Attribute von Dokumentenklassen sind Ordnungskriterien, Berechtigungen, Speicherorte, Aufbewahrungsfristen, etc.
Imprint	Mit dem vom Scanner auf das Papier gedruckten Imprint können Daten aus dem Scanvorgang (z.B. wer hat wann gescannt) sichtbar gemacht werden
Patchblatt	Patchblätter enthalten vom Scanner auslesbare Barcodes. Mithilfe unterschiedlicher Patchblätter kann gesteuert werden, wann im Scanstapel ein neues Dokument oder z.B. auch ein neuer Vorgang beginnt.
PDF/A-Dokument	**PDF/A** ist ein Dateiformat zur Langzeitarchivierung digitaler Dokumente, das von der International Organization for Standardization (ISO) als Teilmenge des Portable Document

Format (PDF) genormt wurde. Die Norm legt fest, wie die Elemente der zugrundeliegenden PDF-Versionen im Hinblick auf die Langzeitarchivierung verwendet werden müssen. Dabei gibt es sowohl zwingend vorgeschriebene als auch nicht zugelassene Bestandteile.

Schutzbedarfskategorie: Zweck der Schutzbedarfsfeststellung ist es zu ermitteln, welcher Schutz für die Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen können. Wichtig ist dabei auch eine realistische Einschätzung der möglichen Folgeschäden. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch".