SEESTADT BREMERHAVEN

Grundsätze für die Organisation der elektronischen Aktenführung (eAkte)

Verfahrensbeschreibung (Richtlinie) für das ersetzende Scannen bei der Stadtverwaltung

Inkrafttreten am 00.00.0000

Zertifikat seit 2007
audit berufundfamilie

Magistrat der Stadt Bremerhaven
Magistratskanzlei
Postfach 21 03 60
27524 Bremerhaven

BREMERHAVEN
MEER ERLEBEN!

Inhalt

1. Einleitung

Ohne elektronische Akten und elektronische Vorgangsbearbeitung ist eine konsequente Verwaltungsmodernisierung nicht möglich. In der Praxis bestehen jedoch erhebliche Unsicherheiten, wie Papieroriginale nach dem heutigen Stand der Technik rechtskonform in elektronische Dokumente überführt werden können.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat eine *Technische Richtlinie zum Ersetzenden Scannen (TR RESISCAN)* herausgegeben. Basis für das beweiswerterhaltende Scannen ist eine Verfahrensbeschreibung für den Prozess des ersetzenden Scannens und die Durchführung einer Schutzbedarfsanalyse für die zu scannenden Papieroriginale.

Diese Verfahrensbeschreibung befasst sich mit der ordnungsgemäßen Digitalisierung von Dokumenten mit dem Ziel der Aufrechterhaltung der Beweiskraft des Digitalisats im Vergleich zum Papieroriginal. Sie benennt sicherheitsrelevante Maßnahmen, die beim (rechtskonformen) ersetzenden Scannen in der Stadtverwaltung zu gewährleisten sind. Darüber hinaus haben alle Organisationseinheiten eine ergänzende Verfahrensbeschreibung für den eigenen Zuständigkeitsbereich zu erstellen.

Betrachtet werden nur die von der Behörde selbst durchgeführten Scanprozesse. Bei der Beauftragung externer Dienstleister müssen besondere Rahmenbedingungen beachtet werden, auf die an dieser Stelle nicht eingegangen wird; hierfür sind eigenständige Regelungen zu erstellen.

Die hier beschriebenen Maßnahmen und Verfahren sind von allen beteiligten Beschäftigten und Organisationseinheiten zu befolgen; die Leitungen der Organisationseinheiten haben dies sicherzustellen. Jede/-r an einem Prozess-Schritt Beteiligte/-r ist unterwiesen und autorisiert.

Es sind alle Wege auszuschöpfen, um die Dokumente auf elektronischem Wege zu erhalten und so den ersetzenden Scanprozess zu vermeiden.

2. Ersetzendes Scannen

2.1 Organisatorisches Umfeld

Die jeweils zuständigen Organisationseinheiten definieren und dokumentieren in eigenen Verfahrensbeschreibungen die Gründe für die Notwendigkeit des ersetzenden Scannens mit Darstellung der organisatorischen Strukturen, in denen das ersetzende Scannen durchgeführt werden soll; die zuständigen Mitbestimmungsgremien sind hierbei einzubeziehen.

2.1 Rechtliches Umfeld

Es sind sowohl spezielle Normen als auch einschlägige Grundprinzipien, wie z.B. die der Aktenhaltung und des Datenschutzes zu beachten. Die etwaigen speziellen Normen sind in der jeweiligen ergänzenden Verfahrensbeschreibung für das ersetzende Scannen der Stadtverwaltung anzugeben.

2.2 Schutzbedarfskategorien

Die KGSt[1] und Vitako[2] gehen davon aus, dass alle deutschen Kommunen überwiegend über den gleichen Dokumentenbestand verfügen und somit den gleichen schriftgutbezogenen Gesetzen und Anforderungen unterliegen. Durch die KGSt wurde daher eine Schutzbedarfsanalyse für typische kommunale Dokumentenarten durchgeführt, mit dem Ergebnis, dass in der Kommunalverwaltung regelmäßig von der **Schutzbedarfskategorie „normal“** auszugehen ist.

Demnach werden die bei der Stadtverwaltung eingehenden Dokumente grundsätzlich der

[1] Kommunale Gemeinschaftsstelle für Verwaltungsmanagement
[2] Bundes-Arbeitsgemeinschaft der kommunalen IT-Dienstleister e.V.

Schutzbedarfskategorie „normal“ zugeordnet. Die Schadensauswirkungen sind begrenzt und überschaubar. Nur wenn aufgrund besonderer Vorschriften (z.B. bei Gesundheitsdaten) ein erweiterter Schutz notwendig ist, werden besondere Standards empfohlen. Eine Einstufung der Originale in die Kategorie „sehr hoch“ findet für Dokumente der Kommunalverwaltungen erfahrungsgemäß nicht statt. Die zuständige Organisationseinheit führt eine Schutzbedarfsanalyse durch. Sind Dokumente einer höheren Schutzbedarfskategorie zu zuordnen, werden besondere Regelungen in der jeweiligen Organisationseinheit getroffen.

2.3 Verarbeitete Dokumente

Digitalisiert werden originär in Papierform vorliegende bzw. eingehende Dokumente, die eine Belegfunktion erfüllen und deshalb einer Dokumentations- und Aufbewahrungspflicht unterliegen.

Aktenrelevant und somit der Dokumentations- und Aufbewahrungspflicht unterliegend sind alle Dokumente, die erforderlich und geeignet sind, die getroffenen Entscheidungen sowie den maßgeblichen Entscheidungsprozess einschließlich der beteiligten Stellen jederzeit nachvollziehbar und überprüfbar zu machen.

2.4 Nicht zu vernichtende Dokumente

Explizit von der Vernichtung ausgeschlossen sind Dokumente, denen aufgrund ihrer Beweiskraft, öffentlichen Glaubens oder gesetzlicher Bestimmung im Original besondere Bedeutung zukommt, wie z.B. Urkunden, Testate unter Siegelverwendung, Papiere mit fluoreszierenden Original-Stempeln auch wenn sie verarbeitet werden. Bei einer Durchsicht vor der Vernichtung werden sie ausgesondert und geordnet archiviert. Für diese Dokumente erfolgt eine papierbasierte Aufbewahrung des Originaldokuments nach den entsprechenden Regelungen.

2.5 Der Scanprozess

Der Prozess für das ersetzende Scannen umfasst folgende Schritte:

- Eingang des Dokuments,
- Dokumentenvorbereitung der Papieroriginale,
- Scannen der Papieroriginale,
- Nachverarbeitung der Digitalisate,
- Integritätssicherung[3] der Dokumente,
- Aufbewahrung der Digitalisate und
- Vernichtung der Papieroriginale.

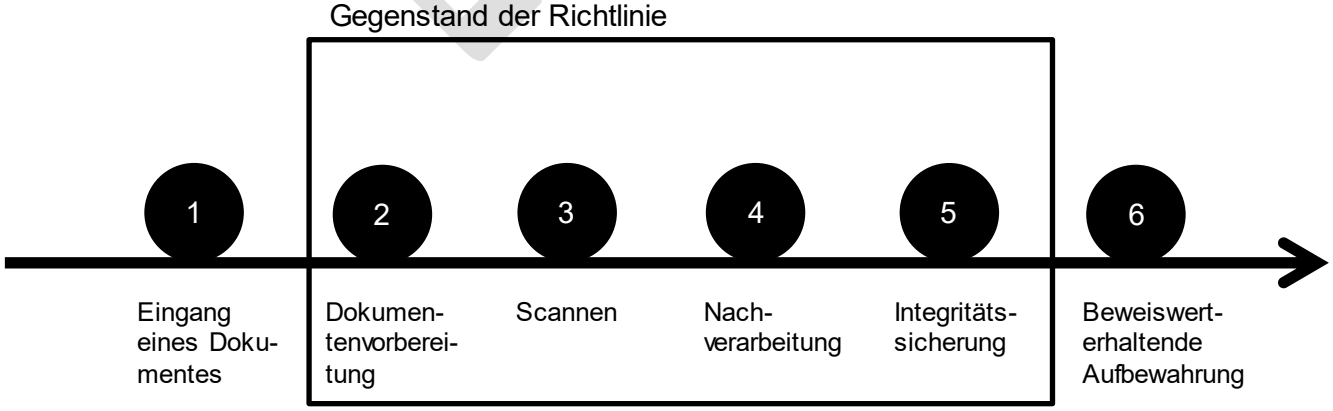

Abb. 1: Prozess (in Anlehnung an TR-RESISCAN)

[3] vgl. Punkt 2.5.5. dieser Richtlinie

2.5.1 Eingang des Dokuments

Der Scanprozess beginnt mit dem Eingang des Papierdokumentes in den jeweiligen Organisationseinheiten.

2.5.2 Dokumentenvorbereitung

2.5.2.1 Vorsortierung mit Prüfung

Bei der Sichtung der Posteingänge bzw. der vorgelegten Dokumente erfolgt eine Prüfung auf Vollständigkeit und Unversehrtheit der Eingangspost. Liegen Zweifel vor, wird das Verfahren bzgl. der betroffenen Dokumente beendet und von einer weiteren Bearbeitung vorläufig abgesehen. Es erfolgt eine Rücksprache mit der zuständigen Stelle und bei Bedarf dem Absender des Dokuments.

2.5.2.2 Identifikation der zu scannenden Belege (rechtliche und faktische Prüfung)

Die Eingangspost wird hinsichtlich des Belegcharakters der einzelnen Dokumente von den zuständigen Beschäftigten geprüft. Dabei werden alle zu erfassenden Dokumente für die anschließende Digitalisierung identifiziert.

Besondere Regelungen (Negativliste für z.B. Werbung, Kataloge etc.) können in den jeweils zuständigen Organisationseinheiten getroffen werden.

Sofern Dokumente wegen ihrer Belegfunktion bereits digitalisiert wurden und in ihrer originalen Papierversion 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 Versionierungsfunktion der eingesetzten Software oder auf manuellem Wege gewährleistet.

Haben die zuständigen Beschäftigten Zweifel am Belegcharakter eines Dokuments, so holen sie bei der zuständigen Stelle eine entsprechende Auskunft ein.

2.5.2.3 Vorbereitung der zu digitalisierenden Dokumente (technische Prüfung)

Alle für eine Digitalisierung identifizierten Belege werden durch die zuständigen Beschäftigten daraufhin geprüft, ob eine Digitalisierung des Dokuments technisch möglich ist und ein originalgetreues Abbild erzeugt werden kann.

Die zuständigen Beschäftigten prüfen, ob für einen erfolgreichen Scanvorgang vorherige Maßnahmen am Dokument erforderlich sind. Als solche kommen beispielhaft in Frage:

- Lösen von Klammern,
- sorgfältiges Sortieren, um die Reihenfolge zu gewährleisten,
- ordnungsgemäße Trennung der Dokumente oder
- Aufbereiten von Dokumenten mit Notiz- und/oder Klebezetteln in eine Form, die dem Digitalisierungsgerät zugeführt werden kann.

2.5.3 Scannen

Der Digitalisierungsvorgang beginnt mit der Zuführung der Dokumente durch die zuständigen Beschäftigten in das Digitalisierungsgerät. Der Digitalisierungsvorgang endet mit der Ausgabe des digitalen Mediums in die eingesetzte Software.

Vor der Digitalisierung ist zu prüfen, ob alle erforderlichen Hard- und Softwarekomponenten betriebsbereit sind und die vorgegebenen Grundeinstellungen am Digitalisierungsgerät eingestellt sind (Scanprofil). Die Einstellungen für die zu verwendenden Digitalisierungsgeräte sind der Verfahrensbeschreibung der jeweiligen Organisationseinheit zu entnehmen. Je nach

Ausprägung des jeweiligen Scanprozesses kann es gegebenenfalls für das gleiche Gerät dokumentenabhängig mehrere Scanprofile geben.

Dadurch wird sichergestellt, dass keine unzulässigen Kompressionsverfahren eingesetzt werden. Unzulässige Kompressionsverfahren sind der technischen Richtlinie BSI TR-03138 (TR-RESISCAN) zu entnehmen.

Der Zugriff auf das Digitalisat wird durch das Rollen- und Berechtigungskonzept der Organisationseinheit geregelt.

Liegen Papieroriginale in Spezialformaten vor, so erfolgt eine Weiterleitung an eine mit entsprechender Technik ausgestattete und für ersetzendes Scannen autorisierte Scanstelle.

2.5.4 Nachverarbeitung

Die zuständigen Beschäftigten überprüfen stichprobenartig unmittelbar im Anschluss an den Digitalisierungsvorgang die Vollständigkeit und Lesbarkeit des Digitalisats und nehmen gegebenenfalls Korrekturen vor. Je höher die festgestellte Fehlerquote ausfällt, desto häufiger werden Stichproben durchgeführt.

Durch technische und organisatorische Maßnahmen ist eine nachträgliche Veränderung des Digitalisats ausgeschlossen.

Bei der nachbereitenden Qualitätssicherung sind die Anforderung von Originalbelegen bzw. ein erneutes Scannen technisch und/oder organisatorisch geregelt.

2.5.5 Integritätssicherung

Die Integrität und Verkehrsfähigkeit der Digitalisate im Vergleich zum Papieroriginal wird durch Anwendung technischer und organisatorischer Maßnahmen abgesichert und gewährleistet. (Vgl. 3.1 und 3.3)

2.5.6 Aufbewahrung und Archivierung

Für digitalisierte Dokumente gelten die gleichen Regelungen wie für Papierdokumente, z.B. Aufbewahrung und Archivierung.

2.5.7 Vernichtung des Originals

Die Vernichtung der digitalisierten Papierbelege erfolgt nach Ablauf der Vorhaltefrist in einem zeitlich festgelegten Turnus. Die Vorhaltefrist ist der Zeitraum, in dem ein erneuter Digitalisierungsvorgang angestoßen werden kann. Die Dauer der Vorhaltefrist wird durch die zuständige Stelle festgelegt. Die für die Aufbewahrung des Papiers zuständige Stelle autorisiert und initiiert die Vernichtung nach festgelegten Vorgaben (Datenschutz). In keinem Falle erfolgt eine Vernichtung vor dem Durchlaufen aller in der vorliegenden Verfahrensbeschreibung dargestellten Schritte.

Bei der Vernichtung werden datenschutzrechtliche Aspekte berücksichtigt. Müssen Originale vor allem aus rechtlichen Gründen als Papierbeleg aufbewahrt werden, erfolgt die Ablage in Papierrumpfakten (Hybridakte).

Die Originaldokumente sollen so kurz wie möglich aufbewahrt werden.

2.6 Das Scansystem

Die Software für die Digitalisierung, Integritätssicherung und Aufbewahrung der digitalisierten Belege wird in einer geeigneten Systemumgebung gemäß der Richtlinie zur Informationssicherheit für das Magistratsnetz betrieben. Die für die Systemumgebung verwendeten Komponenten unterliegen der eigenverantwortlichen Aufsicht und Pflege der zuständigen Organisationseinheit, wobei die Rahmenbedingungen für den Betrieb von Geräten, Software und

Netzen der Datenverarbeitung gemäß der Richtlinie zur Informationssicherheit für das Magistratsnetz eingehalten werden. Eigenerklärungen zur Konformität sind hinreichend.

3. Maßnahmen

3.1 Technische Maßnahmen

Die grundlegenden technischen und organisatorischen Maßnahmen zur Gestaltung der Informationssicherheit im Bereich des Magistrats sind in der Richtlinie zur Informationssicherheit für das Magistratsnetz (IT-Sicherheitsrichtlinie) verankert. Die IT-Sicherheitsrichtlinie gilt für alle Organisationseinheiten des Magistrats sowie für die Wirtschaftsbetriebe und Anstalten des öffentlichen Rechts der Stadt Bremerhaven, soweit sie an das Verwaltungsnetz angeschlossen sind. Durch sie werden Vorgaben zur Umsetzung einer adäquaten IT-Sicherheit definiert und sie basiert auf der gegenwärtigen technischen Infrastruktur. Eine zeitnahe Anpassung bei technischen Änderungen ist durch regelmäßige Überprüfungen sichergestellt.

Als weiterer Baustein der technischen und organisatorischen Maßnahmen ist das Sicherheitskonzept für den Netz- und Serverbetrieb des Magistrats der Stadt Bremerhaven zu betrachten. In diesem Konzept werden einerseits die Sicherheitsmechanismen zur Gewährleistung einer hohen Verfügbarkeit, Vertraulichkeit und Integrität der Netzinfrastruktur beschrieben und andererseits die Serveradministration und der Betrieb des Rechenzentrums detailliert beschrieben.

3.2 Organisatorische Maßnahmen

3.2.1 Verantwortlichkeiten und Regelungen

Die Dokumentenvorbereitung, der Digitalisierungsvorgang, die Nachverarbeitung, die Integritätssicherung, die geeignete Aufbewahrung der Dokumente und die Freigabe zur Vernichtung der Dokumente werden von den jeweils befugten Stellen durchgeführt.

3.2.2 Regelungen für Wartungsarbeiten

Die Wartung der für den Scanvorgang eingesetzten IT-Systeme und Anwendungen wird von der zuständigen Organisationseinheit eigenverantwortlich durchgeführt; ggf. ist der Betrieb für Informationstechnologie BIT zu beteiligen.

Externes Personal zur Lösung von Hardware- und Softwareproblemen oder Dienstleister für die eingesetzte Software erhalten im Rahmen der IT-Sicherheitsrichtlinie nur Zugang zu den entsprechenden Systemen, wenn dies unter Begleitung der zuständigen und verantwortlichen Organisationseinheit stattfindet. Änderungen an den Systemen, die sich auf diese Verfahrensbeschreibung auswirken können, werden dokumentiert. Die zuständigen Mitbestimmungsgremien sind hierüber zu informieren.

3.2.3 Lesbarmachung

Es 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.

3.2.4 Aufrechterhaltung der Informationssicherheit im Scanprozess

In angemessenen zeitlichen Abständen erfolgt eine Überprüfung der Wirksamkeit und Vollständigkeit der für die Informationssicherheit beim ersetzenden Scannen vorgesehenen Maßnahmen. Wer diese Überprüfung durchführt, wird den einzelnen Organisationseinheiten überlassen.

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

Für die Korrekturmaßnahmen wird ein Zeitplan mit den zuständigen Beschäftigten definiert. Detaillierte Festlegungen finden sich im jeweiligen Protokoll.

3.2.5 Anforderungen beim Outsourcing des Scanprozesses

Im Falle einer Durchführung des Scanprozesses durch eine externe Stelle ist eine gesonderte Verfahrensbeschreibung unter der Beteiligung der zuständigen Mitbestimmungsgremien zu erstellen.

3.3 Personelle Maßnahmen

3.3.1 Verpflichtung der Beschäftigten

Die im Rahmen der fachlichen Schutzbedarfsanalyse identifizierten Rahmenbedingungen werden den in den Scanprozess involvierten Beschäftigten der Organisationseinheit zur Kenntnis gebracht. Die Beschäftigten werden auf die Einhaltung der einschlägigen Gesetze, Vorschriften, Regelungen und der Verfahrensbeschreibung verpflichtet. Diese Verpflichtung ist zwingend durchzuführen und zu dokumentieren.

Diese Verpflichtung wird von der für die Beschäftigten zuständigen Organisationseinheit umgesetzt.

3.3.2 Maßnahmen zur Qualifizierung und Sensibilisierung

Die Beschäftigten, die den Scanvorgang durchführen, werden durch die jeweils zuständige Organisationseinheit hinsichtlich der eingesetzten Geräte, Anwendungen und sonstigen Abläufe regelmäßig unterwiesen. Dies umfasst insbesondere

- die grundsätzlichen Abläufe im Scanprozess einschließlich der Dokumentenvorbereitung[4], dem Scannen[5], der zulässigen Nachverarbeitung[6] und der Integritätssicherung[7],
- Anforderungen hinsichtlich der Qualitätssicherung im Rahmen der Nachverarbeitung
- die Konfiguration und Nutzung der Scansysteme zur Integritätssicherung und
- das Verhalten im Fehlerfall,
- das Verhalten in Verdachtsfällen bezüglich der Echtheit der Dokumente
- den Umgang mit personenbezogenen und anderen sensiblen Daten im Rahmen der Datenschutzgrundverordnung (DSGVO), des Bundesdatenschutzgesetzes (BDSG) und des Bremischen Ausführungsgesetzes zur Datenschutzgrundverordnung (BremDSGVOAG)

[4] Punkt 2.5.2 der Richtlinie zum ersetzenden Scannen der Stadtverwaltung
[5] Punkt 2.5.3 der Richtlinie zum ersetzenden Scannen der Stadtverwaltung
[6] Punkt 2.5.4 der Richtlinie zum ersetzenden Scannen der Stadtverwaltung
[7] Punkt 3.1 und 3.2 der Richtlinie zum ersetzenden Scannen der Stadtverwaltung