

Gemeinsames Positionspapier
der kommunalen Spitzenverbände in Nordrhein-Westfalen zur
Thematik der digitalen Archivierung,
insbesondere zur Einrichtung elektronischer Langzeitarchive

A. Ausgangslage

Die Thematik der digitalen Archivierung – der Umgang mit sog. „borndigitals“ aus Verwaltungsfachverfahren oder DMS sowie Digitalisaten – beschäftigt die kommunalen Spitzenverbände in Nordrhein-Westfalen schon seit einigen Jahren. Bereits heute geschieht die Aufgabenerledigung in den meisten kommunalen Verwaltungen ganz oder in großen Teilen auf elektronischem Wege, angefangen vom Meldewesen über das neu geregelte Personenstands- und Katasterwesen sowie das Gewerberegister bis hin zur elektronischen Aktenführung in komplexen Vorgangsbearbeitungs- und Dokumenten-Management-Systemen. Dabei gelten bereits für die Erzeugung und Ablage elektronischer Daten in der Verwaltung bestimmte Auflagen, so die Gewährleistung von Rechts- und Revisionsicherheit.¹

Die langfristige Sicherung rechtsrelevanter (elektronischer) Unterlagen für die Verwaltung einerseits und für die Bürgerinnen und Bürger andererseits ist Aufgabe der Archive. Gemäß ihrem Auftrag (ArchivG NRW vom 16.03.2010) sorgen sie für eine dauerhafte Transparenz des Verwaltungshandelns, indem sie Archivgut, das aus rechtlicher oder historisch-kultureller Sicht von Bedeutung ist, erhalten und erschließen damit elektronische Unterlagen durch kommunale Archive auf der gesetzlichen Grundlage dauerhaft – das heißt zeitlich unbefristet – gesichert und nutzbar gehalten werden können, sind bestimmte Weichenstellungen unumgänglich. Es müssen elektronische Langzeitarchive vorhanden sein, damit die Archive elektronisches Archivgut sichern, über die notwendigen Metadaten erschließen und der Öffentlichkeit für die Benutzung zugänglich machen können.

Die Thematik der digitalen Archivierung betrifft jedoch über diese archivfachlichen Aspekte hinaus zentrale datenverarbeitungstechnische, verwaltungsorganisatorische und juristische Fragestellungen der kommunalen Verwaltungen. Bis dato wird sie allerdings sowohl von den verschiedenen Verwaltungsebenen – von der kommunalen, über die Landes- und Bundes- bis hin zu europäischen Ebene – sowie den jeweils betroffenen Fachbereichen (Archive, IT, Organisations- und Rechtsämter) vornehmlich im Rahmen von Ein-

¹ Rechtssicherheit bedeutet, dass auch für elektronische Dokumente dauerhaft der Nachweis der Echtheit und Unverfälschtheit ihres Inhalts möglich und ihr zeitlicher und räumlicher Entstehungszusammenhang eindeutig erkennbar sein muss. Revisionsicherheit heißt, dass digitale Dokumente und Datensätze so sicher abgelegt werden müssen, dass sie stets wiederauffindbar sind, vor allem aber nicht verloren gehen oder verändert werden können (Anforderungen entsprechend §§ 146 und 147 AO, §§ 239 und 257 HGB; Grundsätze ordnungsmäßiger DV-Datenverarbeitung-gestützter Buchführungssysteme [GoBS]; Merksätze des Verbandes Organisations- und Informationssysteme [VOI] zur reversionssicheren elektronischen Archivierung). In besonderem Maße gelten diese Anforderungen für bereits jetzt schon oder künftig ausschließlich in elektronischer Form geführte Register, in denen besonders sensible, z. B. personenbezogene Daten gepflegt und vorgehalten werden.

zelinitiativen, jedenfalls ohne erkennbare Gesamtkoordination bearbeitet. Dies soll jedenfalls für den kommunalen Bereich mit Hilfe des vorliegenden Positionspapieres geändert werden.

B. Vorgehensweise

Ausgangspunkt ist die aus archivischer, rechtlicher und verwaltungsorganisatorischer Sicht vordringliche Aufgabe, den drohenden Verlust großer Datenmengen zu verhindern, die seit Jahren in den elektronischen Verwaltungsfachverfahren, Datenbanken und Dokumentenmanagement-Systemen entstehen. Die Erfüllung dieser kommunalen Pflichtaufgabe der gesetzesmäßigen Langzeitarchivierung (ArchivG NRW, weitere rechtliche Vorgaben über elektronische Dokumentation und Aktenführung) ist in der Betrachtung getrennt von der Frage der digitalen Präsentation digitalen Archivguts zu sehen.

Die nordrhein-westfälischen Kommunen wollen sich also zunächst auf die vordringliche Aufgabe der Langzeitarchivierung konzentrieren. Sie schafft erst die notwendigen Voraussetzungen für die Präsentation und Nutzbarmachung von digitalem Archivgut, d. h. der „borndigitals“ und der Digitalisate.

Hinsichtlich der elektronischen Langzeitarchivierung ist eine möglichst einheitliche und praktikable Lösung für die Kommunen in NRW zu finden, die insbesondere das Entstehen von Insellösungen im IT-Bereich vermeidet. Dabei sollte möglichst ein modularer Aufbau angestrebt werden, der bereits bestehende „best-practice“-Beispiele integriert und somit Synergieeffekte erzeugt.

Über einen möglichen einheitlichen Weg für die Präsentation bedarf es zum jetzigen Zeitpunkt noch keiner Entscheidung. Denkbar sind neben einer Mitnutzung von Plattformen wie „archive.nrw.de“ oder des Landesprojektes „Digitales Archiv NRW“ auch eigene kommunale Präsentationslösungen. Jede Lösung sollte jedoch Schnittstellen zu den im Aufbau befindlichen nationalen (DDB) und europäischen Portalen (Europeana) vorsehen.

C. Fachliche Anforderungen an elektronische Langzeitarchive in kommunaler Hoheit

Damit elektronische Unterlagen durch kommunale Archive zeitlich unbefristet gesetzeskonform gesichert und nutzbar gehalten werden können, müssen elektronische Langzeitarchive eingerichtet werden. Als elektronisches Langzeitarchiv werden im Folgenden die technischen (Soft- und Hardware) und organisatorischen Mittel bezeichnet, die es Gemeinden, Städten und Kreisen ermöglichen, den an sie gestellten archivrechtlichen Anforderungen nachzukommen.

Elektronische Langzeitarchive sollten den folgenden fachlichen, organisatorischen und technischen Anforderungen genügen, um den gestellten rechtlichen Anforderungen² nachzukommen:

- Möglichkeit zur Übernahme „elektronischer Aufzeichnungen“ (§ 1 i. V. m. § 10 Abs. 4 ArchivG NRW) und zur Bewertung nach archivfachlichen Kriterien,
- Erhaltung des so entstandenen Archivguts „in seiner Entstehungsform“ (§ 3 i. V. m. § 10 ArchivG NRW)
- Dauerhafte Nutzbarmachung (§ 6 i. V. m. § 10 ArchivG NRW)

Archive müssen „geeignete technische und organisatorische Maßnahmen zur Sicherung solcher Unterlagen [...] ergreifen, die personenbezogene Daten enthalten oder einem besonderen gesetzlichen Geheimnisschutz unterliegen“ (§ 5 i. V. m. § 10 ArchivG NRW).

Verpflichtet werden die „Träger der kommunalen Selbstverwaltung, deren Verbände sowie kommunale Stiftungen“, die für ihr Archivgut in eigener Zuständigkeit Sorge zu tragen haben (§ 10 Abs. 1 ArchivG NRW). In Betracht kommt die Errichtung und Unterhaltung eigener Archive, die Übertragung auf eine für Archivierungszwecke geschaffene Gemeinschaftseinrichtung oder die Übergabe des Archivguts zur Archivierung in einem anderen öffentlichen, nichtstaatlichen Archiv (§ 10 Abs. 2 ArchivG NRW).

Die im Anhang dargestellten Rahmenvorgaben sind dazu bestimmt, diesen gesetzlichen Anforderungen Rechnung zu tragen.

Düsseldorf und Köln, Oktober 2012

² Im Wesentlichen handelt es sich um das Gesetz über die Sicherung und Nutzung öffentlichen Archivguts im Lande Nordrhein-Westfalen (Archivgesetz Nordrhein-Westfalen -ArchivG NRW) vom 16. März 2010.

Anhang

Rahmenvorgaben

1. Ein elektronisches Langzeitarchiv muss sich an den Vorgaben nationaler und internationaler Standards orientieren, um eine langfristige Funktionalität sicher zu stellen. Zentral ist das international anerkannte „Open Archival Information System“-Modell (OAIS, ISO 14721:2003). Dieses Organisationskonzept stellt sicher, dass Fehlbedienungen und ungewollte Löschungen oder Datenkorruption verhindert werden und die Lesbarkeit und Unverändertheit der enthaltenen Objekte überwacht und gewährleistet werden. Dabei verfolgt es die Idee, weitgehend selbsttragende und -erklärende Archiv-Informationspakete (AIPs) zu erzeugen. Alle Prozesse der Datenübernahme („Ingest“) und des Datenerhalts („Preservation Management“) werden in den Metadaten des AIP festgehalten, da sie im Zuge des zukünftigen Datenerhalts eine Rolle spielen können. Die Benutzung erfolgt über Benutzungskopien, sogenannte „Dissemination Information Packages“ (DIPs), die aus dem AIP erzeugt werden.

2. Das elektronische Langzeitarchiv muss dem von NESTOR entwickelten „Kriterienkatalog vertrauenswürdige digitale Langzeitarchive“ entsprechen; die Übereinstimmung muss über ein Zertifikat nachgewiesen sein³.

3. Ein elektronisches Langzeitarchiv sollte modular aufgebaut sein, damit „Best-Practice“ Modelle leicht übernommen und das Langzeitarchiv als Ganzes auf dem technischen Stand seiner Zeit gehalten werden kann. Die Verwendung von Modulen reduziert die Abhängigkeit von einem Softwarehersteller und sorgt auf diese Weise für eine gute Langfristperspektive. Aus dem gleichen Grund sollten Archivprogramme (Erschließungssoftware) und Langzeitarchiv-Software und -Hardware unabhängig voneinander austauschbar sein.

4. Für den Datenerhalt müssen möglichst genaue Informationen über die verwahrten Daten erhoben und dokumentiert werden. Ein elektronisches Langzeitarchiv sollte mit einem Standard-Tool zur Formaterkennung arbeiten, das eine detaillierte Formatbestimmung ermöglicht⁴. Das erkannte Format erhält im Aufbereitungsprozess zwingend eine Kennung aus der Formatliste PRONOM⁵, die in den PREMIS-Metadaten (s. Nr. 6) nachgehalten werden kann. Ergänzende Tools zur Formaterkennung sollten ebenfalls einsetzbar sein, um Zweifelsfälle und besonders komplizierte Formate bearbeiten zu können.

³ Vgl. http://nestor.cms.hu-berlin.de/moinwiki/AG_Vertrauensw%C3%BCrdige_Archive_-_Zertifizierung.

⁴ Ein geeignetes Formaterkennungs-Tool ist beispielsweise DROID, das als Freeware unter <http://droid.sourceforge.net> erhältlich ist. Es wird gepflegt durch das britische Nationalarchiv: The National Archives.

⁵ PRONOM wird gepflegt durch das britische Nationalarchiv: The National Archives, <http://www.nationalarchives.gov.uk/PRONOM/Default.aspx>.

5. Die Formatvalidierung sollte ebenfalls mit einem Standard-Tool möglich sein⁶. Geeignete Tools müssen eine Vielzahl der zuvor ermittelten Text-, Audio- und Videoformate darauf prüfen können, ob eine Datei tatsächlich alle Voraussetzungen, die an ein Format gestellt werden, erfüllt. Auf diese Weise wird sichergestellt, dass fehlerhafte oder unvollständige Kodierungen nicht zu späteren Problemen beim Datenerhalt (Migrationen) führen. Ergänzende Tools zur Formatvalidierung sollten ebenfalls einsetzbar sein, um Spezialfälle abdecken zu können.

6. Die Metadaten, die dem Datenerhalt dienen, sollten sich an dem international anerkannten Standard PREMIS (für „PREservationMetadata: Implementation Strategies“) orientieren⁷. Dabei ist eine archivspezifische Ausprägung zu berücksichtigen, die Details über Entstehungssysteme, Formatkonvertierung in den Metadaten protokolliert. Eine Orientierung an den Modellen des Bundesarchivs, der Landesarchive Baden-Württemberg, Hessen und Nordrhein-Westfalen sowie vor allem der Stadtarchive Köln und Stuttgart ist zu empfehlen. Das Langzeitarchiv sollte das in PREMIS vorgeschlagene Repräsentationsmodell verwenden, d.h. es sollte Inhaltliche Einheiten (IE, entspricht in der Regel einer Verzeichnungseinheit) und darunter Repräsentationen – d.h. physische Manifestationen dieser IE erlauben: Bei einer Migration (Formatwandlung), wird unter der IE eine neue Repräsentation erzeugt, die sich nur hinsichtlich ihrer technischen Ausprägung von ihrer Vorgängerin unterscheidet.

7. Ein elektronisches Langzeitarchiv muss den unterschiedlichen Datentypen, die in einer Kommune entstehen, Rechnung tragen. Aufgrund der Heterogenität des angebotenen Materials sind flexibel anpassbare und modulare Schnittstellen zum Langzeitarchiv und zur Erschließungssoftware unverzichtbar. Folgende Importe müssen möglich sein:

- a) Unstrukturierte Daten (z.B. Daten in einem Filesystem oder Bilder der Pressestelle, Ton- und Videodokumente),
- b) Strukturierte Textdateien aus Fachverfahren (XML-Dateien, oft in XÖV-Kodierung – z.B. Melderegister, Personenstandsregister, Gewerberegister),
- c) Elektronische Akten aus Dokumenten-Management-Systemen (hier empfiehlt sich eine Abbildung der Akten-/Vorgangsstruktur über den XÖV-Standard XDomea2)
- d) Datenbanken / Datenbankauszüge (z.B. aus Geoinformationssystemen, elektr. Liegenschaftsbüchern u.ä.)
- e) Perspektivisch: Internet- / Intranetseiten

⁶ Hierfür ist z.B. JHOVE - JSTOR/Harvard Object Validation Environment geeignet. JHOVE wurde in einem Projekt der JSTOR und des Präsidenten und der Fellows des Harvard College entwickelt, vgl. <http://hul.harvard.edu/jhove>; als Freeware erhältlich unter: <http://sourceforge.net/projects/jhove>.

⁷ PreservationMetadata: Implementation Strategies, gepflegt durch: Library of Congress Network Development and MARC Standards Office (<http://www.loc.gov/standards/premis>); Eine gute Einführung bei Priscilla Caplan (übersetzt von: Tobias Beinert), PREMIS verstehen. 2009 http://www.loc.gov/standards/premis/understanding_premis_german.pdf.

8. Wenn Gemeinschaftseinrichtungen für die Speicherung und das Datenmanagement des elektronischen Langzeitarchivs eingerichtet werden oder bestehende Einrichtungen wie kommunale Rechenzentren diese Aufgabe übernehmen, muss Mandantenfähigkeit gewährleistet sein, d.h. es sind die Datenbestände (Primär- und Metadaten und Indexdatenbank) der einzelnen Kommunen klar voneinander zu trennen. Die Migrationsfähigkeit der Mandanten inkl. aller Primär- und Metadaten ist zu jedem Zeitpunkt verlustfrei zu gewährleisten. Die facharchivischen Entscheidungen im Zuge der Datenübernahme (Ingest) und der Datenpflege (z.B. Migrationen, Erhalt der gesamten Repräsentationenkette u. s. w.) stehen lt. Gesetz dem einzelnen Archiv zu und dürfen nicht - soweit nicht anders vereinbart - durch die Gemeinschaftseinrichtung vorgegeben werden. Beim Aufbau einer gemeinsamen Infrastruktur muss diesen Vorgaben durch ein dezidiertes Rechtekonzept und entsprechende technische Maßnahmen Rechnung getragen werden. Es ist von einem hochwertigen Speichersystem, das die Daten an zwei räumlich voneinander getrennten Orten redundant speichert, auszugehen, wie ihn die meisten kommunalen Rechenzentren in ihren Sicherungskonzepten vorsehen. Eine Speicherung in nicht-kommunalen Einrichtungen oder in verteilten öffentlichen Webspeicher-Lösungen („Public-Clouds“) erscheint angesichts der archiv- und datenschutzrechtlichen Schranken bei der Erfüllung hoheitlicher Aufgaben nicht geeignet. Zumal Maßnahmen, die im privatwirtschaftlichen öffentlichen Cloud Computing der Datensicherung dienen (Zerstückelung von Dateien und Verschlüsselung dieser Datenpakete vor der verteilten Speicherung), den Anforderungen des OAIS Modells nach möglichst unverschlüsselt und verständlich gespeicherten Informationsobjekten widersprechen.

9. Ein elektronisches Langzeitarchiv muss einen nutzerspezifischen Zugang zum Archivgut ermöglichen (vgl. OAIS). Neben dem Vollzugriff für den bearbeitenden Archivar / die bearbeitende Archivarin müssen DIPs für den „Standardbenutzer“ erstellt werden können; bei personenbezogenem Archivgut oder anderem Schutz- und Geheimhaltungsbestimmungen unterliegendem Archivgut sowie bei komplexen Objekten wie Datenbanken müssen die DIPs den entsprechenden Anforderungen angepasst werden können.