

# Ein Bergungsort für digitale Kulturgüter

Studie im Auftrag des Fachbereichs Kulturgüterschutz KGS,  
Bundesamt für Bevölkerungsschutz BABS

Tobias Wildi, 2. März 2020

## Inhalt

Management Summary .....	3
Glossar und Abkürzungen .....	3
Ausgangslage und Ziele .....	4
Von analogen zu digitalen Kulturgütern .....	4
Braucht die Schweiz einen digitalen Bergungsort? .....	5
Wer und was gefährdet digitale Kulturgüter? .....	6
Was sichert der digitale Bergungsort? .....	8
Digital geboren versus digitalisiert .....	11
Konzeption .....	12
Auf welche Normen und Standards stützt sich der Bergungsort? .....	12
Organisatorischer Rahmen .....	13
Zielgruppe und grundlegende Ziele des digitalen Bergungsortes .....	13
Auftrag und rechtlicher Rahmen .....	14
Kriterien für die Auswahl der digitalen Objekte .....	16
Betriebsorganisation .....	17
Geschäftsmodell .....	18
Umgang mit digitalen Objekten .....	19
Container .....	19
Identifikatoren .....	21
Prozesse im Umgang mit digitalen Objekten .....	24
Infrastruktur und Sicherheit .....	27
Dezentral und verteilt .....	27
Teilautomatisierung versus Vollautomatisierung .....	27
Überprüfung und Sicherstellung der Datenintegrität .....	28
Nachhaltige und ressourcenschonende Technologien .....	28
Empfohlene Lösungsvariante .....	30
Literaturverzeichnis .....	31
Gesetzestexte .....	31
Anhang: Ergebnisse der Umfrage 2016 .....	32

## Management Summary

Eilige Leser\*innen gehen direkt zum Fazit «Empfohlene Lösungsvariante» am Ende der Studie, dieses fasst die aus heutiger Sicht technisch, wirtschaftlich und politisch am ehesten machbare Variante für einen präventiven Bergungsort für digitale Kulturgüter in der Schweiz zusammen.

## Glossar und Abkürzungen

ARK	Archival Resource Key
BABS	Bundesamt für Bevölkerungsschutz
BagIt	Containerformat für digitale Objekte der Library of Congress
BZG	Bevölkerungs- und Zivildschutzgesetz
DOI	Digital Object Identifier
EKKGS	Eidgenössische Kommission für Kulturgüterschutz
GEVER	(elektronische) Geschäftsverwaltung
IKT	Informations- und Kommunikationstechnologien
KGS	Kulturgüterschutz
KGSG	Kulturgüterschutz-Gesetz
KGSV	Kulturgüterschutz-Verordnung
LOCKSS	Lots of Copies Keep Stuff Safe, <a href="https://www.lockss.org/">https://www.lockss.org/</a>
NAAN	Name Assigning Authority Number, in ARK eindeutiger Identifikator pro Institution
NCS	Nationale Strategie zum Schutz vor Cyber-Risiken
OAIS	Open Archival Information System, ISO 14721
PID	Persistent Identifier, persistente Identifikatoren zur eindeutigen Identifikation von digitalen Objekten
SKI	Schutz kritischer Infrastrukturen
VSFS	Verordnung des VBS über Sicherstellungsdokumentationen und fotografische Sicherheitskopien

## Ausgangslage und Ziele

### Von analogen zu digitalen Kulturgütern

Auf nationaler Ebene gilt heute die Erstellung von Mikrofilmen und Sicherstellungsdokumentationen als wichtigste präventive Massnahme für die langfristige Erhaltung von Kulturgütern beziehungsweise für die Dokumentation in einem Katastrophenfall.<sup>1</sup> Auch wenn die Konsultation etwas mühsam ist, so gilt der Mikrofilm als verlässliches analoges Langzeitspeichermedium und ist bei richtiger Herstellung, Handhabung und Lagerung mehrere hundert Jahre haltbar. Der Schweizer Kulturgüterschutz speichert heute auf Tausenden von Mikrofilmen wesentliche Archiv- und Bibliotheksbestände sowie Sicherstellungsdokumentationen (Fotografien, fotogrammetrische Aufnahmen, Beschriebe, Pläne, Skizzen, Zeichnungen usw.). Diese Mikrofilmkopien lagern im bundeseigenen Mikrofilmarchiv in Heimiswil (BE). Sicherstellungsdokumentationen ermöglichen im Fall der Beschädigung oder Zerstörung eines Kulturguts eine Wiederinstandstellung oder zumindest eine Überlieferung des letzten bekannten Zustandes. Dank dieser Dokumente konnten in den vergangenen Jahren einige durch Brände oder Hochwasser zerstörte oder beschädigte Kulturgüter der Schweiz wiederhergestellt werden.<sup>2</sup>

Der Mikrofilm stösst jedoch an Grenzen. Heute werden viele mobile Kulturgüter und praktisch alle Sicherstellungsdokumentationen digital erzeugt, abgelegt und auch in digitaler Form dauerhaft archiviert. Eine Überführung respektive Ausbelichtung dieser Daten auf Mikrofilm bedeutet einen Medienbruch oder lässt sich gar nicht mehr durchführen. Zeitbasierte Medien (Audio, Video, Film), 3D-Pläne und 3D-Scans oder Datenbanken lassen sich nicht sinnvoll auf Mikrofilm ausgeben. Zudem ist der Nachschub an Mikrofilm-Rohmaterial langfristig nicht mehr gesichert und zahlreiche Archive und Bibliotheken, aber auch Dienstleister haben ihre Naslabs für die Entwicklung aufgegeben. Die bestehenden Mikrofilmbestände sind weiterhin zu sichern, es ist aber absehbar, dass die Neuproduktion von Mikrofilm Jahr für Jahr abnehmen wird.

Es braucht somit neue, an die digitale Welt angepasste Strategien für präventive Sicherungsmassnahmen von Kulturgütern und Sicherstellungsdokumentation. Die vorliegende Studie bildet einen Schritt in diese Richtung und zeigt Perspektiven auf, wie die bewährten Aspekte des Mikrofilms in die digitale Welt übersetzt werden können. Für die Fortführung des Mikrofilmarchivs im Digitalen wird in dieser Studie ein «Bergungsort für digitale Kulturgüter» oder schlicht ein «digitaler Bergungsort» konzipiert. Darauf aufbauend wird eine systematische Bedürfnisabklärung erfolgen müssen sowie die Spezifizierung der Geschäftsprozesse und der Systemlandschaft. Danach kann eine erste konkrete Umsetzungsetappe erfolgen.

In der Schweiz liegt die Verantwortung für Kultur grundsätzlich bei den Kantonen, diese setzen Recht, verwalten, fördern und schützen. Übergreifend kann der Bund beispielsweise im Rahmen des Kulturgüterschutzes Aktivitäten zum Schutz von Kulturgütern koordinieren. Ein solches Angebot – und nicht eine Verpflichtung – bildet auch der zukünftige nationale digitale Bergungsort. Es ergäbe wenig Sinn, wenn eine Gruppe von Kantonen selber einen Verbund für digitale Archivierung aufbauen würde, hier muss Synergiepotential auf nationaler Ebene genutzt werden.

Die vorliegende Studie nimmt in einem ersten Teil eine Analyse vor. Es werden die zentralen Gefahren identifiziert, denen digitale Kulturgüter heute ausgesetzt sind und denen mit einem nationalen digitalen Bergungsort begegnet werden soll. Zudem werden die für die Archivierung wichtigen Unterschiede zwischen analogen und digitalen Kulturgütern herausgearbeitet, was

---

<sup>1</sup> KGS Guidelines, Sicherstellungsdokumentation, 2/2006, p. 3.  
<https://www.babs.admin.ch/de/aufgabenbabs/kgs/prints.html>

<sup>2</sup> <https://www.babs.admin.ch/de/aufgabenbabs/kgs/massnahmen.html>

dann zur Frage führt, welche Aspekte von digitalen Kulturgütern im Bergungsort überhaupt gesichert werden sollen. Die Konzeption im zweiten Teil der Studie stützt sich auf internationale Normen und Standards, was die Überlegungen vergleichbar macht mit ähnlichen Vorhaben in anderen Ländern. Neben dem weitherum bekannten Standard ISO 14721, «Open Archival Information System» (OAIS), bieten vor allem der nestor-Kriterienkatalog für vertrauenswürdige Langzeitarchive und der Standard ISO 16363 «Audit and Certification of Trustworthy Digital Repositories» eine Leitlinie für die Konzeption. In diesem zweiten Teil wird geklärt, wie der Betrieb des digitalen Bergungsortes organisiert werden kann, in welcher Form die digitalen Objekte archiviert und identifiziert werden und welche Anforderungen an die Speicherinfrastruktur gestellt werden. Für die Konzeption werden mehrere Varianten erläutert und einzelne Varianten exemplarisch vertieft. Die Studie will bewusst keine Technik- und Systemscheide vorwegnehmen, die Diskussion konkreter Lösungsvorschläge hilft aber, gewisse Problemlagen richtig herauszuschälen. Die Studie endet mit einem Fazit, das eine aus heutiger Sicht technisch, politisch und wirtschaftlich realisierbare Lösungsvariante zusammenfasst.

Für die Erarbeitung der Studie wurden mit mehreren Institutionen und Personen Gespräche geführt. Auch wenn noch keine systematische Erhebung der Bedürfnisse durchgeführt wurde, so gaben diese Gespräche doch wertvolle Hinweise auf die heutige Bedürfnislage. Der Autor dankt folgenden Institutionen und Personen:

- Fachbereich KGS im BABS (Laura Albisetti, Rino Büchel)
- Digital Humanities Lab, Universität Basel (Peter Fornaro)
- Kunstmuseum Basel (Rainer Baum, Bruno Jehle, Bernhard Witz)
- Kantonsarchäologie Bern (Adriano Boschetti, Wenke Schimmelpfennig, Werner Schmutz, Urs Zimmermann)
- Staatsarchiv Wallis (Alain Dubois)
- Swisspeace (Rahel von Arx)
- Universitätsbibliothek Basel (Beat Mattmann)

## **Braucht die Schweiz einen digitalen Bergungsort?**

Das Digital Humanities Lab der Universität Basel (dhlab)<sup>3</sup> führte im Auftrag der Eidgenössischen Kommission für Kulturgüterschutz EKKGS 2016 eine Umfrage bei 244 Schweizer Gedächtnisinstitutionen durch, um zu ermitteln, wie viele digitalen Objekten heute schon in diesen Institutionen lagern und wie diese beschaffen sind.<sup>4</sup> In dieser Umfrage zeigte sich deutlich, dass in vielen Institutionen digitale Objekte nicht mehr einfach eine Ergänzung für die Verbreitung von Inhalten bilden, sondern selbst Originalcharakter haben. In vielen Fällen waren also keine analogen Originale vorhanden, auf die man im Notfall hätte zurückgreifen können. Auch die Mengen sind erstaunlich. Mehr als die Hälfte der befragten Institutionen gab an, einen Bestand von über 10'000 digitalen Objekten zu besitzen.

Das dhlab zog aus dieser Umfrage die Folgerung, dass die Gedächtnisinstitutionen pragmatische, einfach verständliche und vor allem finanzierbare Massnahmen benötigen, um ihre digitalen Objekte langfristig zu sichern. Viele Institutionen fühlten sich überfordert mit dem Themen-

---

<sup>3</sup> <https://dhlab.philhist.unibas.ch/>

<sup>4</sup> Befragt wurden im Auftrag der EKKGS des BABS total 244 Institutionen, bei einem Rücklauf von 112 Institutionen. Es wurde eine Online-Umfrage mit 11 Fragen durchgeführt. Die Resultate zu drei Fragen, die einen direkten Zusammenhang mit der vorliegenden Studie haben, finden sich im Anhang.

komplex der digitalen Langzeitarchivierung. Das Thema lag schlicht ausserhalb ihrer Kernaufgaben – eine Ausnahme bildeten höchstens noch die Staatsarchive. Der Tenor der Umfrage war eindeutig, ein digitales Äquivalent des nationalen Mikrofilmarchivs war ein klares Bedürfnis. Ob die Schweiz einen digitalen Bergungsort *braucht*, ist damit noch nicht erwiesen. Aber die Tatsache, dass bereits 2016 knapp zwei Drittel der befragten Institutionen angaben, dass sie digitale Objekte mit Originalcharakter besitzen, gibt doch klare Hinweise. In diesen Institutionen haben die digitalen Objekte Unikatscharakter (wenn man das überhaupt sagen kann von Dateien, die 1:1 vervielfältigt werden können), die entweder zerfallende oder gar nicht vorhandene analoge Objekte ersetzen oder die genuin digital erstellt wurden. Ein Datenausfall oder eine Obsoleszenz würde den unwiederbringlichen Verlust dieser Kulturgüter bedeuten. In der Zwischenzeit ist der Anteil von Institutionen, die digitale Originale besitzen, mit Sicherheit noch gestiegen. Denn im Zeitraum 2016–2020 fand in vielen Verwaltungen die Einführung von GEVER-Systemen (elektronische Geschäftsverwaltung) und zusätzlicher Fachanwendungen und Asset-Management-Systemen statt, womit der Übergang vom sogenannten analogen zum digitalen Primat (Original) vollzogen wurde. Die Verwaltungen müssen entsprechend auch ihre Archive in digitaler Form führen und die Daten langfristig nutzbar halten, ansonsten ist die Rechtssicherheit gefährdet. Ein nationaler Bergungsort zur präventiven Lagerung einer Datenkopie bietet hier zweifelsohne zusätzliche Sicherheit.

## Wer und was gefährdet digitale Kulturgüter?

Im April 2018 verabschiedete der Bundesrat die nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022<sup>5</sup> sowie die nationale Strategie zum Schutz kritischer Infrastrukturen (SKI).<sup>6</sup> Beide Strategien sehen vor, die Resilienz der kritischen Infrastrukturen in der Schweiz zu überprüfen und bei Bedarf zu stärken. Zu diesem Zweck wurde für jeden der insgesamt 28 als kritisch eingestufteten Infrastruktur-Teilsektoren eine Risiko- und Verwundbarkeitsanalyse erstellt und wurden basierend darauf in einem Folgebericht Vorschläge für Massnahmen zur Stärkung der Resilienz erarbeitet.

In den Kreis der kritischen Infrastrukturen wurde auch der Teilsektor der Kulturgüter aufgenommen. Die Gruppe «Schutz kritische Infrastrukturen» des BABS verabschiedete 2017 eine «Risiko- und Verwundbarkeitsanalyse des kritischen Teilsektors Kulturgüter».<sup>7</sup> Diese Analyse war im Vorfeld abgestimmt worden mit dem Informatiksteuerorgan des Bundes, mit dem Fachbereich Kulturgüterschutz im BABS und mit der Eidgenössischen Kommission für Kulturgüterschutz.

Die Analyse konzentrierte sich primär auf Archive (Staatsarchive und Bundesarchiv), weil diese einen Beitrag an die Rechtssicherheit leisten. Zusätzlich wurde der Teilsektor Kulturgüter auch in seiner identitätsstiftenden Funktion analysiert. Die höchste Kritikalität und Verwundbarkeit wurde in der Analyse in folgenden zwei Geschäftsprozessen festgestellt:

- Verwaltung, Bewirtschaftung und Zugriff (Access),
- Sicherung der Bestände (Dokumente, Daten und Metainformationen).

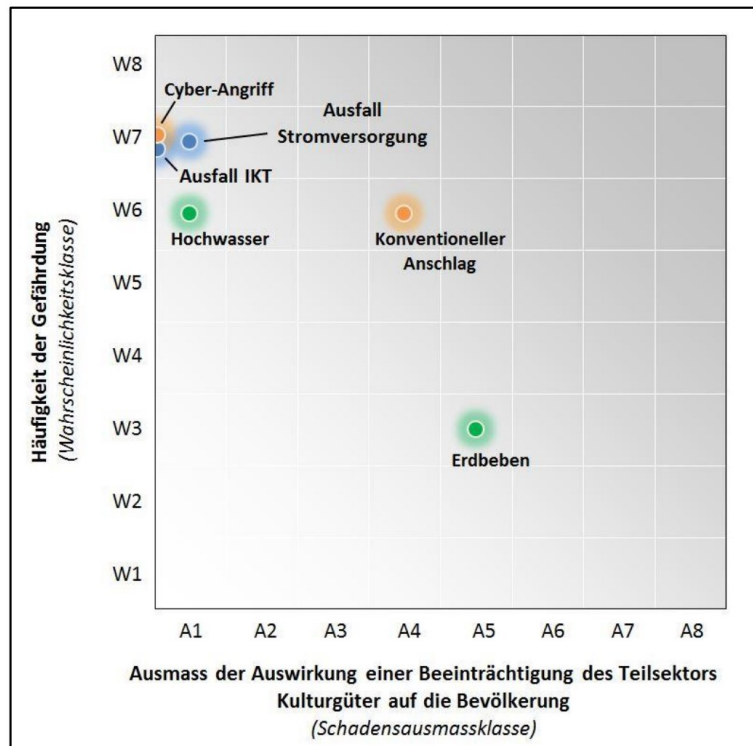
---

<sup>5</sup> <https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale-strategie-schutz-schweiz-cyber-risiken-ncs.html>

<sup>6</sup> <https://www.babs.admin.ch/de/aufgabenbabs/ski.html>

<sup>7</sup> Bundesamt für Bevölkerungsschutz, Risiko- und Verwundbarkeitsanalyse des kritischen Teilsektors Kulturgüter

Für diese zwei Aufgaben respektive Prozesse wurden Gefahren identifiziert in Form von Cyber-Angriffen, Ausfall der IKT (Informations- und Kommunikationstechnologien), Ausfall der Stromversorgung und auch Hochwasser oder Erdbeben. In einer Grafik wurden die Gefahrenbereiche und die angenommenen Eintrittswahrscheinlichkeiten einander gegenübergestellt:<sup>8</sup>



Das Ausmass der Auswirkungen (= Kosten für die Wiederherstellung) wurde ausser bei Erdbeben und einem konventionellen Anschlag als vergleichsweise gering eingeschätzt (wirtschaftlicher Schaden pro Ereignis unter CHF 50 Mio.). Dies aus dem Grund, weil das Archivwesen in der Schweiz dezentral organisiert ist und somit pro Ereignis – so die Annahme – nur ein- oder bloss wenige Archive Schaden erleiden. Zudem geht die Studie davon aus, dass die Staatsarchive über ein «sehr ausgeprägtes» Disaster Recovery Management verfügen, was aber wohl eine zu optimistische Annahme ist, denn die Staatsarchive basieren mit ihren digitalen Archiven ausnahmslos auf den für allgemeine Verwaltungstätigkeit ausgelegten IT-Infrastrukturen der Kantone. Diese ist nicht auf die speziellen Bedürfnisse der digitalen Archivierung hin konzipiert worden. Diese Gefährdungen zeichnen sich durch die folgenden Merkmale aus:

1. **Cyber-Angriffe** und kriminelle Energie, zum Beispiel Ransomware (Verschlüsselung von Speicher); Entwendung von Passwörtern über Phishing oder Social Engineering; schlecht abgesicherte Netzwerke.
2. **Ausfall IKT**, beispielsweise nicht erkannte Fehler in Instanzen des Archivspeichers; die Kopien liegen geografisch zu nahe zusammen oder benutzen alle die gleiche Basisinfrastruktur; Fehlmanipulationen wie unbeabsichtigtes Löschen; Systemadministratoren mit Zugriffsrechten auf sämtliche Daten inkl. Backups.

<sup>8</sup> Ebenda, p. 39. Auf die Kalibrierung von W1–W8 und A1–A8 wird hier verzichtet, sie setzt sich in der Risiko- und Verwundbarkeitsanalyse aus zahlreichen Faktoren zusammen.

3. Ein **Ausfall der Stromversorgung** unterbricht den Betrieb der Server und Speichersysteme. Es besteht die Gefahr, dass die Systeme beim unkontrollierten Ausfall respektive beim Wiederanfahren der Stromversorgung Schaden erleiden.
4. **Konventionelle, physische Angriffe** auf die Institution.
5. Naturkatastrophen wie **Feuer, Hochwasser, Erdbeben**.

In sämtlichen Gefahrenfeldern kann sowohl das potentielle Schadensausmass wie auch die Eintrittswahrscheinlichkeit verringert werden, wenn Daten in einer oder mehreren zusätzlichen Kopien räumlich und institutionell getrennt von der Institution gesichert werden. Wichtig ist dabei, dass mit dieser zentralen, zeitlich unbegrenzten treuhänderischen Aufbewahrung lediglich ein zusätzliches Sicherheitsnetz gebildet wird. Die Staatsarchive, Kantonsbibliotheken und Museen werden damit nicht von ihrer teilweise gesetzlich festgeschriebenen Aufgabe befreit, eigene Infrastrukturen für die langfristige Nutzbarhaltung ihrer digitalen Kulturgüter zu betreiben. Der Fokus des Bergungsortes liegt auf der Bereitstellung von Speicher und der Sicherung von Integrität und Authentizität der Daten. Basierend auf der vorliegenden Risiko- und Verwundbarkeitsanalyse scheint es vorerst ausreichend, eine Datenrückgabe nur für den Katastrophenfall vorzusehen, wenn alle anderen Sicherheitsmechanismen versagt haben.

### Was sichert der digitale Bergungsort?

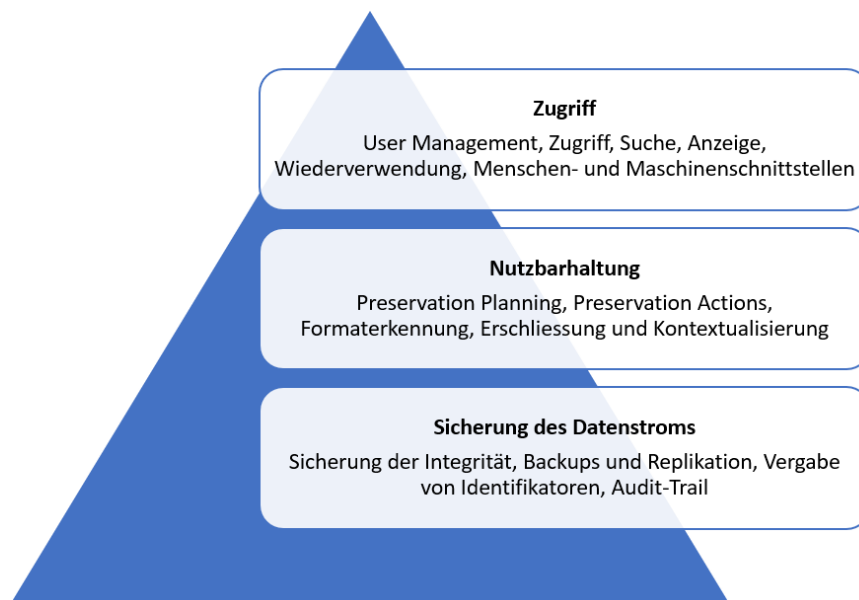
Analoge und digitale Kulturgüter weisen in einigen grundsätzlichen Merkmalen Unterschiede auf, was entsprechend Auswirkungen auf die Ausgestaltung eines Bergungsortes hat. Bei analogen Kulturgütern respektive beim Mikrofilm bilden der Informationsträger und die darauf gespeicherten Informationen eine untrennbare Einheit. Für die Konsultation wird der Film in ein Lesegerät eingespannt, an die richtige Stelle gespult und mittels optischer Vergrößerung und Lichtquelle lesbar gemacht. Grundsätzlich gilt für analoge Informationsträger wie Papier, Pergament oder Fotografien, dass sie ohne zusätzliche Hilfsmittel (ausser der genannten Vergrößerungsapparatur) gelesen werden können. Bei digitalen Kulturgütern ist dies nicht der Fall. Diese werden in Form von Datenströmen gespeichert. Für die Konsultation und Visualisierung der Informationen ist eine geeignete Kombination von Prozessorarchitektur, Betriebssystem und Software notwendig. Jede Konsultation von digitalem Kulturgut setzt eine Rekonstruktion des Datenstroms voraus, damit Informationen sinnvoll dargestellt werden.

Analoge Kulturgüter	Digitale Kulturgüter
Was konsultiert wird, ist identisch mit dem, was konserviert wird.	Konserviert wird ein Datenstrom.
	Konsultiert wird eine Sicht auf den Datenstrom. Jede Konsultation bedeutet eine Rekonstruktion des Datenstroms mit Hilfe von Hard- und Software.
Beispiele	
Mikrofilm: Die archivierte Mikrofilmrolle wird mittels Vergrößerungsoptik und Lichtquelle konsultiert.	PDF-Datei: Gespeichert wird ein Datenstrom, für die Konsultation wird ein zum Zeitpunkt der Konsultation aktuelles und aufeinander abgestimmtes System von Hardware, Betriebssystem und Lesesoftware benötigt.



Diese in der digitalen Welt existierende Trennung zwischen Konservierung und Konsultation führt zur grundsätzlichen Frage, für welche Aspekte der digitalen Erhaltung der zukünftige digitale Bergungsort überhaupt verantwortlich sein soll. In einem einfachen Modell können drei Stufen unterschieden werden:

- a) **Sicherung des Datenstroms** durch Replikation/Backups, periodische Prüfung von Integrität, Vergabe von eindeutigen Identifikatoren, Protokollierung aller Massnahmen zum Nachweis der Authentizität (Audit-Trail).
- b) Darüber hinaus zusätzlich die **Nutzbarhaltung** sicherstellen durch Erhaltungsplanung und gegebenenfalls Erhaltungsmaßnahmen. Dazu gehört die Konvertierung (Umwandlung) von Dateien aus obsoleten in neue archivaugliche Formate und auch der Umgang mit komplexen Objekten wie Websites, Datenbanken oder Software, die archiviert werden soll.
- c) Und schliesslich auch den **Zugriff** für Menschen und Maschinen sicherstellen, beispielsweise in Form eines digitalen Lesesaals, respektive eines «nationalen Kulturgüterportals».



Wenn es sich bei Variante a) primär um Herausforderungen der Speicherorganisation und der Ein- und Auslieferung digitaler Objekte handelt, dann sind für Variante b) die Herausforderungen ungleich grösser. Der digitale Bergungsort müsste für alle archivierten digitalen Objekte die langfristige Nutzbarhaltung sicherstellen. Die Organisation, die für den Betrieb des Bergungsortes zuständig ist, müsste über das Spezialwissen der datenliefernden Institutionen verfügen, um diese Aufgabe erbringen zu können. Für Standardformate im Bereich Rasterbilder oder Office- und Mailanwendungen wäre dies womöglich noch zu leisten. Bei komplexen, aus mehreren Einzeldateien zusammengesetzten Objekten wie beispielsweise 3D-CAD oder Datenbanken ist der Aufwand bereits ungleich grösser. Die Nutzbarhaltung von Kulturgütern wie Computerspielen oder ganzen Videoinstallationen ist ohne das Fachwissen der verantwortlichen Gedächtnisinstitution so gut wie unmöglich. Realistischerweise wird sich der Bergungsort also auf die Datensicherung konzentrieren, die Fragen der Nutzbarhaltung bleibt in der Verantwortung der abliefernden Institution. Auch das Szenario c), der Aufbau eines Endbenutzer-Zugriffs auf die Daten, wird hier ausgeschlossen. Es handelt sich um ein eigenes Aktivitätsfeld mit eigenen Herausforderungen und trägt nicht dazu bei, die von der Fachgruppe SKI identifizierten Risiken herabzusetzen.

Wenn die Schichten b) und c) unseres Modells durch den digitalen Bergungsort nicht abgedeckt werden, so ist doch festzuhalten, dass sie in den Gesprächen, die während der Erarbeitung dieser Studie geführt wurden, immer wieder genannt und gefordert wurden. Gerade kleine Institutionen erhoffen sich hier Unterstützung. Die Unterstützung muss jedoch in Form von Wissensaustausch und Koordination zwischen Institutionen mit ähnlichen Aufgaben und Zielen erfolgen. Die Koordination von domänenspezifischem Wissen kann durchaus durch den Fachbereich KGS und den digitalen Bergungsort in Form von Workshops oder Guidelines gefördert werden. Primär liegt die Verantwortung, sich besser zu vernetzen und auszutauschen, aber bei den Institutionen selbst. In der Schweiz existieren heute lediglich in zwei Bereichen ständige Austausch- und Koordinationsgremien, welche Wissen bezüglich digitaler Archivierung koordinieren:

- Die Staatsarchive haben 2003 gemeinsam die «Koordinationsstelle für die dauerhafte Archivierung elektronischer Unterlagen **KOST**» gegründet, welche bis heute eine mit 200 Stellenprozent dotierte Geschäftsstelle betreibt. Die Erkenntnisse der KOST stehen allerdings nur den Mitgliedsarchiven zur Verfügung, was die koordinative Wirkung dieses Gremiums stark einschränkt.<sup>9</sup>
- Für audiovisuelles Kulturgut nimmt der Verein **MEMORIAV** eine koordinierende Funktion ein, indem die MEMORIAV-Geschäftsstelle Empfehlungen zur Erhaltung von audiovisuellen Dokumenten (auch digitalen) erlässt und regelmässig aktualisiert und sich stark in der Aus- und Weiterbildung engagiert.<sup>10</sup>

Keine systematische institutionsübergreifende Koordination ist bisher in den Bereichen Archäologie und Denkmalpflege erkennbar, wo Daten zu Grabungen oder zu Bauwerken ebenfalls über sehr lange Zeiträume nutzbar gehalten werden müssen. Auch im Bereich der Museen und insbesondere der digitalen Kunst fehlt ein systematischer und institutionalisierter Austausch in Bezug auf die Sicherung digitaler Kulturgüter. Die Berner Fachhochschule verfasste 2017 im Auftrag der Schweizerischen Nationalbibliothek eine Studie zum Thema «Digitale Langzeitarchivierung in der Schweiz» und konstatierte die nicht existente institutionsübergreifende Koordination: «Die fehlende bereichs- und fachübergreifende Koordination erschwert auch den gezielten Aufbau von fehlenden Kompetenzen. So konnten beispielsweise im Rahmen dieser Studie keine Institutionen identifiziert werden, die Kompetenzen in der digitalen Langzeiterhaltung von neueren Formen des Digitalen wie z. B. Facebook-Posts oder Apps aufweisen.»<sup>11</sup>

Die Förderung von Austausch und Koordination wird nicht primäres Ziel des digitalen Bergungsortes sein. Allerdings kann der Aufbau eines solchen digitalen Bergungsortes ein Katalysator sein, um auf nationaler Ebene verbesserte domänenspezifische Koordinationsbemühungen in Gang zu bringen. Dies ist in verschiedenen Bereichen denkbar:

- **Ausbildung und Workshops** für die Aufbereitung von Daten und Metadaten für die Speicherung im digitalen Bergungsort. Im Rahmen der Vorbereitung und Durchführung solcher Ausbildungsmodule findet ganz automatisch eine Koordination statt.
- Verfassen von **Guidelines** mit Empfehlungen für domänenspezifische Daten- und Metadatenmodelle für den digitalen Bergungsort.

Aus diesen Aktivitäten entsteht mit der Zeit ein gemeinsames Verständnis für geeignete Dateiformate, Werkzeuge und Prozesse, das gerade auch kleinen, wenig finanzkräftigen Institutionen weiterhilft.

---

<sup>9</sup> <https://kost-ceco.ch/>

<sup>10</sup> <http://memoriav.ch/>

<sup>11</sup> Burda/DunggaWinterleitner/Estermann, Digitale Langzeitarchivierung in der Schweiz, p.22

## Digital geboren versus digitalisiert

Oftmals werden digitale Kulturgüter unterteilt in die Kategorien «retrodigitalisiert» und «genuin digital». So gilt das Digitalisat einer analogen Fotografie als «Retrodigitalisat», eine mit der gleichen Digitalkamera erstellte Portraitaufnahme aber als «genuin digital» erstellte Fotografie. Die vorliegende Studie unterscheidet diese beiden Kategorien nicht beziehungsweise stellt sie als ebenbürtig nebeneinander. Denn die Grenzen zwischen den beiden vermeintlich scharf voneinander abtrennbaren Konzepten lösen sich bei genauerem Hinschauen mehr und mehr auf. Viele sogenannte «genuine digitale Kulturgüter» referenzieren in irgendeiner Form eine analoge Wirklichkeit. Jede digitale Fotografie bildet eine analoge Welt ab. Eine digital erstellte Landkarte stellt das Modell einer analogen Welt dar. Die Studie verzichtet darauf, digitale Kulturgüter der einen oder der anderen Kategorie zuzuschreiben. Der kulturelle Wert digitaler Objekte muss an anderen Massstäben gemessen werden – und zwar an genau den gleichen bewährten Kriterien, die bereits für analoge Kulturgüter zur Anwendung kommen. Der Wert von Kulturgütern hängt nicht von ihrem Informationsträger ab (analog oder digital) und auch nicht von ihrer Entstehungsweise (retrodigitalisiert oder digital erstellt).

Soweit die Ausgangslage dieser Studie: Das analoge Speichermedium Mikrofilm hat sich dank seiner Einfachheit und Langlebigkeit während langer Zeit bewährt. Für die digitale Welt gilt es nun ein Äquivalent zu entwickeln. Dieses soll insbesondere dazu beitragen, die von der Fachgruppe SKI identifizierten Risiken in den Bereichen Cyber-Angriffe, Ausfall der IKT, Ausfall der Stromversorgung und Naturgefahren herunterzusetzen. Eine Herausforderung ist, dass bei digitalen Objekten die Konservierung und Konsultation zwei unterschiedliche Aufgabenfelder bilden. Realistischerweise wird sich der Bergungsort auf die Konservierung der Datenströme digitaler Kulturgüter konzentrieren, die inhaltliche Nutzbarhaltung muss auf andere Weise organisiert werden. Vorgeschlagen wird die Förderung domänenspezifischer Koordinationsbemühungen, bei denen der Bergungsort durchaus eine Katalysatorfunktion übernehmen kann.

## Konzeption

### Auf welche Normen und Standards stützt sich der Bergungsort?

Das folgende Kapitel hat die Konzeption des digitalen Bergungsortes zum Ziel. Es orientiert sich zu diesem Zweck an bestehenden Normen und Standards, die im Bereich der digitalen Archivierung heute existieren und breit akzeptiert sind. Diese Normen und Standards beruhen sowohl auf akademischen Arbeiten, als auch Erfahrungen, die viele Institutionen in vergleichbaren Projekten schon gemacht haben. Entsprechend helfen sie, den Planungsprozess gezielter zu durchlaufen, Kosten zu sparen, grobe Fehler zu vermeiden und systematisch sicherzustellen, dass alle wichtigen Aspekte und Bereiche mitbedacht wurden. Und um das Vertrauen in den digitalen Bergungsort zu erhöhen, kann später auch auf eine Zertifizierung hingearbeitet werden. Die folgenden Normen und Standards bilden die Grundlage für den Aufbau des zukünftigen Bergungsortes für digitale Kulturgüter:

- **ISO 14721, «Open Archival Information System» (OAIS)**<sup>12</sup> bildet weltweit das wichtigste Referenzmodell im Bereich digitale Archivierung. Der Standard ist aufgeteilt in ein funktionales und ein Informationsmodell. Er lässt jedoch offen, wie die technisch-organisatorische Umsetzung konkret vorgenommen wird. Entsprechend ist es auch nicht möglich, sich ISO 14721-zertifizieren zu lassen.
- **ISO 16363 «Audit and Certification of Trustworthy Digital Repositories»**<sup>13</sup> dient der Auditierung und Zertifizierung vertrauenswürdiger digitaler Archive und stammt aus dem gleichen Gremium wie das OAIS-Modell. Es handelt sich um ein Maturitätsmodell, um die Konformität zu ISO 14721 zu messen, und behandelt drei Aspekte des digitalen Archivs:
  - o Organisatorischer Rahmen
  - o Umgang mit Objekten
  - o Infrastruktur und Sicherheit
- Der deutsche **nestor-Kriterienkatalog vertrauenswürdige digitale Langzeitarchivierung**<sup>14</sup> ist ein Vorläufer für die **DIN-Norm 31644:2012**<sup>15</sup> und umfasst Kriterien und Grundprinzipien für die Vertrauenswürdigkeit von digitalen Archiven. DIN 31644 erschien gleichzeitig wie ISO 16363, ist jedoch knapper gehalten.

In den letzten Jahren wurden verschiedene Stufen und Modelle der Zertifizierung entwickelt, die von einem Self-Assessment bis zu einer Auditierung durch eine zugelassene Zertifizierungsstelle reichen. Auf diese Mechanismen soll in der vorliegenden Studie nicht weiter eingegangen werden.

Als Raster für die nachfolgende Konzeption wird der nestor-Kriterienkatalog genutzt, der nach dem gleichen Muster wie ISO 16363 aufgebaut ist. Dieser Kriterienkatalog bildet ein praxisnahes Hilfsmittel, nicht nur um bestehende digitale Archive auf ihre Vertrauenswürdigkeit zu prüfen, sondern vor allem auch um neue Archive entlang standardbasierter Kriterien zu konzipieren, zu spezifizieren und zu realisieren. Im nestor-Kriterienkatalog werden die drei gleichen

---

<sup>12</sup> <https://www.iso.org/standard/57284.html>. Identischer Text frei verfügbar unter <https://public.ccsds.org/pubs/650x0m2.pdf>.

<sup>13</sup> <https://www.iso.org/standard/56510.html>. Identischer Text frei verfügbar unter <https://public.ccsds.org/pubs/652x0m1.pdf>.

<sup>14</sup> nestor-Arbeitsgruppe Vertrauenswürdige Archive - Zertifizierung, Kriterienkatalog vertrauenswürdige digitale Langzeitarchive

<sup>15</sup> <https://www.beuth.de/de/norm/din-31644/147058907>

zentralen Bereiche verwendet, wie sie auch ISO 16363 nennt. Die untenstehende Tabelle unterteilt die drei grossen Bereiche des nestor-Kriterienkatalogs in feinere Kategorien. Die fett gesetzten Punkte werden detailliert und vertieft behandelt. Die anderen Punkte spielen in den Vorüberlegungen auf Stufe Studie noch eine untergeordnete Rolle respektive liegen ausserhalb des zukünftigen Aufgabenbereichs des digitalen Bergungsortes.<sup>16</sup>

<b>Organisatorischer Rahmen</b>	<b>Umgang mit Objekten</b>	<b>Infrastruktur und Sicherheit</b>
<b>Ziele und Zielgruppe</b> sind definiert	<b>Integrität</b> sichern	<b>Angemessene IT-Infrastruktur</b>
Angemessene Nutzung ist sichergestellt	Authentizität sichern	<b>Schutz vor internen und externen Gefahren</b>
<b>Gesetzliche und vertragliche Regelungen</b> werden eingehalten	Erhaltungsmassnahmen	
<b>Organisationsform</b> und Nachhaltigkeit	<b>Definierte Ablieferungsprozesse</b>	
Qualitätsmanagement	<b>Definierte Archivpakete</b>	
	Nutzung nach definierten Vorgaben	
	Datenmanagement, <b>Identifizierbarkeit</b>	

## Organisatorischer Rahmen

Der erste grosse Block zur Konzeption des digitalen Bergungsortes betrifft den organisatorischen Rahmen. Dieser wird abgesteckt durch die Zieldefinition, die rechtlichen Bedingungen sowie die Ausgestaltung des Betriebs in organisatorischer, personeller und finanzieller Hinsicht. Es liegt auf der Hand, dass der organisatorische Rahmen klar geregelt, transparent und nachvollziehbar sein muss, damit die datenabliefernden Institutionen überhaupt Vertrauen in den digitalen Bergungsort haben. Eine wichtige Aufgabe bei der späteren Spezifizierung und Umsetzung wird sein, diesen im Folgenden angerissenen Rahmen in allen Details auszuarbeiten und zu implementieren.

### Zielgruppe und grundlegende Ziele des digitalen Bergungsortes

Die Zielgruppe für den digitalen Bergungsort **deckt sich weitgehend mit der Zielgruppe des bestehenden Mikrofilmarchivs**. Die Dienstleistungen richten sich grundsätzlich an die Kantone und ihre Institutionen mit Kulturgütern von nationaler oder regionaler Bedeutung (A- und B-Objekte), die eine Kopie ihrer digitalen Objekte an einem zusätzlichen Standort speichern wollen. Weiter sieht die Strategie des Bundesrats vor, den Bergungsort auch für Kulturgüter aus dem Ausland zu öffnen. Der Bergungsort bietet diesen Institutionen ein Sicherheitsnetz, das

<sup>16</sup> Die Tabelle übernimmt die Kapitelübersicht des nestor-Kriterienkatalogs. Vgl. nestor-Arbeitsgruppe Vertrauenswürdige Archive - Zertifizierung, Kriterienkatalog vertrauenswürdige digitale Langzeitarchive, p. 11ff.

von ihrer eigenen Infrastruktur komplett getrennt ist. Die Betriebsorganisation und die IT-Infrastruktur des Bergungsortes sind darauf ausgelegt, digitale Kulturgüter gerade auch in Krisen- und Katastrophenphasen zu sichern.

Der Datentransfer, also An- wie auch Auslieferung, findet immer zwischen einer Institution und dem Bergungsort statt. Der Bergungsort betreibt selber keine Infrastruktur zur Auslieferung von Daten direkt an Endnutzer und will kein «nationales Kulturgüterportal» sein, er ist vielmehr ein sogenanntes «**Dark Archive**». Das bedeutet, dass ein Rückgriff auf die gespeicherten digitalen Objekte nur dann stattfindet, wenn sämtliche institutionseigenen Kopien zerstört, korrupt oder aus einem anderen Grund nicht mehr zugänglich sind.

### **Auftrag und rechtlicher Rahmen**

Der Bundesrat veröffentlichte im März 2019 seine Strategie 2020–2023 zum Schutz des gefährdeten Kulturerbes.<sup>17</sup> Einer der Schwerpunkte dieser Strategie lautet: «Der internationalen Gemeinschaft das Know-how und die Erfahrung der Schweiz zum Schutz des gefährdeten Kulturerbes zur Verfügung stellen». Das erste strategische Ziel innerhalb dieses Schwerpunktes bezieht sich auf die Bereitstellung eines Bergungsortes: «Der Bergungsort für gefährdete Kulturgüter ist einsatzbereit». Der Bundesrat sieht dafür Massnahmen sowohl im konventionell-analogen wie auch im digitalen Bereich vor:

- «a) Den Schweizer Bergungsort auf internationaler Ebene bekannt machen und auf die Vorteile und die Erfahrung der Schweiz hinweisen.
- b) An Initiativen zur internationalen Verbreitung des Konzepts der Bergungsorte und an deren Vernetzung unter der Schirmherrschaft der UNESCO mitarbeiten (mit dem Ziel, sich über die Aktivierung des Schweizer Bergungsortes zu verständigen).
- c) Ein Projekt für einen Bergungsort für digitale Kulturgüter sowie die Grundlagenforschung im Bereich digitale Daten entwickeln.»<sup>18</sup>**

Damit ist der **Auftrag** für die Konzeption und die Spezifizierung des Bergungsortes gegeben. Entsprechend erwähnt auch die Botschaft zur Totalrevision des vom Parlament im Dezember 2019 verabschiedeten «Bevölkerungs- und Zivilschutzgesetzes» (BZG) explizit «digitale Kulturgüter» und «digitale kulturgüterschutzrelevante Datensammlungen» als Teil der mobilen Kulturgüter.<sup>19</sup>

Das bestehende «**Bundesgesetz über den Schutz der Kulturgüter bei bewaffneten Konflikten, bei Katastrophen und in Notlagen**» (KGSG) regelt heute neben zahlreichen anderen Fragen auch das nationale Mikrofilmarchiv und den bereits bestehenden Bergungsort für physische mobile Kulturgüter.<sup>20</sup> Art. 2 der KGSG definiert zwei auch für den zukünftigen digitalen Bergungsort zentrale Begriffe:

- «a. **Kulturgüter:** Güter, Gebäude und Orte nach Artikel 1 des [Haager] Abkommens; [...]

---

<sup>17</sup> <https://www.bak.admin.ch/bak/de/home/aktuelles/nsb-news.msg-id-74245.html>

<sup>18</sup> <https://www.news.admin.ch/news/message/attachments/56039.pdf>

<sup>19</sup> <https://www.news.admin.ch/news/message/attachments/54621.pdf>

<sup>20</sup> <https://www.admin.ch/opc/de/classified-compilation/20122172/index.html>

c. **Bergungsort:** geschützte Räumlichkeit, die der Bund zur vorübergehenden treuhänderischen Aufbewahrung von beweglichen Kulturgütern, die ein Teil des kulturellen Erbes eines Staates sind und in ihrem Eigentümer- oder Besitzerstaat akut gefährdet sind, zur Verfügung stellt.»

Die Definition von Kulturgütern im Sinne des Haager Abkommens spielt eine Rolle bei der Frage, welche Daten im digitalen Bergungsort überhaupt gesichert werden sollen und wer diese auswählt (siehe nächstes Kapitel über Kriterien für die Auswahl digitaler Objekte). In Art. 5 Abs. 3 KGSG wird festgelegt, dass die Erstellung von Sicherstellungsdokumentationen explizit eine **Aufgabe der Kantone** ist:

«Sie [die Kantone] erstellen von ihren besonders schutzwürdigen Kulturgütern Sicherstellungsdokumentationen und fotografische Sicherheitskopien.»

Da heute sowohl Sicherstellungsdokumentationen wie auch Sicherheitskopien mehr und mehr nur noch in digitaler Form erstellt werden, ist den Kantonen eine neue Perspektive zum Schutz dieser Daten zu eröffnen. Ansonsten investieren sie Ressourcen in die Produktion von Daten, für deren langfristige Sicherung keine adäquaten Infrastrukturen bereitstehen.

Die konkreten Modalitäten für das heutige Mikrofilmarchiv sind in der **«Kulturgüterschutz-Verordnung» (KGSV)**, Art. 5 geregelt:

«Art. 5 Sicherstellungsdokumentationen und fotografische Sicherheitskopien

1. Das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) legt die **Anforderungen** an Sicherstellungsdokumentationen und die Einzelheiten der Herstellung, Handhabung, Verarbeitung und Aufbewahrung von fotografischen Sicherheitskopien fest.
2. Das BABS führt ein **zentrales Mikrofilmarchiv** zur Aufbewahrung der fotografischen Sicherheitskopien.
3. Es **erwirbt** von jedem Verfilmungsprojekt der Kantone eine fotografische Sicherheitskopie in Form einer Positivkopie und bewahrt sie auf.»

Das sind die drei Grundpfeiler, auf denen das analoge Mikrofilmarchiv basiert. Sie gelten, allenfalls modifiziert, auch für einen Bergungsort für digitale Kulturgüter:

1. **Anforderungen:** Einige grundlegende Anforderungen an die Paketierung und Identifizierung von Daten werden weiter unten im Teil «Umgang mit digitalen Objekten» genannt. Weiterführende Anforderungen können nach Bedarf in Form von Guidelines ausformuliert werden.
2. **BABS ist Betriebsorganisation:** Diese Frage wird weiter unten im Teil «Betriebsorganisation» diskutiert. Vorweg: Es ergibt auch für einen digitalen Bergungsort Sinn, dass die Betriebsverantwortung beim BABS liegt.
3. **Erwerbung:** Die Archivierung der Mikrofilme im nationalen Lager verursacht für die Kantone keine Fixkosten. Für den digitalen Bergungsort muss geprüft werden, wie ein sinnvolles zukünftiges Geschäftsmodell ausgestaltet werden kann.

In der **«Verordnung des VBS über Sicherstellungsdokumentationen und fotografische Sicherheitskopien» (VSFS)** von 2016 werden detaillierte technische Anforderungen an die Er-

stellung der digitalen Unterlagen (Fotografien, Dokumentation) formuliert. Der rechtliche Rahmen für einen digitalen Bergungsort besteht somit grundsätzlich sowohl auf Gesetzes- wie auch Verordnungsstufe. Die detailliert ausformulierte VSFS muss parallel zum Aufbau des digitalen Bergungsortes voraussichtlich revidiert und aktualisiert werden.

### **Kriterien für die Auswahl der digitalen Objekte**

Gemäss KGSG Abs. 2 dient der Bergungsort dem Zweck, Kulturgüter und/oder Sicherstellungsdokumentationen im Sinne der Haager Konvention zu sichern. Der digitale Bergungsort dient also explizit nicht der Aufgabe, ein generelles nationales Auffangbecken für Daten mit langen oder dauerhaften Aufbewahrungsfristen zu sein, sondern konzentriert sich auf die Speicherung digitaler Kulturgüter – ergänzt durch Sicherstellungsdokumentationen derselben. Der Begriff des Kulturguts dient somit als zentrales Kriterium für die Auswahl der digitalen Objekte, die in den digitalen Bergungsort aufgenommen werden. Die Definition in Art. 1 des Haager Abkommens lautet wie folgt:

«**Kulturgut** im Sinne dieses Abkommens sind, ohne Rücksicht auf Herkunft oder Eigentumsverhältnisse:

**a) bewegliches oder unbewegliches Gut, das für das kulturelle Erbe der Völker von grosser Bedeutung ist**, wie z.B. Bau-, Kunst- oder geschichtliche Denkmäler kirchlicher oder weltlicher Art, archäologische Stätten, Gruppen von Bauten, die als Ganzes von historischem oder künstlerischem Interesse sind, Kunstwerke, Manuskripte, Bücher und andere Gegenstände von künstlerischem, historischem oder archäologischem Interesse sowie wissenschaftliche Sammlungen und bedeutende Sammlungen von Büchern, von Archivalien oder von **Reproduktionen des oben umschriebenen Kulturguts**;

b) Gebäude, die in der Hauptsache und tatsächlich der Erhaltung oder Ausstellung des unter a umschriebenen beweglichen Guts dienen, wie z.B. Museen, grosse Bibliotheken, Archive sowie Bergungsorte, in denen im Falle bewaffneter Konflikte das unter a umschriebene bewegliche Kulturgut in Sicherheit gebracht werden soll. [...]»<sup>21</sup>

Beispiele für digitale Kulturgüter und Sicherstellungsdokumentationen respektive Reproduktionen sind:

- Ein Museum bewahrt den Nachlass eines Fotografen, dieser Nachlass umfasst digital erstellte Fotografien.
- Ein Kunstmuseum digitalisiert seine Werke zum Zwecke der Sicherstellungsdokumentation.
- Ein archäologischer Dienst fertigt Drohnenvideos an, um eine offene Fundstelle zu dokumentieren.
- Ein Kanton erstellt, speichert und archiviert seine Regierungsratsprotokolle ausschliesslich in digitaler Form.
- Eine Kantonsbibliothek digitalisiert die Tageszeitungen ihres Kantons und übernimmt das audiovisuelle Sendungsarchiv eines ansässigen Lokalradios oder -fernsehens.

---

<sup>21</sup> <https://www.admin.ch/opc/de/classified-compilation/19540079/index.html>



Daneben existieren zahlreiche Datenbestände, die aus gesetzlichen, administrativen, wissenschaftlichen oder anderen Gründen zwar über lange Zeit nutzbar gehalten werden müssen, aber nicht per se dem kulturellen Erbe zugerechnet werden. Beispiele dazu sind:

- Verwaltungsunterlagen, die als nicht archivwürdig eingestuft sind und nach Ablauf der gesetzlichen und administrativen Aufbewahrungsfristen vernichtet werden können.
- Register wie Grundbuch, Einwohnerkontrolle, Zivilstandsregister
- Daten, Unterlagen, Pläne zu Infrastrukturen, die ausschliesslich dazu dienen, den Unterhalt derselben sicherzustellen (Nationalstrassennetz, SBB-Schienennetz etc.).
- Pensionskassenunterlagen und Unterlagen der kantonalen Ausgleichskassen (AHV, IV)
- Forschungsdaten, medizinische Daten
- Persönliche Archive und Nachlässe von Einzelpersonen, sofern es sich nicht um Personen des öffentlichen Lebens handelt.

Die Selektion und die Verantwortung für die Anfertigung der Sicherstellungsdokumentation fällt nach KGSG in den Aufgabenbereich der KGS-Verantwortlichen der Kantone. Durch die Veränderung des Informationsträgers (digitale Objekte statt Mikrofilm) ändern sich weder die Selektionskriterien, noch die Selektionsprozesse.

### **Betriebsorganisation**

Der Betrieb des digitalen Bergungsortes muss durch eine geeignete Organisation sichergestellt werden. Diese Organisation bietet die nötige Kontinuität und Sicherheit und ist in Stichworten für die folgenden **Aufgabenfelder** zuständig:

- **Betriebskoordination** des digitalen Bergungsortes basierend auf den gesetzlichen Grundlagen und den Vorgaben des BABS.
- Abschliessen von **Verträgen** mit den Kantonen respektive mit den abliefernden Institutionen.
- Institutionen bei der **Datenlieferungen** instruieren und unterstützen.
- **Kontrolle** der angelieferten Datenbestände, Rückgabe von Metadaten (insbesondere PID, persistente Identifikatoren) an die Institutionen.
- Unterstützung beim **Datenrückgriff**.
- Gegebenenfalls Fakturierung.
- **Wartung** der Software, Server und Speicherinfrastruktur, in Koordination mit den dafür beauftragten Dienstleistern.
- **«Community Outreach»**, also Ausbildung, Durchführung von Kursen für abliefernde Institutionen und KGS-Verantwortliche, Verfassen von Guidelines. Ziel ist es, die Datenqualität über Beratung hoch zu halten, ohne dass der Bergungsort selber Daten überprüfen muss.

Die Betriebsverantwortung für das Mikrofilmarchiv liegt heute beim BABS, Fachbereich Kulturgüterschutz. Für den digitalen Bergungsort sind grundsätzlich verschiedene **Varianten** denkbar, um den Betrieb zu organisieren:

- **Variante geteilte Verantwortung:** Mehrere Partner und Institutionen gründen ein Konsortium, das den Bergungsort finanziert und betreibt. Für ähnliche Aufgaben, allerdings nicht für den Betrieb von Infrastruktur, wurden in der Schweiz der Verein Memoriav und die Koordinationsstelle Kost gegründet.
- **Variante Mandat:** Der Betrieb des digitalen Bergungsortes wird als Mandat an eine geeignete Institution vergeben. Das kann zum Beispiel eine grosse Bibliothek oder ein Archiv sein, das über die notwendigen Fachkenntnisse, die Fachleute und die Prozesse verfügt. Das Mandat wird periodisch (z. B. alle 8–10 Jahre) neu ausgeschrieben.

- **Variante Bund:** Die Verantwortung liegt, wie bereits beim Mikrofilmarchiv, beim BABS, Fachbereich Kulturgüterschutz.

Die beiden Varianten «geteilte Verantwortung» und «Mandat» hätten tiefgreifende gesetzliche und organisatorische Neuordnungen zur Folge. Zudem müssten die neuen Träger in der Community ihre Vertrauenswürdigkeit zunächst einmal unter Beweis stellen. Als nicht sinnvoll betrachtet wird zudem eine unterschiedliche organisatorische Ausgestaltung von Mikrofilmarchiv und digitalem Bergungsort, je nach Informationsträger wären dann unterschiedliche Ablieferungsprozesse und Ansprechpartner zu berücksichtigen. Auf die Neugründung einer Organisation respektive eines Konsortiums soll deshalb verzichtet werden.

Wenn die Betriebsorganisation beim BABS angesiedelt wird, ist sie in jedem Fall auf einen engen fachlichen Austausch mit den abliefernden Institutionen angewiesen, viel stärker, als dies bisher beim Mikrofilmarchiv der Fall war. Diesem Umstand ist bei der institutionellen Ausgestaltung Rechnung zu tragen. Denkbar wäre der Aufbau eines begleitenden Expertengremiums im Sinne eines «Technical Sounding Boards» oder ein Einbezug der «Eidgenössischen Kommission für Kulturgüterschutz» (EKKGS), die bereits heute als fachliches Beratungsgremium für den Fachbereich Kulturgüterschutz fungiert.

### Geschäftsmodell

Für den digitalen Bergungsort muss ein Geschäftsmodell ausgearbeitet werden, das seine Finanzierung langfristig sicherstellt. Es liegt in der Natur von digitalen Archiven, dass der Betrieb und die periodische Erneuerung von Speicher und IT-Systemen Fixkosten verursachen. Vielleicht werden Speicherpreise noch weiter sinken, die Kosten für die Speicherorganisation (Backup, Replikation, Überprüfung) und für den Betrieb des digitalen Bergungsortes werden aber bestehen bleiben. Um die Vertrauenswürdigkeit des digitalen Bergungsortes sicherzustellen, muss das Geschäftsmodell durch einen gesetzlichen Auftrag und ein transparentes und nachvollziehbares Finanzierungsmodell abgesichert sein. Grundsätzlich sind für die Finanzierung des Bergungsortes folgende Modelle denkbar:

- **Variante «zentralisiert»:** Der Bund beziehungsweise das BABS trägt die gesamten Betriebskosten des Bergungsortes, unabhängig von der Speichermenge und vom Speicherzuwachs. Diese Variante macht es möglich, dass der Bergungsort explizit als Angebot formuliert wird. Im Falle eines Datenverlustes im Bergungsort haftet der Bund nicht für eventuelle Schäden.
- **Variante «Verursacherprinzip»:** Das BABS trägt einen Teil der Fixkosten, beispielsweise für die ersten 4 TB Daten jeder Institution. Für grössere Datenbestände wird zusätzlich eine Hosting-Gebühr erhoben. Diese Variante hat den Vorteil, dass auch kleine, finanzschwache Institutionen ihre wichtigsten Daten abliefern können.
- **Variante «ex post»:** Kosten fallen erst bei einem Rückgriff auf die Daten an. Die Kosten können beispielsweise erlassen werden, wenn der Datenrückgriff nachweislich aufgrund eines Katastrophenfalls geschieht (Elementarschäden, bewaffneter Konflikt etc.). Eine Untervariante kann auch sein, dass die potentiellen Kosten für den Datenrückgriff versichert werden können.

Im Rahmen der vorliegenden Studie ist es noch nicht möglich, eine dieser Varianten zu präferieren. Es gilt aber festzuhalten, dass ein nationaler Bergungsort nur Erfolg haben kann, wenn die datenliefernden Institutionen den Bund für die Einlagerung ihrer Daten höchstens symbolisch entschädigen müssen. Ansonsten werden sie auf kommerzielle Angebote ausweichen wie beispielsweise auf die Amazon-Cloud mit Angeboten wie «Amazon Glacier» und «Glacier Deep

Archive», wo Daten für Preise ab CHF 12.15 pro Terabyte und Jahr sehr günstig eingelagert werden können.<sup>22</sup>

## Umgang mit digitalen Objekten

Nachdem im ersten Teil des Kapitels die gesetzlichen Grundlagen und die mögliche organisatorische Ausgestaltung des Bergungsortes aufgezeigt wurde, konzentriert sich der zweite Teil auf den Umgang mit digitalen Objekten. Im Folgenden wird eine Möglichkeit für die Strukturierung und den Aufbau der Archivpakete vorgeschlagen, wie sie an den digitalen Bergungsort abgeliefert werden könnten. Zudem wird die Notwendigkeit eines verlässlichen Systems für eindeutige Identifikatoren hervorgehoben. Weiter werden funktionale Anforderungen an die Prozesse zur Ablieferung, Überprüfung und Auslieferung von digitalen Objekten definiert.

### Container

Um aus einer Institution Daten an den digitalen Bergungsort zu liefern, müssen sie für die Übertragung und die Speicherung in geeigneter Form paketiert werden. Mit der Paketierung wird aus einzelnen Dateien eine Einheit geschnürt, ähnlich einer Archivschachtel oder einem Aktenbündel. Im Sinne des OAIS-Modells speichert der digitale Bergungsort nicht einzelne Dateien, sondern ganze Informationspakete respektive digitale Objekte. Die Pakete können aus einer einzelnen, aber auch aus sehr vielen Dateien bestehen und wiederum in Unterstrukturen in Form von Ordnern und Unterordnern aufgeteilt sein. Zudem tragen solche Pakete zusätzliche Metadaten (beschreibende Information), um beispielsweise die Provenienz, eine inhaltliche Beschreibung oder eindeutige Identifikatoren festzuhalten. Zu diesen Metadaten zählen auch Checksummen, welche die Überprüfung der Integrität der Dateien zulassen.

Für die Paketierung existieren heute verschiedene Containerformate, die sich teilweise schon seit vielen Jahren in grossen Archiven und Bibliotheken bewährt haben. Im Rahmen der weiteren Planung und Feinkonzeption des Bergungsortes muss ein Containerformat in den nötigen Details spezifiziert werden.

Für die vorliegende Studie wird exemplarisch das Format **BagIt** verwendet, um aufzuzeigen, wie ein solches Format funktioniert. BagIt wurde gemeinsam von der California Digital Library und der Library of Congress entwickelt.<sup>23</sup> Das Format ist nach einfachen Prinzipien aufgebaut, offen dokumentiert und für die Erzeugung nicht an Spezialsoftware gebunden. Ein BagIt-Paket kann mit sehr einfachen Skripten in allen Betriebssystemen erzeugt werden.

Ein Container (genannt „Bag“) enthält die folgenden Elemente:

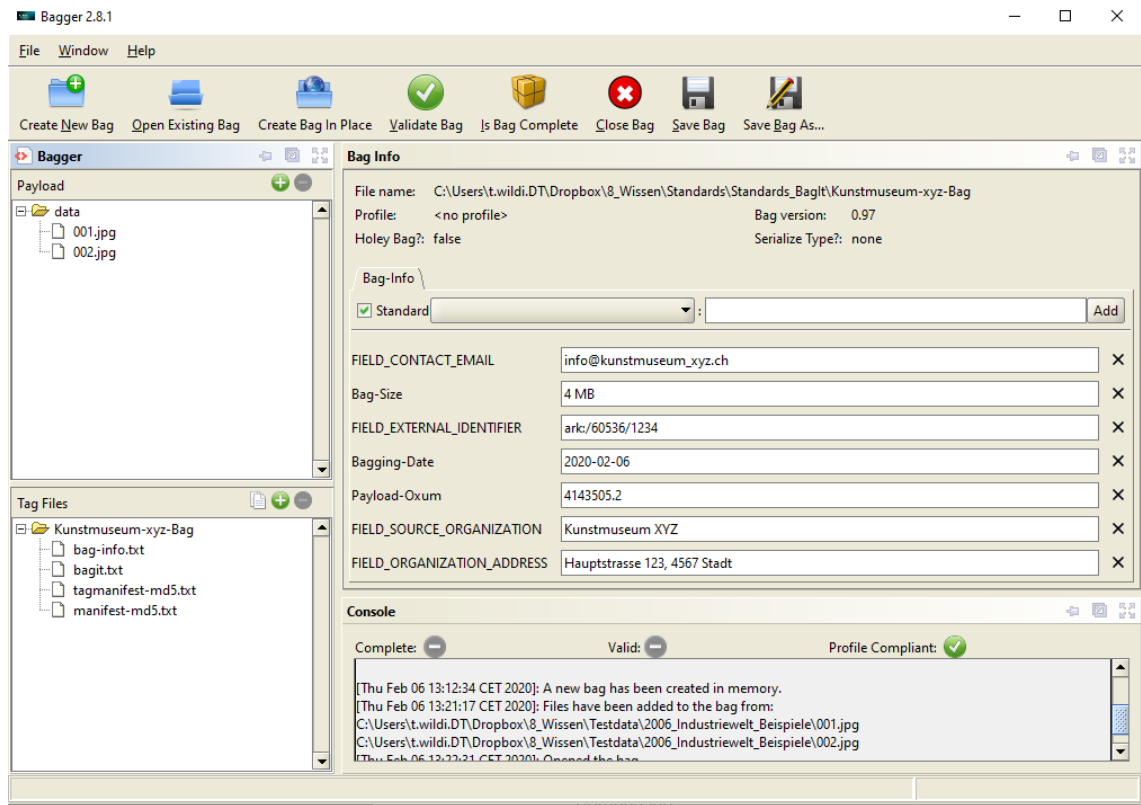
- **Ordner «data»:** In diesem Ordner werden die zu archivierenden Dateien (Primärdaten) abgelegt. Der Ordner kann auch weitere Unterordner beinhalten.
- **bagit.txt-Datei:** Identifiziert den Ordner als Bag.
- **bagit-info.txt:** Enthält beschreibende und technische Metadaten, beziehungsweise Tags.
- **manifest-md5.txt:** Checksummen für jede Datei im Ordner «data», gebildet mit MD5, andere Algorithmen können ebenfalls verwendet werden und erzeugen entsprechend anders benannte Checksummendateien.

---

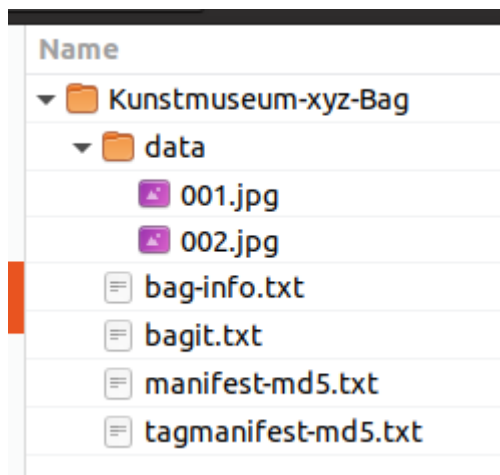
<sup>22</sup> <https://aws.amazon.com/de/glacier/>. Abgerufen am 17.1.2020, Speicherpreis zu diesem Zeitpunkt für «S3 Glacier Deep Archive» 0.00099 USD pro GB und Jahr, entspricht USD 12.16 pro TB und Jahr.

<sup>23</sup> The BagIt File Packaging Format (V1.0). J. Kunze; J. Littman; E. Madden; J. Scancellia; C. Adams. 17 September 2018. URL: <https://tools.ietf.org/html/draft-kunze-bagit-17>

Das folgende Beispiel zeigt die Bildung eines Bags mit Hilfe der frei verfügbaren Software «Bagger».<sup>24</sup> Es werden zwei Bilddateien «001.jpg» und «002.jpg» verpackt und verschiedene Metadaten zur Identifikation und Angabe der Provenienz beigefügt. Ein solcher Bag wäre bereit für die Speicherung im digitalen Bergungsort.



Die Struktur des Bags sieht im Dateisystem wie folgt aus:



In der Datei bag-info.txt werden folgende Metadaten gespeichert:

```
FIELD_SOURCE_ORGANIZATION: Kunstmuseum XYZ
FIELD_ORGANIZATION_ADDRESS: Hauptstrasse 123, 4567 Stadt
```

<sup>24</sup> <https://github.com/LibraryOfCongress/bagger>

```
FIELD_CONTACT_EMAIL: info@kunstmuseum_xyz.ch
FIELD_EXTERNAL_IDENTIFIER: ark:/60536/1234
Payload-Oxum: 4143505.2
Bagging-Date: 2020-02-06
Bag-Size: 4 MB
```

Bags lassen sich grundsätzlich betriebssystemunabhängig erzeugen, auf Integrität überprüfen und archivieren. Es existieren dafür Open Source-Programme, Skripte oder Programmbibliotheken in unterschiedlichen Programmiersprachen.<sup>25</sup> Für den vereinfachten Transport können Bags zusätzlich in einen Tar- oder Zip-Container gepackt werden, so dass nur eine einzige Datei übermittelt werden muss.

Der **Vorteil** von BagIt gegenüber anderen in Gedächtnisinstitutionen verbreiteten Containerstandards wie METS<sup>26</sup> oder in der Schweiz dem Ablieferungsstandard eCH-0160<sup>27</sup> ist die Einfachheit in der Bildung, Verwendung und Überprüfung der Pakete. Dank der breit verfügbaren Software können BagIt-Container auch von kleinen Institutionen, die nur über beschränkte IT-Ressourcen verfügen und ohne spezialisiertes IT-Personal auskommen müssen, selber gebildet werden. BagIt ist ein sehr generisches Format, das von allen Typen von Gedächtnisinstitutionen genutzt werden kann und das über einige wenige Standard-Metadaten hinaus keine Einschränkungen bezüglich Daten- und Metadatenformaten macht.

Der **Nachteil** von BagIt sind fehlende Mechanismen für die Versionierung von Inhalten. Die Inhalte von einmal im Bergungsort gespeicherten Bags können nicht nachträglich ergänzt oder verändert werden, ohne dass der gesamte Bag neu geschrieben werden muss. Bei Änderungen muss also ein Bag komplett neu gebildet und nochmals abgeliefert werden. Hier stellt sich auch die Frage, ob und über welchen Prozess Bags im Bergungsort gelöscht werden können. Diese Möglichkeit muss grundsätzlich bestehen, denn es ergibt wenig Sinn, fehlerhafte oder veraltete Bags dauerhaft zu speichern.

### Identifikatoren

Wenn ein Bag an den Bergungsort übergeben wird, muss ihm ein persistenter Identifikator (Persistent Identifier, PID) zugewiesen werden. Der PID dient der weltweit eindeutigen und dauerhaften Referenzierung eines digitalen Objekts, über die auch ein allfälliger Rückgriff erfolgt. Auch im bestehenden Mikروفilmarchiv kommt der eindeutigen Identifikation der einzelnen Filmrolle eine hohe Bedeutung zu. Für jeden Film wird eine Kontrollkarte mit mehreren Durchschlägen angefertigt, diese gibt Auskunft über den Ort der Einlagerung innerhalb des Archivs. Diese Kontrollkarten werden redundant sowohl beim Bund als auch beim abliefernden Kanton aufbewahrt.

Es existieren heute mehrere Möglichkeiten und Systeme, um eindeutige Identifikatoren für digitale Objekte zu bilden. Vor allem im akademischen Kontext (Forschungsdaten und akademische Paper) und für elektronische Publikationen werden «**Digital Object Identifier**» (**DOI**) verwendet.<sup>28</sup> Die DOI werden durch eine Institution gebildet und dann bei einer «Registration Agency» angemeldet. Diese «Registration Agencies» basieren grundsätzlich auf einem kommerziellen Geschäftsmodell. Die DOI verursachen also Fixkosten, wie hoch diese sind, bleibt

---

<sup>25</sup> Für eine Übersicht über die Werkzeuge siehe: <https://de.wikipedia.org/wiki/BagIt>, <https://en.wikipedia.org/wiki/BagIt>

<sup>26</sup> <http://www.loc.gov/standards/mets/>

<sup>27</sup> <http://www.ech.ch/de/standards/39187>

<sup>28</sup> <https://www.doi.org/>

jeder Registrierungsstelle überlassen. Zudem gibt das DOI-System vor, wie der Identifier aufgebaut sein muss. Dies macht das DOI-System wenig attraktiv für den spezifischen Anwendungsfall Bergungsort.<sup>29</sup>

Für die Identifizierung der datenliefernden Institutionen kann der **ISIL-Code** verwendet werden. ISIL basiert auf der Norm ISO 15511:2011 und dient der eindeutigen Identifizierung von Bibliotheken, Archiven und verwandten Institutionen. In der Schweiz vergibt die Nationalbibliothek die ISIL-Kennzeichen mit dem Präfix *CH*.<sup>30</sup> Mit dem ISIL-Code kann jedoch nur die Institution, nicht aber eine einzelne Ressource innerhalb der Institution referenziert werden, aus diesem Grund eignet sich ISIL nicht als Identifier-System für den Bergungsort. Die meisten Gedächtnisinstitutionen in der Schweiz verfügen aber über einen ISIL-Eintrag. Er kann zur eindeutigen Identifikation der Provenienz den digitalen Objekten als Metadatum mitgegeben werden.

Ein weiteres System zur Vergabe von PID ist der **«Archival Resource Key» (ARK)**. Der ARK setzt sich zusammen aus einem Identifier der Institution und einer internen Bezeichnung (z. B. Laufnummer). Jede abliefernde Institution löst sich kostenlos eine **«Name Assigning Authority Number» (NAAN)** über ein Formular der California Digital Library.<sup>31</sup> Das einzelne digitale Objekt wird dann über eine Bezeichnung oder Laufnummer innerhalb der Institution eindeutig identifiziert. Der komplette ARK setzt sich aus den folgenden Komponenten zusammen:

- **NAAN:** Name Assigning Authority Number, eindeutiger Identifikator pro Institution.
- **NMAH:** Name Mapping Authority Host, optionaler und austauschbarer Hostname einer Organisation.
- **LocalID:** eindeutiger Identifier innerhalb der Institution, frei zu vergeben, auch in der Struktur frei zu wählen. Es muss mit ARK somit nicht ein neues Identifier-System eingeführt werden, sondern bereits bestehende interne Identifier, Signaturen oder Nummernsysteme können weiterverwendet und werden.
- **Qualifier:** optionale weitere Informationen zu Subkomponenten oder Varianten.

Die Komponenten werden nach dem folgenden Schema zusammengefügt:

```
[http://NMAH/]ark:/NAAN/LocalID[Qualifier]
```

Ein kompletter Namenseintrag in der NAAN-Datenbank lautet wie folgt:

```
ark:/60536:
  type: "naan"
  manager: "n2t"
  name: "docuteam (=) DOCUTEAM"
  date: "2018.12.05"
  redirect: "https://docuteam.ch/ark:$id"
  na_policy: "FP | (:unkn) unknown | 2018 |"
```

<sup>29</sup> Die französische Nationalbibliothek vergleicht in einem Blog-Post das DOI-System mit anderen Identifier-Systemen und thematisiert dort die Fixkosten von DOI: <https://www.bnf.fr/fr/centre-d-aide/identifiants-internationaux>

<sup>30</sup> <https://www.nb.admin.ch/snl/de/home/fachinformationen/isil.html>

<sup>31</sup> Formular, um für die eigene Institution einen kostenlosen NAAN zu beantragen: <https://docs.google.com/forms/d/e/1FAIpQLSfd1CX6idwLB47g8OGKUG654auV8IU8yI7DAs61cXGOoFDn0g/viewform?c=0&w=1>

Ein fiktiver ARK-Identifizier für eine digitale Ressource im Firmenarchiv von docuteam würde also lauten:

`https://docuteam.ch/ark:/60536/01234`

Wenn diese Ressource im digitalen Bergungsort gespeichert wird, dann ist keine Namensauflösung über einen Host notwendig. Es genügt die folgende Angabe:

`ark:/60536/01234`

Der **Vorteil** von ARK ist, dass das Identifier-System zwar auf die einmalige Vergabe von Institutionseinträgen in Form von NAAN angewiesen ist, ansonsten aber autonom ohne weitere involvierte Stellen funktioniert. Präventiv ist im Bergungsort eine Liste der NAAN-Einträge der abliefernden Institutionen zu archivieren.<sup>32</sup> Auch wenn in einem Katastrophenfall kein Zugriff auf die zentrale NAAN-Datenbank mehr möglich ist, so ist die Zuordnung der digitalen Objekte zu ihren Provenienzen weiterhin gewährleistet. Ein weiterer Vorteil von ARK ist, dass keine Kosten für eine Registrierung entstehen.

Unabhängig vom zu wählenden Identifier-System stellt sich die Frage, wie granular im Bergungsort Identifier vergeben werden sollen.

**Variante A:** Im Minimum erhält der Container (Bag) einen Identifier. Damit ist er für den Bergungsort eindeutig identifizierbar. Wie dann die einzelnen Elemente innerhalb des Containers identifiziert werden, liegt bei dieser Variante im Aufgabenbereich der abliefernden Institution:

Name	
▼ Kunstmuseum-xyz-Bag	ark:/60536/1
▼ data	
001.jpg	
002.jpg	

**Variante B:** Zusätzlich zur Identifikation des Containers identifiziert der Bergungsort auch jede einzelne Ressource (Primärdateien und allfällige Unterordner) innerhalb eines Containers:

Name	
▼ Kunstmuseum-xyz-Bag	ark:60536/1
▼ data	
001.jpg	ark:60536/2
002.jpg	ark:60536/3

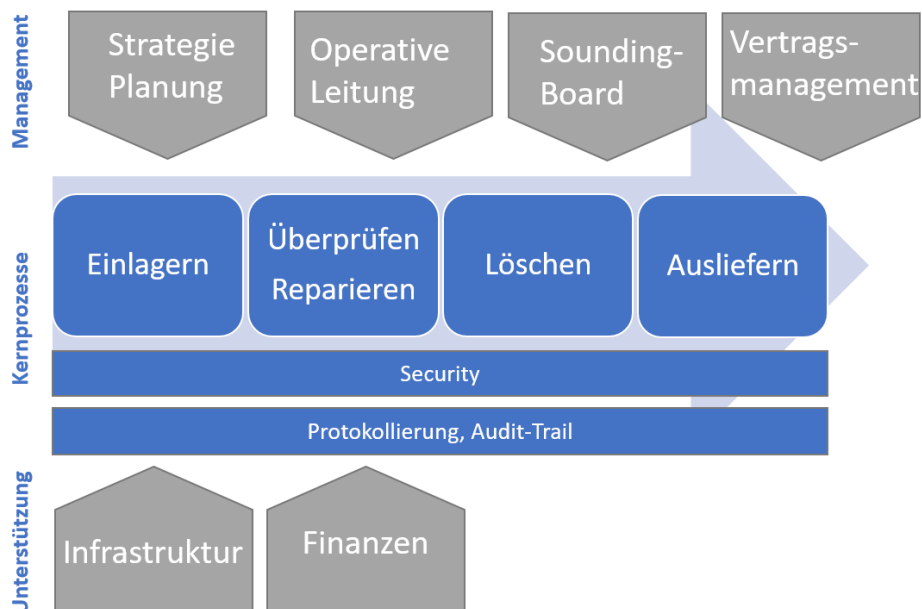
Die Variantenwahl wird von unterschiedlichen Faktoren abhängen. Die Praxis zeigt klar, dass die Identifikation jeder einzelnen Ressource oder Datei Vorteile bietet, die oft erst bei späteren

<sup>32</sup> Die gesamte NAAN-Datenbank ist knapp über 100 kB gross (respektive klein) und kann über folgenden Link heruntergeladen werden: [https://n2t.net/e/pub/naan\\_registry.txt](https://n2t.net/e/pub/naan_registry.txt)

Ausbaustufen eines digitalen Archivs richtig zum Tragen kommen. Vorteile sind etwa, dass technische/beschreibende Metadaten nicht nur dem gesamten Container, sondern auch einzelnen Dateien zugewiesen werden können. Zudem ist eine allfällige Auslieferung einzelner Dateien oder Ordner aus dem Bergungsort nur möglich, wenn diese Elemente auch eindeutig identifizierbar sind. Dies alles sind Szenarien, die vorderhand ausserhalb des angedachten Funktionsumfangs liegen. Aber bei einer guten Planung der Identifikatoren-Vergabe wird es keine Behinderung von späteren Ausbaustufen des Bergungsortes aufgrund ungünstig gewählter Identifikationssysteme geben.

### Prozesse im Umgang mit digitalen Objekten

Nach der Sicht auf die Container und deren Identifikatoren wird im folgenden Teil der Fokus auf die Geschäftsprozesse des Bergungsortes gelegt. Eine noch grobe Prozesslandkarte unterteilt in die üblichen Kategorien von Management-, Unterstützungs- und Kernprozessen sieht wie folgt aus:



Innerhalb der Kernprozesse werden folgende Tätigkeiten erbracht:

#### 1. Einlagern von digitalen Objekten:

In den Prozess involviert sind die abliefernde Institution sowie die Betriebsorganisation des Bergungsortes.

- Die Institution wählt Daten in Absprache mit dem KGS-Verantwortlichen des Kantons für die Ablieferung aus und strukturiert sie.
- Sie erstellt für die Ablieferung einen oder mehrere Container mit Hilfe von Software, die sie vom Bergungsort zur Verfügung gestellt bekommt oder die ihr empfohlen wird.
- Diese Arbeiten erbringt die Institution selbst oder sie beauftragt dafür einen spezialisierten Dienstleister – genau wie sie dies zur Erstellung von Mikrofilmen in der Vergangenheit auch schon gemacht hat.
- Die Daten werden über einen geeigneten Transportweg an den Bergungsort übermittelt. Ob das über eine geschützte Online-Plattform oder bei grossen Datenmengen durch die Übergabe physischer Medien geschieht, muss spezifiziert werden.



- Konzipiert werden muss auch, ob im Bergungsort aus Sicherheitsgründen initiale Validierungsschritte, wie zum Beispiel eine Virenprüfung oder Prüfung von Metadaten auf Vollständigkeit, vorgenommen werden sollen.
- Die Container und eventuell auch ihre Bestandteile (Ordner, Dateien) erhalten eindeutige Identifier, falls sie nicht schon mit solchen angeliefert wurden.
- Die Daten werden im Bergungsort in mehreren Instanzen gespeichert.
- Wenn die Speicherung und Replikation erfolgreich abgeschlossen sind, erhält die abliefernde Institution eine entsprechende Bestätigung zusammen mit den eindeutigen Identifikatoren ihrer abgelieferten Container.
- Die Ablieferung wird protokolliert.

### 2. *Überprüfen und gegebenenfalls Reparieren von digitalen Objekten:*

Für diesen Prozess ist der digitale Bergungsort verantwortlich. Der Prozess läuft periodisch ganz- oder teilautomatisiert ab.

- Durchführung von Prüfschritten in unterschiedlicher Periodizität und Tiefe. Überprüft wird, ob im digitalen Objekt
  - o die korrekte Anzahl Dateien vorhanden ist,
  - o die korrekte Anzahl Bytes vorhanden ist,
  - o die Checksummen stimmen.
- Oberflächliche Prüfungen wie Anzahl Dateien oder Bytes sind weit weniger rechenintensiv und somit zeitsparender wie die Prüfung der Checksumme jeder einzelnen Datei. Diese Prüfungen geben erste wichtige Hinweise über die Vollständigkeit der Speicherbereiche.
- Eine vertiefte Prüfung des Archivspeichers erfolgt, indem die Integrität jeder Datei anhand ihrer Checksumme geprüft wird.
- Der Überprüfungsprozess muss alle Kopien respektive Instanzen des Archivspeichers umfassen.
- Bei Fehlerfällen wird ein Unterprozess in Gang gesetzt, welcher korrekte und fehlerhafte Instanzen identifiziert und fehlerhafte Speicherbereiche repariert. Der Auftrag für solche Vorgänge wird je nach Fall automatisiert oder manuell in Auftrag gegeben.
- Wenn der Archivspeicher des digitalen Bergungsortes geografisch über mehrere Standorte verteilt ist und wenn zudem noch verschiedene Speichertechnologien zum Einsatz kommen, dann ist die Organisation und Automatisierung des Überprüfungs- und Reparaturprozesses mit erheblichem Aufwand verbunden.
- Protokollieren der Vorgänge.

### 3. *Löschen von digitalen Objekten:*

Das Löschen von Ablieferungen stellt einen Ausnahmefall dar, der aber mitbedacht werden muss. Ein Löschvorgang kann aufgrund gesetzlicher oder archivfachlicher Vorgaben nötig sein. Gründe dafür können Änderungen in der Archivgesetzgebung in einem Kanton sein, fehlerhafte Ablieferungen, die ersetzt werden sollen, oder die Löschung von Dateien in obsoleten Formaten, die in neuer Form bereits wieder eingelagert wurden. In den Löschmodus involviert sind genau gleich wie bei der Einlagerung die abliefernde Institution und die Betriebsorganisation des Bergungsortes.

- Identifikation des/der zu löschenden Container anhand seines Identifiers.
- Ausfertigung eines Löschauftrags nach Vieraugenprinzip, z. B. gemeinsam unterzeichnet durch die Institution und den KGS-Beauftragten des Kantons.

- Durchführen der Löschung durch die Betriebsorganisation. Löschen der digitalen Objekte auf allen Instanzen des Speichers. Je nach eingesetzter Speichertechnologie wird die Löschung mit grosser zeitlicher Verzögerung stattfinden.
- Protokollieren des Löschvorgangs. Technische Metadaten von gelöschten digitalen Objekten werden zu Dokumentationszwecken weiterhin archiviert. Der Nachweis zu digitalen Objekten verschwindet trotz Löschung nicht spurlos.

#### 4. *Ausliefern von digitalen Objekten:*

In den Prozess involviert sind die abliefernde Institution sowie die Betriebsorganisation des Bergungsortes.

- Die Institution meldet die Identifier der auszuliefernden digitalen Objekte.
- Die Betriebsorganisation des Bergungsortes erzeugt eine Kopie der Daten und übermittelt diese über einen geeigneten Transportweg an die Institution. Ob das über eine geschützte Online-Plattform oder bei grossen Datenmengen durch die Übergabe physischer Medien geschieht, muss spezifiziert werden.
- Vorgesehen ist, dass digitale Objekte grundsätzlich an die datenliefernde Institution übermittelt werden. Wenn Institutionen aufgelöst oder zusammengelegt werden, dann ist zu definieren, in wessen Besitz die digitalen Objekte im Bergungsort übergehen und an wen diese künftig ausgeliefert werden.
- Protokollierung der Auslieferung.

Die folgenden zwei Prozesse gehören ebenfalls zu den Kernaufgaben des digitalen Bergungsortes, befassen sich aber nicht direkt mit der Einlagerung oder Auslieferung digitaler Objekte.

#### *Security-Prozess:*

Regelmässige Überprüfung der Gefahrenszenarien und der Massnahmen. Absprache und Austausch mit anderen Gremien, wie der Gruppe SKI des BABS. Neue Cyber-Gefahrenbilder werden periodisch analysiert und in die Infrastrukturplanung aufgenommen.

#### *Protokollierungsprozess und Audit-Trail:*

Sämtliche Aktionen, die in den Kernprozessen vorgenommen werden, sind in standardisierter Form zu protokollieren. Dieser Audit-Trail gehört zu den Nachweisakten des digitalen Bergungsortes und ist zu archivieren. Die Protokolle schaffen Transparenz, sie weisen nach, welche Massnahmen im Bergungsort getroffen wurden, und dienen als wichtige vertrauensbildende Massnahmen.<sup>33</sup>

Ausgangspunkt für einen standardisierten Protokollierungsprozess im Bereich der digitalen Archivierung ist die Sammlung von «Preservation Vocabularies» der Library of Congress.<sup>34</sup> Diese Vokabularien decken ganz unterschiedliche Aktionen ab, die beim Betrieb eines digitalen Archivs typischerweise anfallen.

---

<sup>33</sup> Der Protokollierungsprozess als Grundlage für ein vertrauenswürdigen digitales Archiv wird behandelt im Kapitel «Capturing Audit Trail Data» in: *Bantin*, Building trustworthy digital repositories, 169–197.

<sup>34</sup> Folgender Ausgangspunkt verlinkt die unterschiedlichen Vokabularien: <http://id.loc.gov/vocabulary/preservation.html>. Wichtig für die Dokumentation der Prozessschritte sind vor allem die unterschiedlichen «Event Types», die auftreten können: <http://id.loc.gov/vocabulary/preservation/eventType.html>.

## Infrastruktur und Sicherheit

Der nachhaltige Betrieb des zukünftigen digitalen Bergungsortes baut auf einer verlässlichen und stabilen Infrastruktur auf. Der erste Schritt zum Entwurf einer solchen Infrastruktur besteht in der Formulierung grundsätzlicher Leitlinien und Prinzipien. Es werden im folgenden Kapitel keine konkreten Technologien diskutiert oder spezifiziert, sondern ausschliesslich Anforderungen formuliert, die aus fachlicher Sicht sinnvoll erscheinen.

Im späteren Betrieb werden die verschiedenen technischen Komponenten, sowohl Hardware wie auch Software, periodisch modernisiert und ausgewechselt. Auch wenn die Umgebung ausschliesslich der Langzeitarchivierung dient, wird sie sich dem technischen Wandel nicht entziehen können: Ein typisches Merkmal digitaler Langzeitarchive ist, dass die Geschäftsprozesse (beschrieben im letzten Kapitel) über sehr viel längere Zeit stabil sind als die technischen Komponenten, mit denen sie umgesetzt werden. Diese unterschiedlichen Geschwindigkeiten müssen bei der Konzeption der Infrastruktur mitbedacht werden. Die nachfolgenden vier Unterkapitel strukturieren die fachlichen Anforderungen an die Infrastruktur des digitalen Bergungsortes. Selbstredend muss die Infrastruktur des digitalen Bergungsortes regelmässig überprüft und gegebenenfalls erneuert werden:

- Technische Komponenten erreichen das Ende ihres Lebenszyklus und müssen ersetzt werden.
- Neue Cyber-Risiken werden erkannt und müssen berücksichtigt werden
- Zusammen mit den datenliefernden Institutionen wird der Funktionsumfang des Bergungsortes erweitert.

Die Infrastruktur des Bergungsortes wird sich also ständig wandeln.

### Dezentral und verteilt

Die Resilienz des digitalen Bergungsortes steigt, wenn seine Infrastruktur **dezentral und verteilt** aufgebaut wird. Dies bedeutet, dass idealerweise keine Aufgabe, weder organisatorisch noch technisch, an eine einzige Stelle gebunden ist. Beispielsweise würde ein zentrales Katalogsystem oder eine Datenbank von Identifikatoren und Checksummen nur an einem Standort ein Sicherheitsrisiko bedeuten. Genau aus diesem Grund werden bereits heute die Kontrollkarten des Mikrofilmarchivs sowohl beim BABS als auch bei den Kantonen abgelegt.

Die Aufgaben und Verantwortungen für den Bergungsort müssen verteilt werden oder sich beim Ausfall eines Akteurs oder Systems zeitnah auf andere Organisationen übertragen lassen.

Denn wenn der Bergungsort auf einer einzelnen Softwareinstanz, einer einzigen Hardwareplattform oder einigen wenigen Personen mit umfassender technischer Kontrolle basiert, kann beim Ausfall einer einzelnen Komponente das Archiv als Ganzes gefährdet sein.

### Teilautomatisierung versus Vollautomatisierung

Ein verteiltes System, das Schäden an den Daten innerhalb eines vordefinierten Zeitraums erkennen und vollautomatisiert beheben kann, ist zwar attraktiv im Betrieb, birgt aber auch Risiken. Erstens kann dieses Verhalten zu einer Überlastung der Netzwerkinfrastruktur führen, insbesondere wenn grosse Datenmengen an unterschiedlichen geografischen Standorten ersetzt werden müssen. Zweitens birgt es auch das Risiko, dass sich eventuell eingeschleppte **Schadsoftware** wie Verschlüsselungstrojaner **automatisiert auf sämtliche vorhandene Kopien ausbreiten** und diese ebenfalls kompromittieren. Die Datenreparatur muss auf einem sogenannten Polling-Mechanismus basieren, also auf Umfragen zur Datenintegrität, die zwischen den einzelnen Kopien stattfinden. Eine automatische Reparatur darf nur in Fällen erfolgen, wo

es einen überwältigenden Konsens gibt, wo also klar ist, dass bei einer einzelnen Kopie beispielsweise ein Ausfall von Hardware aufgetreten ist. In allen anderen Fällen hat eine manuelle Bestätigung zur Reparatur zu erfolgen. Dieser mit Absicht nur teilautomatisierte Ansatz verschafft Zeit zu einer vertieften Untersuchung von Vorkommnissen und für eine geplante Wiederherstellung der Speicherinstanzen. Der teilautomatisierte Ansatz ist eine präventive Massnahme gegen Cyber-Angriffe, die die Erkennung von Manipulationen erlauben soll, bevor alle Kopien gefährdet sind. Der Bergungsort stellt einen Anwendungsfall dar, bei dem es kaum eine Rolle spielt, ob die Wiederherstellung von Speicherinstanzen Tage, Wochen oder sogar Monate dauert. Deshalb können in einem solchen Umfeld teilautomatisierte Lösungen durchaus eingesetzt werden.

Ein konkretes Beispiel eines Systems, das diese Anforderung umsetzt, ist **LOCKSS** respektive **«Lots of Copies Keep Stuff Safe»**.<sup>35</sup> LOCKSS ist eine an der Stanford University basierte Initiative rund um ein Open Source-Softwaresystem für den Aufbau und Betrieb verteilter Speicherumgebungen für digitale Archive. Die Software kann für den Aufbau und Betrieb eigener Speichernetzwerke verwendet werden, die über mehrere geografische Standorte und/oder Institutionen hinweg verteilt sind. Rund um LOCKSS besteht eine aktive Community mit vielen Akteuren, die das System nutzen, insbesondere Universitäten und Forschungsbibliotheken.<sup>36</sup>

### **Überprüfung und Sicherstellung der Datenintegrität**

Der Bergungsort stellt eine präventive Schutzmassnahme dar und entsprechend stellt sich die folgende grundsätzliche Frage: Wie können die datenliefernden Institutionen und Kantone heute dem Bergungsort vertrauen, wenn sie die Daten potentiell erst in vielen Jahren oder Jahrzehnten je wieder nutzen werden? Wie wissen sie, ob die im Bergungsort gelagerten Daten noch intakt sind? Es braucht für diesen Zweck regelmässige Kontrollen, um festzustellen, ob die Kopien im Datenspeicher integer sind oder ob Fehler aufgetreten sind. «Integrität» bedeutet in diesem Zusammenhang **«Unverändertheit des Datenstroms»**. Diese Überprüfung findet, wie bereits bei den Geschäftsprozessen beschrieben, in verschiedenen Stufen statt. Im Archivspeicher kann beispielsweise geprüft werden, ob die korrekte Anzahl Dateien und Bytes vorhanden ist. Diese Prüfungen lassen sich mit relativ geringem Rechenaufwand in kurzer Zeit durchführen und erlauben erste Rückschlüsse auf den Gesundheitszustand des Repositories. Eine vertiefte Prüfung wird mit Hilfe der Prüfsummen der einzelnen Dateien durchgeführt. Diese Prüfung ist aufwändig und zeitintensiv, wenn grosse Mengen von Dateien geprüft werden.

Der Normalbetrieb des digitalen Bergungsortes umfasst neben dem Überprüfen der Daten auf Integrität gegebenenfalls auch das Reparieren (zurückspielen von Daten aus unbeschädigten Kopien). Die technische Infrastruktur des Bergungsortes muss darauf ausgelegt sein, diese Aufgaben vorzunehmen und in Form technischer Metadaten in einem Audit-Trail zu protokollieren.

### **Nachhaltige und ressourcenschonende Technologien**

Der digitale Bergungsort wird potentiell eine grosse Datenmenge umfassen und diese Daten müssen über sehr lange Zeiträume vorgehalten werden – sie werden jedoch nur in Ausnahmefällen auch aktiv genutzt. Um in diesem Szenario die Fixkosten für den Betrieb tief zu halten, braucht es Speichertechnologien, die sich unter anderem durch einen tiefen Energieverbrauch auszeichnen.

---

<sup>35</sup> <https://www.lockss.org/>, Dokumentationsportal siehe: <https://lockss.github.io/>

<sup>36</sup> Corrado / Moulaison Sandy, Digital preservation for libraries, archives, and museums, p. 93.

Die Umweltorganisation Greenpeace publiziert in regelmässigen Abständen Studien, in denen sie die Energieeffizienz und den Energiemix kommerzieller Cloudanbieter prüft.<sup>37</sup> In diesen Studien wird eine Reihe von Kriterien formuliert, die als fachliche Anforderungen auch für den digitalen Bergungsort übernommen werden können:

- *Energieeffizienz*: Im Gesamtsystem werden Komponenten mit hoher Energieeffizienz verwendet (Rechenzentrum Gebäude/Stromversorgung/Kühlung; Server; Speichertechnologie).
- *Hohe Zugriffszeiten*: Da der Rückgriff auf die Daten voraussichtlich nur in seltenen Fällen geschieht und eine Datenrückgabe im Normalfall auch vorgängig geplant werden kann, spielen die Zugriffszeiten auf den Datenspeicher eine absolut untergeordnete Rolle. Dies lässt den Einsatz von Offline-Technologien zu.
- *Standby*: Speicherknoten werden zeitweise abgeschaltet oder in einen Standby-Modus versetzt. Voraussetzung ist, dass sie über eine genügend hohe Fehlertoleranz verfügen und sich nach einem Wiederanfahren gegebenenfalls selber reparieren können.
- *Server-zu-Disks-Verhältnis*: Wird ein diskbasiertes Speichersystem verwendet, dann verwaltet jeder Server eine hohe Anzahl von Disks (z. B. >100), um die Energieeffizienz des Gesamtsystems zu steigern.
- *Storage Tiering*: Daten werden auf Speichermedien mit tiefem Energieverbrauch ausgelagert (wie z. B. Tape-Libraries), wobei die periodische Integritätsprüfung gewährleistet sein muss.
- *Erneuerbare Energie*: Der digitale Bergungsort wird ausschliesslich mit erneuerbarer Energie betrieben.

Weitere Verfahren wie Daten-Deduplizierung oder Datenkompression würden die Datenmenge zwar verringern und damit zu einer Einsparung des Energieverbrauchs führen. Diese beiden Massnahmen widersprechen aber wichtigen Grundprinzipien der digitalen Archivierung und werden hier explizit nicht empfohlen.

**Zusammenfassend** ist festzuhalten, dass eine Infrastruktur nach diesen Kriterien in der Schweiz heute so nicht besteht und für einen digitalen Bergungsort neu aufgebaut werden muss, durchaus unter Nutzung existierender Komponenten und Angebote. Bei der **Umsetzung** des digitalen Bergungsortes ist folgendes Vorgehen denkbar: Eine erste Etappe der Umsetzung startet mit wenigen Speicherknoten. In der Folge werden nach und nach weitere Knoten an zusätzlichen Standorten hinzugefügt. Auch wenn das BABS als Betreiberorganisation fungiert, müssen nicht zwingend alle Speicherknoten in Rechenzentren liegen, die unter der Kontrolle des Bundes liegen. Zur Erhöhung der Resilienz können weitere Speicherinstanzen des digitalen Bergungsortes auch auf der Infrastruktur akademischer Rechenzentren (z. B. bei Switch) oder bei grossen Bibliotheken und Archiven aufgebaut werden. So liessen sich die Anforderung «dezentral und verteilt» und bei entsprechender Planung und Organisation auch «teilautomatisiert» nach und nach umsetzen.

---

<sup>37</sup> Vgl. etwa die Studie „Clicking Clean: Who is winning the race to build a green internet“ (Ausgabe 2017)

<https://storage.googleapis.com/planet4-international-stateless/2017/01/35f0ac1a-clickclean2016-hires.pdf>

## Empfohlene Lösungsvariante

Im Verlauf dieser Studie wurden verschiedene Möglichkeiten und Varianten erörtert. Im Sinne eines Fazits wird hier zusammenfassend eine Variante für einen Bergungsort für digitale Kulturgüter empfohlen, die heute sowohl politisch wie auch wirtschaftlich machbar erscheint. Sie zeichnet sich durch die folgenden Merkmale aus:

- Der künftige Bergungsort basiert auf einem **strategischen Auftrag des Bundesrats**, wobei die notwendigen **gesetzlichen Grundlagen** zu schaffen oder anzupassen sind. Der Aufbau und der Betrieb eines digitalen Bergungsortes müssen politisch auf höchster Stufe legitimiert werden.
- Die **zentrale Betriebsorganisation** ist beim **BABS, Fachbereich Kulturgüterschutz** angesiedelt. Die Betriebsorganisation verfügt über die notwendigen technischen und organisatorischen Kompetenzen, eventuell ergänzt durch ein beratendes Gremium, das aus Experten der datenliefernden Institutionen und aus Personen der Forschung zusammengesetzt ist.
- Der Bergungsort basiert wo vorhanden auf den gängigen **internationalen Normen und Standards** und stellt keine Schweizer Sonderlösung dar.
- Die Dienstleistung des digitalen Bergungsort konzentriert sich auf die **Sicherung des Datenstroms**, da eine Überwachung und Migration von Dateiformaten und komplexen Objekten (Websites, Datenbanken) den Rahmen sprengen würde. Den abliefernden Institutionen wird Speicher beispielsweise bis zu einer Grössenordnung von **4 TB je Institution unentgeltlich** zur Verfügung gestellt. Höhere Datenmengen werden zu einem attraktiven Preis verrechnet, so dass für die Institutionen ein Ausweichen auf kommerzielle Cloudanbieter uninteressant ist.
- Die Kantone respektive die einzelnen Institutionen sind für die Selektion, die technische Aufbereitung, die Paketierung und **Ablieferung** der digitalen Kulturgüter an den Bergungsort verantwortlich.
- Die **Auslieferung** der Daten findet grundsätzlich nur in einem **Krisen- oder Katastrophenfall** statt. Der digitale Bergungsort ersetzt nicht den Betrieb institutionseigener Systeme für die digitale Archivierung, auch nicht deren Backup, sondern stellt ein zusätzliches **Sicherheitsnetz** dar.
- Die Verwendung von **BagIt als Containerformat und ARK als Identifiersystem** stellen konkrete technische Möglichkeiten zur Organisation und Identifizierung digitaler Objekte dar. Diese Formate müssen in Konzeptions- und Umsetzungsphasen vertieft geprüft werden, die Studie will ausdrücklich kein Präjudiz schaffen.
- Die eingesetzte **IT-Infrastruktur** muss nach und nach ausbaubar sein und insbesondere die Kriterien «dezentral und verteilt» wie auch «teilautomatisiert» abdecken. Neue Cyber-Gefahrenbilder werden regelmässig analysiert und in die Infrastrukturplanung aufgenommen.

Der Aufgabenbereich des zukünftigen Bergungsortes muss sorgfältig eingegrenzt und auf die Kernfunktionalitäten rund um die Datenstrom-Archivierung konzentriert werden. Nur so bleiben die Investitions- und Betriebskosten in einem überschaubaren Rahmen und das Vorhaben wird finanzierbar und realisierbar. Damit bietet sich der Schweiz die Chance, eine internationale Vorreiterrolle für die präventive Sicherung digitaler Kulturgüter zu übernehmen.

## Literaturverzeichnis

*Bantin*, Philip C. (Hrsg), Building trustworthy digital repositories. Theory and implementation, Lanham 2016.

Bundesamt für Bevölkerungsschutz, Risiko- und Verwundbarkeitsanalyse des kritischen Teilssektors Kulturgüter. Bericht zur Umsetzung der Massnahme 2 der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken NCS im Teilssektor Kulturgüter, Bern 2017.

*Burda*, Daniel / Angelina Dunga Winterleitner / Beat Estermann, Digitale Langzeitarchivierung in der Schweiz. Ergebnisse einer Studie im Auftrag der Schweizerischen Nationalbibliothek, Bern 2017.

*Corrado*, Edward M. / Heather Moulaison Sandy, Digital preservation for libraries, archives, and museums, Second edition, Lanham 2017.

nestor-Arbeitsgruppe Vertrauenswürdige Archive - Zertifizierung, Kriterienkatalog vertrauenswürdige digitale Langzeitarchive, hrsg. v. Astrid Schoger / Susanne Dobratz (nestor-materialien, 8), Frankfurt am Main 2008.

## Gesetzestexte

Botschaft zur Totalrevision des Bevölkerungs- und Zivilschutzgesetzes

<https://www.news.admin.ch/news/message/attachments/54621.pdf>

Haager Abkommen für den Schutz von Kulturgut bei bewaffneten Konflikten

<https://www.admin.ch/opc/de/classified-compilation/19540079/index.html>

KGSG Bundesgesetz über den Schutz der Kulturgüter bei bewaffneten Konflikten, bei Katastrophen und in Notlagen

<https://www.admin.ch/opc/de/classified-compilation/20122172/index.html>

KGSV Verordnung über den Schutz der Kulturgüter bei bewaffneten Konflikten, bei Katastrophen und in Notlagen

<https://www.admin.ch/opc/de/classified-compilation/20132905/index.html>

Strategie zum Schutz des gefährdeten Kulturerbes 2019–2023

<https://www.news.admin.ch/news/message/attachments/56039.pdf>

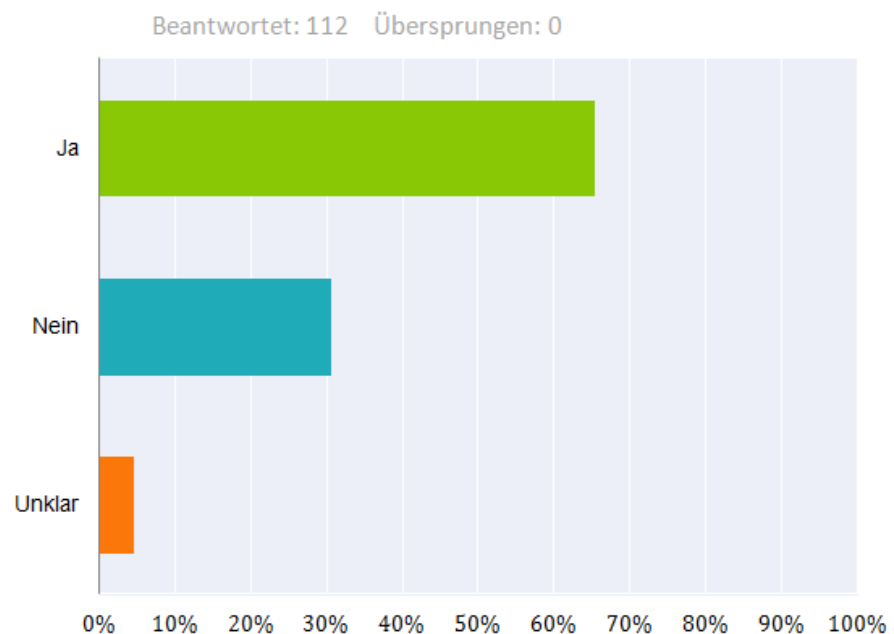
VSFS Verordnung des VBS über Sicherstellungsdokumentationen und fotografische Sicherheitskopien

<https://www.admin.ch/opc/de/classified-compilation/20152486/index.html>

## Anhang: Ergebnisse der Umfrage 2016

Die folgenden drei Fragen aus der Umfrage des dhlab der Universität Basel von 2016 haben inhaltlich einen direkten Zusammenhang mit vorliegender Studie und zeigen auf, dass bereits heute grosse Mengen an digitalen Originalen in den Gedächtnisinstitutionen gelagert werden. Ein digitaler Bergungsort als nationale Disaster Recovery-Strategie würde die Resilienz dieser Institutionen stärken.

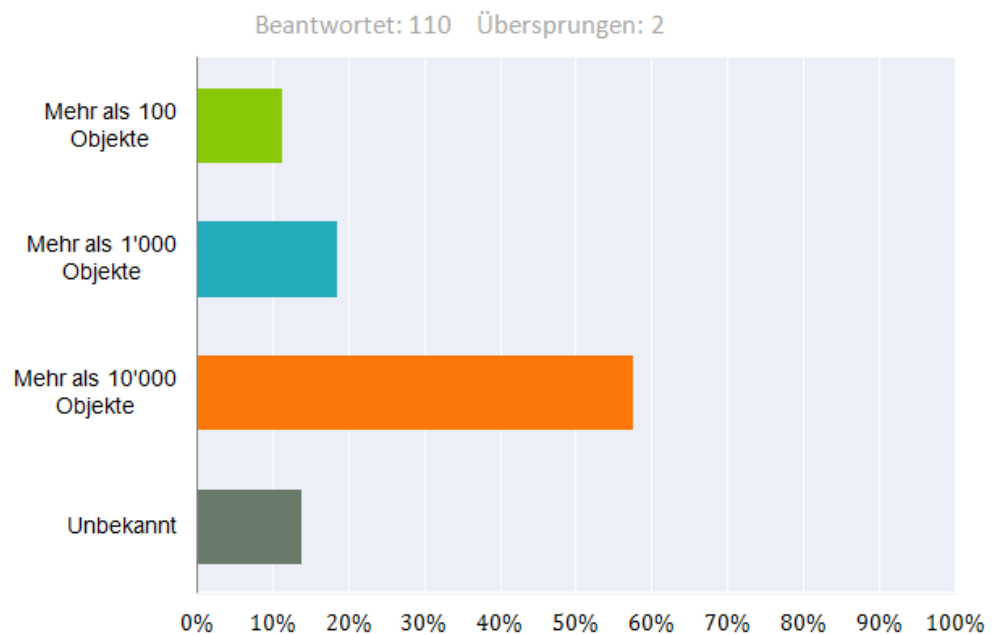
### Frage 1 Stellen digitale Daten (primäre Quellen, digitale Reproduktionen, Fotografien...) einen signifikanten Teil der Sammlung Ihrer Institution dar?



Antwortoptionen	Beantwortungen	Anzahl
Ja	65,18%	73
Nein	30,36%	34
Unbekannt	4,46%	5
<b>Gesamt</b>		<b>112</b>

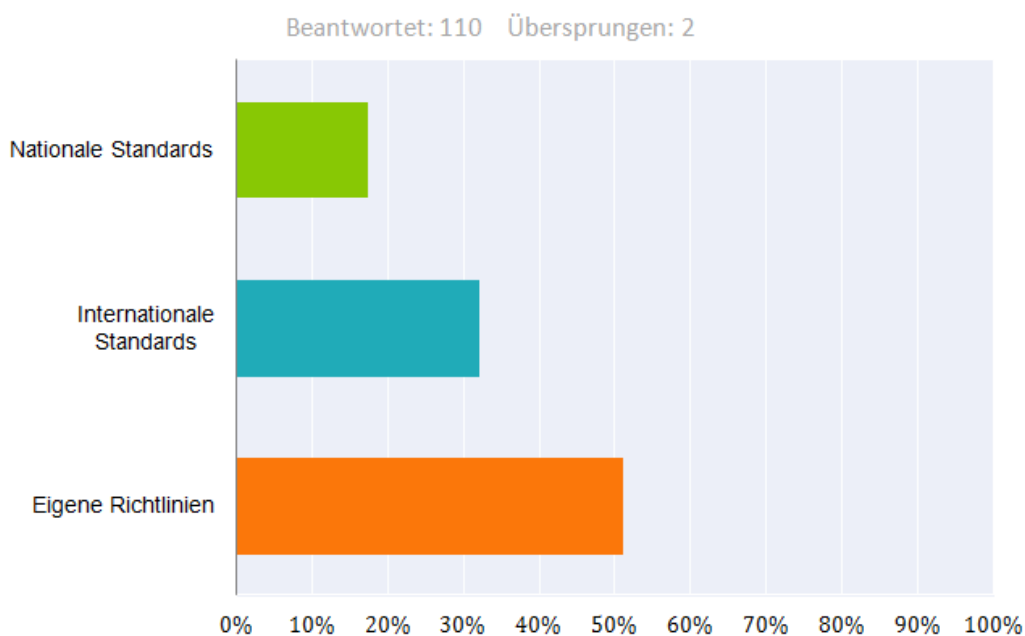


## Frage 2 Wie gross ist etwa der digitale Bestand Ihrer Sammlung?



Antwortoptionen	Beantwortungen	Anzahl
Mehr als 100 Objekte	10,91%	12
Mehr als 1'000 Objekte	18,18%	20
Mehr als 10'000 Objekte	57,27%	63
Unbekannt	13,64%	15
<b>Gesamt</b>		<b>110</b>

**Frage 11 Richtet sich die Vorgehensweise bei der digitalen Archivierung nach nationalen oder internationalen Standards und Empfehlungen?**



Antwortoptionen	Beantwortungen	
Die Vorgehensweise richtet sich nach nationalen Standards	17,27%	19
Die Vorgehensweise richtet sich nach internationalen Standards (z. B. nach DIN, ISO)	31,82%	35
Wir orientieren uns an eigenen Richtlinien	50,91%	56
<b>Gesamt</b>		<b>110</b>