

Jens Ludwig / Harry Enke (Hrsg.)

# Leitfaden zum Forschungsdaten-Management

Handreichungen aus dem WissGrid-Projekt



GEFÖRDERT VOM



vwh

Ludwig/Enke (Hrsg.) · Leitfaden zum Forschungsdaten-Management



Jens Ludwig/Harry Enke (Hrsg.)

# Leitfaden zum Forschungsdaten- Management

Handreichungen aus dem WissGrid-Projekt

**vwh**

Verlag Werner Hülsbusch  
Fachverlag für Medientechnik und -wirtschaft

J. Ludwig / H. Enke (Hrsg.): Leitfaden zum Forschungsdaten-Management

**Bibliografische Information der Deutschen Bibliothek**

Die Deutsche Bibliothek verzeichnetet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet unter <http://dnb.ddb.de> abrufbar.

Verlag Werner Hülsbusch, Glückstadt, 2013



[www.vwh-verlag.de](http://www.vwh-verlag.de)

– in Kooperation mit dem Universitätsverlag Göttingen –

Einfache Nutzungsrechte liegen beim Verlag Werner Hülsbusch, Glückstadt.



Der Inhalt dieser Veröffentlichung steht unter einer „Creative Commons Namensnennung 3.0 Unported“-Lizenz (<http://creativecommons.org/licenses/by/3.0/>).

BMBF Förderkennzeichen: 01|G09005A-G (Verbundprojekt)

Markenerklärung: Die in diesem Werk wiedergegebenen Gebrauchsnamen, Handelsnamen, Warenzeichen usw. können auch ohne besondere Kennzeichnung geschützte Marken sein und als solche den gesetzlichen Bestimmungen unterliegen.

Korrektorat und Satz: Werner Hülsbusch

Umschlag: Martina Kerzel

Druck und Bindung: SOWA Sp. z o.o., Warszawa

Printed in Poland

ISBN: 978-3-86488-032-2

# Vorwort

Der vorliegende Leitfaden ist entstanden aus der Zusammenarbeit verschiedener Forschungsdisziplinen innerhalb des WissGrid-Projekts. Die Ziele des Projekts bestanden darin, die Nutzung von kollaborativen Forschungs-umgebungen, wie sie im Rahmen der D-Grid-Initiative entwickelt wurden, und deren organisatorische und technische Nachhaltigkeit zu fördern. Ein Teil dieser Aufgabe war die Entwicklung von Werkzeugen für die Langzeitarchivierung von Forschungsdaten, die mit den technischen Mitteln der wissenschaftlichen Grid-Projekte und der Grid-Technologie bewältigt werden sollte. Im Laufe des Projekts wurde deutlich, dass die Klärung allgemeiner Fragen des Forschungsdaten-Managements noch wichtiger und gefragter war als technische Hilfsmittel.

Zwar gibt es im anglo-amerikanischen Bereich bereits eine Reihe von Planungsinstrumenten für das Forschungsdaten-Management, aber es gibt bisher keine vergleichbaren deutschsprachigen Hilfsmittel und aufgabenorientierten Einführungen.\* Zudem kamen im WissGrid-Projekt in einer einmaligen Konstellation Naturwissenschaften, Geistes- und Sozialwissenschaften sowie Rechenzentren und Bibliotheken mit ihren Überlegungen, Erfahrungen und Verfahren zum Umgang mit Forschungsdaten zusammen. Angesichts dieser Chance und aus dieser Motivation heraus wurden der Leitfaden und die Checkliste entwickelt. Wir hoffen, dass sie bei einem Einstieg in die Praxis, bei einer kritischen Überprüfung der eigenen bisherigen Praxis und auch der Entwicklung neuer Ansätze für das Forschungsdaten-Management behilflich sind.

Neben den Herausgebern haben als weitere Autoren (in alphabetischer Reihenfolge) Norman Fiedler, Thomas Fischer, Timo Gnadt, Erik Ketzan, Torsten Rathmann und Gabriel Stöckle mitgewirkt. Wir möchten ihnen sowie allen Wissenschaftlern, die uns Feedback gegeben haben, und den Förderern des WissGrid-Projekts ganz herzlich danken. Besonderer Dank geht an die D-Grid gGmbH, ohne deren Unterstützung dieses Buchprojekt nicht umsetzbar gewesen wäre.

---

\* Allerdings sei an dieser Stelle auf das thematische *Handbuch Forschungsdatenmanagement* von Büttner et al. (2011) sowie die disziplin-orientierte *Bestandsaufnahme Langzeitarchivierung von Forschungsdaten* von Neuroth et al. (2012) hingewiesen.

Das WissGrid-Projekt wurde von Mai 2010 bis April 2012 vom BMBF im Rahmen der D-Grid Initiative gefördert.

*Die Herausgeber*

# Inhaltsverzeichnis

<b>Vorwort</b>	<b>5</b>
<b>Leitfaden zum Forschungsdaten-Management</b>	<b>11</b>
Einleitung	13
Der Lebenszyklus von Forschungsdaten	14
Übergreifende Aufgaben	16
Benutzung der Checkliste	17
<b>Teil I:</b>	
<b>Aufgaben im Lebenszyklus von Forschungsdaten</b>	<b>19</b>
1 Planung und Erstellung	19
2 Auswahl und Aufbewahrungs dauer	24
3 Ingest: Einspeisen und Verantwortungsübernahme	28
4 Speicherung und Infrastruktur	33
5 Erhaltungsmaßnahmen und ihre Planung	36
6 Zugriff und Nutzung	39
<b>Teil II:</b>	
<b>Übergreifende Aufgaben des Forschungsdatenmanagements</b>	<b>47</b>
7 Organisation, Management und Policies	47
8 Kosten	51
9 Rechtliche Aspekte von Forschungsdaten	55
10 Metadaten	61
11 Identifikatoren und Informationsobjekte	67
<b>Anhang: Urheberrecht</b>	<b>75</b>
Einführung	75
Rechtliche Situation	76
Bestandsaufbau und Datensammlung	76
Bestandserhaltung und Kopien	77

Zugriffsrechte	80
Haftung	81
Fazit	82
<b>Checkliste zum Forschungsdaten-Management</b>	<b>83</b>
Vorwort: Anleitung zur Benutzung der Checkliste	85
<b>Teil I:</b>	
<b>Aufgaben im Lebenszyklus von Forschungsdaten</b>	<b>87</b>
1 Planung und Erstellung	87
2 Auswahl und Aufbewahrungsdauer	88
3 Ingest: Einspeisen und Verantwortungsübernahme	89
4 Speicherung und Infrastruktur	90
5 Erhaltungsmaßnahmen und ihre Planung	90
6 Zugriff und Nutzung	91
<b>Teil II:</b>	
<b>Übergreifende Aufgaben des Forschungsdaten-Managements</b>	<b>93</b>
7 Organisation, Management und Policies	93
8 Kosten	94
9 Rechtliche Aspekte von Forschungsdaten	95
10 Metadaten	96
11 Identifikatoren und Informationsobjekte	96
Kurzfassung	98
Formale Informationen zur Checkliste	100

<b>Bitstream Preservation: Bewertungskriterien für Speicherdienste</b>	<b>101</b>
1 Einleitung	103
2 Allgemeine Service-Level-Kriterien für Speicherdienste	106
3 Spezifische Bitstream-Preservation-/Integritätskriterien	107
4 Sicherheit und Vertraulichkeit	109
5 Checkliste	111
<b>Quellen</b>	<b>113</b>
Literaturverzeichnis	113
Websites	118



# Leitfaden zum Forschungsdaten-Management



# Einleitung

Digitale Forschungsdaten sind wichtige Produkte der wissenschaftlichen Arbeit, in deren Erstellung viel Geld, Zeit und Expertise investiert wird. Gleichzeitig sind durch die modernen wissenschaftlichen Arbeitsinstrumente das Volumen und die Komplexität der Forschungsdaten gestiegen und der sinnvolle Umgang mit Forschungsdaten ist deutlich anspruchsvoller geworden. Vor diesem Hintergrund haben Wissenschaftsorganisationen wiederholt Anforderungen an das Management von Forschungsdaten gestellt, wie z. B. die DFG, die seit 2010 in Anträgen eine Darstellung des Umgangs mit Forschungsdaten verlangt [DFG-Antrag 2012, S. 6]. Dieser Leitfaden und die begleitende Checkliste sollen als Instrumente für WissenschaftlerInnen und Service-Einrichtungen (wie z. B. Rechenzentren) dienen, um für ein Vorhaben gemeinsam und systematisch alle wesentlichen Themen des Forschungsdatenmanagements zu untersuchen und einen Plan für das Datenmanagement aufzustellen. Die Kapitel des Leitfadens und die Abschnitte der Checkliste entsprechen sich, sodass die Kapitel als Erklärung der Checklistenabschnitte benutzt werden können.<sup>1</sup>

Unter dem Management von Forschungsdaten werden alle Maßnahmen verstanden, die sicherstellen, dass digitale Forschungsdaten nutzbar sind. Was dafür notwendig ist, variiert aber stark mit den verschiedenen Zwecken, für die Forschungsdaten genutzt werden sollen. Es lassen sich vier Arten von Zwecken unterscheiden:

1. die Nutzung als Arbeitskopie für das wissenschaftliche Arbeiten,
2. die Nachnutzung von Forschungsdaten für spätere Forschung,
3. die Aufbewahrung als Dokumentation des korrekten wissenschaftlichen Arbeitens und
4. die Aufbewahrung, um rechtlichen oder anderen forschungsfremden Anforderungen nachzukommen.

Unabhängig von diesen Nutzungsarten unterliegen digitale Forschungsdaten besonderen Bedingungen, die in den letzten Jahren unter dem Thema der

---

1 Es existieren eine Reihe von englischen Checklisten, die vom DataOne-Projekt verglichen werden, siehe <https://www.dataone.org/plans>. Die hier vorgestellte Checkliste ist insbesondere von der DCC-Checkliste inspiriert, siehe [http://www.dcc.ac.uk/webfm\\_send/431](http://www.dcc.ac.uk/webfm_send/431).

Langzeitarchivierung digitaler Daten behandelt wurden. Langzeitarchivierung umfasst die sogenannte Bitstream Preservation, technische Nachnutzbarkeit und inhaltliche Nachnutzbarkeit. Eine Grundvoraussetzung ist die Bitstream Preservation, d. h. die Erhaltung der Bitfolge, was angesichts der Kurzlebigkeit und Fehleranfälligkeit von digitalen Datenträgern bei großvolumigen Forschungsdaten bereits eine Herausforderung sein kann. Der Erhalt der Bitfolge gewährleistet aber noch nicht, dass Forschungsdaten immer technisch nachnutzbar sind. Die Nutzung von Forschungsdaten kann z. B. durch spezialisierte Dateiformate besondere technische Anforderungen an Software, Hardware oder Infrastruktur stellen, die langfristig schwer erfüllbar sein können. Und selbst wenn die technische Nutzbarkeit gewährleistet ist, erfordert die inhaltliche Nutzung immer Hintergrund- und Kontextwissen, das bei der Erstellung der Forschungsdaten nachvollziehbar dokumentiert werden muss. Zu einem späteren Zeitpunkt können weitere Ergänzungen notwendig werden, wenn sich z. B. in einem wissenschaftlichen Gebiet bisher selbstverständliche Annahmen, Methoden oder Begriffe ändern, die späteren NutzerInnen explizit erklärt werden müssen. Und schließlich gibt es allgemeine Herausforderungen wie die Fragen der Organisation und Finanzierung: Wer übernimmt die Verantwortung für den Erhalt der Nutzbarkeit, wie aufwendig ist das und wer wird das bezahlen? Für traditionelle Publikationen oder Dokumente öffentlicher Institutionen existiert ein System von Bibliotheken und Archiven, für die es im Bereich der Forschungsdaten nur selten eine Entsprechung gibt.

Der vorliegende Leitfaden behandelt die Aufgabenbereiche, die für das Management von Forschungsdaten bedacht werden müssen, in zwei Teilen. Einige Aufgaben können klar in einem als Lebenszyklus vorgestellten Ablauf von Schritten verortet werden (siehe Abb. 1). Andere Aufgaben hingegen spielen in jedem Abschnitt des Lebenszyklus eine Rolle (siehe Abb. 2).

## Der Lebenszyklus von Forschungsdaten

Es gibt eine Vielzahl von Lebenszyklus-Modellen für digitale Informationen, von denen das Modell des Digital Curation Centers besonders elaboriert und auf Forschungsdaten ausgerichtet ist.<sup>2</sup> Im Folgenden wird ein vereinfachtes Modell benutzt.

---

<sup>2</sup> DCC, The DCC Curation Lifecycle Model, <http://www.dcc.ac.uk/resources/curation-lifecycle-model>



Abb. 1 Aufgaben im Lebenszyklus von Forschungsdaten

- **Planung und Erstellung** Um das spätere Management von Forschungsdaten möglichst zu vereinfachen, ist es sinnvoll, die Daten schon entsprechend zu erzeugen. Ein wichtiger Aspekt in dieser Phase ist z. B. die Wahl der richtigen Standards.
- **Auswahl und Bewertung** Nicht alle Forschungsdaten müssen und können auf Dauer aufbewahrt werden. Die Gründe, Methoden und Kriterien der Selektion und die daraus resultierende Dauer der Aufbewahrung von Forschungsdaten müssen geklärt werden.
- **Ingest/Übernahme** Forschungsdaten, die längerfristig aufbewahrt werden sollen, müssen in eine geeignete Umgebung wie z. B. ein Datenarchiv überführt werden. In dieser Phase werden üblicherweise zusätzliche Checks, Homogenisierungen und Anreicherungen der Daten notwendig, die besonders aufwendig sind.
- **Speicherung** Die langfristige Speicherung von Forschungsdaten mit Verfahren, die die Chancen von Datenverlust minimieren, sollte am besten von erfahrenen Anbietern von Speicherdiestleistungen übernommen werden.
- **Erhaltungsmaßnahmen** Es ist nicht selbstverständlich, dass digitale Forschungsdaten in anderen Umgebungen als der ursprünglichen Erstellungs- und Nutzungsumgebung nutzbar bleiben. Deshalb ist es bereits im Vorfeld sinnvoll zu bedenken und zu dokumentieren, welche Anforderungen an eine technische Umgebung zur Nutzung der Daten gestellt

werden und wie mit Veränderungen der Technik umgegangen werden soll.

- **Zugriff und Nutzung** Die besten Daten nutzen wenig, wenn sie nicht gefunden werden. Wie die Daten gefunden werden können, wer autorisiert auf sie zugreifen darf und mit welchen Mitteln, sind daher ebenfalls wichtige Fragen.

## Übergreifende Aufgaben

Neben den eindeutig im Lebenszyklus verortbaren Aufgaben gibt es einige Themen, die in jedem Abschnitt des Lebenszyklus wichtig sind. Es handelt sich dabei um Querschnittsthemen, die separat behandelt werden.

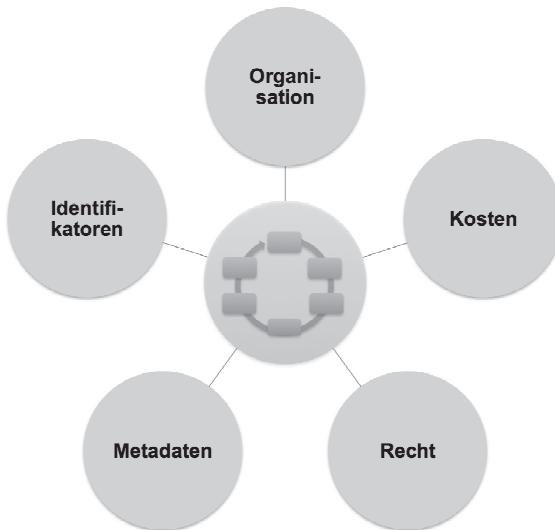


Abb. 2 Übergreifende Aufgaben des Forschungsdatenmanagements

- **Management, Organisation und Policies** Technik allein bewahrt keine Forschungsdaten auf. Es muss immer eine Organisation dafür die Verantwortung übernehmen und mit definierten Prozessen, die dokumentiert sind, sicherstellen, dass auch langfristig alle notwendigen Maßnahmen erfolgen. Ob es sich bei dieser Organisation dann um ein fachspezifisches Datenarchiv oder Konsortium oder um eine fachübergreifende Ein-

richtung wie ein universitäres Rechenzentrum handelt, ist nur von nachrangiger Bedeutung.

- **Recht und Ethik** Forschung muss sich an geltendes Recht und ethische Forderungen halten. Für das Management von Forschungsdaten sind u. a. der Schutz personenbezogener Daten, Urheberrechte, Lizenzierung von Forschungsdaten und Vertraulichkeit zu bedenken.
- **Finanzierung und Förderung** Ein limitierender Faktor für die Aufbewahrung von Forschungsdaten sind die damit verbundenen Kosten. Insbesondere die Kostenentwicklung und Gesamtkosten einer dauerhaften, zeitlich unbefristeten Archivierung sind offene Forschungsfragen.
- **Metadaten** Metadaten sind strukturierte Informationen über die vorliegenden Daten und für das Management von Forschungsdaten in jeder Phase des Lebenszyklus unverzichtbar.
- **Identifikatoren** Identifikatoren stellen einen nicht vernachlässigbaren Aspekt des Forschungsdatenmanagements dar. Ein präzises und durchdachtes Konzept zur Identifizierung von Forschungsdaten erfordert auch ein präzises Konzept der Informationsobjekte und klärt dadurch eine Reihe von wichtigen Fragen.

## Benutzung der Checkliste

Die in diesem Leitfaden und der begleitenden Checkliste dargestellten zentralen Aufgaben des Forschungsdaten-Managements können weder von den Wissenschaftlern noch von den Service-Einrichtungen allein gelöst werden, sondern erfordern ihre Zusammenarbeit. Entsprechend muss auch die Planung des Datenmanagements gemeinsam erfolgen, z. B. in einer Reihe von Gesprächen oder Workshops. Soll die Checkliste als Gerüst eines Datenmanagementplans dienen, dann sind zudem einige formale Rahmenaspekte zu beachten. Dazu gehört es festzuhalten, wann und von wem der Plan erstellt und abgenommen wurde.

Es ist auch sinnvoll, im Vorfeld zu klären, für welchen Bereich im Modell des „Curation Continuum“ (siehe Abb. 3) das Datenmanagement geplant wird. Im privaten Arbeitsbereich eines Forschers (private Domäne) werden Daten individuell gesammelt und erstellt und es muss kein Bedarf für explizite Regelung vorhanden sein; jedoch schon für den Übergang in die Arbeitsgruppe (Gruppendomäne) sind (wenigstens informelle) Regelungen erforderlich, z. B. in Bezug auf standardisierte Metadaten. Für eine längerfristige

Nutzung (dauerhafte Domäne) und eine Veröffentlichung (Zugang und Nachnutzung) müssen höhere Maßstäbe angelegt werden, um die Nutzbarkeit in diesem Kontext sicherzustellen. Solche Wechsel von einer Domäne in die nächste sind oftmals kritische Phasen, die nicht nur mit veränderten Anforderungen, sondern auch mit veränderten Verantwortlichkeiten einhergehen.

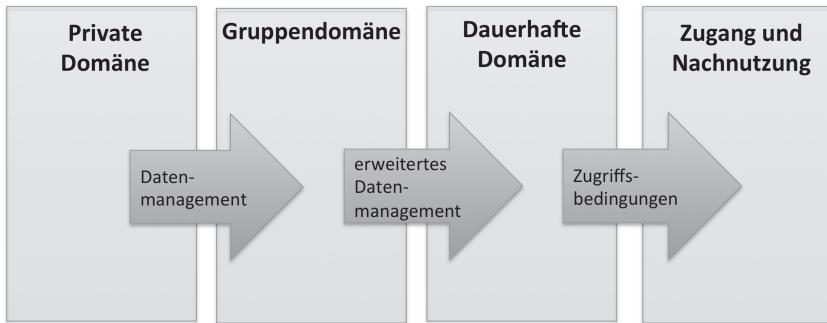


Abb. 3 Das Curation Continuum in Anlehnung an Treloar & Harboe-Ree (2008) und Arbeiten des DFG-Projekts „Radieschen“

In allen Fragen des Datenmanagements ist zu bedenken, dass je nach Disziplin und Szenario der Klärungsbedarf und die Antworten auf die Fragen sehr unterschiedlich ausfallen können. Auch wenn die Autoren glauben, alle wesentlichen Punkte für einen Datenmanagementplan bedacht zu haben, so kann es weitere wichtige Aspekte geben, die hier nicht erwähnt werden. Und umgekehrt wird es oftmals Aufgaben geben, die den Beteiligten für ihren Kontext selbstverständlich erscheinen, die aber in anderen Kontexten expliziter Klärung bedürfen. Für beide Fälle ist es sinnvoll, dass Service-Einrichtungen die vorliegende Checkliste als generisches Instrument verstehen, die sie für bestimmte Zielgruppen erweitern oder einschränken sollten, wenn sie einen Bedarf nach größerer oder geringerer Granularität sehen. Die hier beschriebenen Aufgaben und Fragen sollten deshalb als Hilfsmittel, aber keineswegs als in allen Punkten zwingend oder erschöpfend angesehen werden.

# **Teil I: Aufgaben im Lebenszyklus von Forschungsdaten**

## **1 Planung und Erstellung**

Am Beginn des Lebenszyklus von Daten steht die Projektplanung und die Erstellung bzw. Erfassung sowie erstmalige Speicherung der Daten. Dieses Kapitel fasst die wichtigsten Punkte hierzu zusammen.

### **Planung**

Die Ziele des Projektes bestimmen, welche Daten erfasst und bearbeitet werden. Für deren unmittelbare Bearbeitung und Auswertung sind herkömmliche Arten der Aufbewahrung und des Austauschs oft schon unzureichend. Darauf hinaus besitzen gesammelte Forschungsdaten einen eigenen Wert; ihre Nachnutzung wird zunehmend thematisiert und findet sich in Vorgaben und Erwartungen der Fördergeber.

Die Planung der Daten-Nachnutzung sollte bei Forschungsvorhaben von Beginn an bedacht werden, da dies die Wahrscheinlichkeit erhöht, dass in der weiteren Forschung sinnvolle Datenpflege-Richtlinien beachtet werden. Weiterhin gilt es schon zu Beginn eines Projektes zu beurteilen, wie man geplante und erwartete Datenmanagement-Aufgaben erfüllen kann und ob hierfür genug Personal und Finanzmittel vorgesehen wurden.

Die Frage der Rechte an geistigem Eigentum ist von Anfang an zu klären und entsprechend zu dokumentieren; in diesem Zusammenhang ist es unumgänglich, die für eine Veröffentlichung der Daten nötigen Anforderungen und Beschränkungen zu definieren. Abschließend müssen spezifische Rollen und Verantwortlichkeiten so früh wie möglich geklärt und dokumentiert werden.

### **Vorhandene Daten**

Es ist wichtig zu prüfen, in welcher Beziehung neue Datensätze zu bereits vorhandenen stehen. Besonders die Wichtigkeit eines Datensatzes klar darzu-

stellen, kann für spätere Nutzer und Archivare nützlich bei der Bewertung der Daten sein. In diesem Kontext sollte man Möglichkeiten zur Nachnutzung bestehender Datensätze recherchieren und die technischen und inhaltlichen Bedingungen klären, unter denen neu geschaffene Daten in bereits vorhandene Datenbestände integriert und mit diesen kombiniert werden können. Auch ist zu bedenken, ob ihre weitere Verwendung rechtlich unbedenklich ist (siehe Kap. 9 *Rechtliche Aspekte von Forschungsdaten*, S. 55 ff.).

Ist Vernetzung und Nachnutzung ein Hauptanliegen des Projektes, so sollte man sich auch Gedanken zur Bereitstellung von Daten machen (siehe Kap. 6 *Zugriff und Nutzung*, S. 39 ff.). Wie werden die Daten zur Verfügung stehen, zum Beispiel in öffentlichen Datenbanken? Gibt es Einschränkungen hinsichtlich ihrer Verwendung? Wann werden sie öffentlich zugänglich gemacht?

## Arten von Daten

Die hier aufgeführte Aufzählung unterscheidet Daten nach ihrer inhaltlichen Art sowie nach der Art ihrer Erstellung und Erfassung. Eine solche Klassifizierung dient vor allem der Bewertung des Datensatzes und der Entscheidungsfindung bezüglich dessen Nachnutzung und Archivierung. Sind die Daten beispielsweise reproduzierbar oder handelt es sich um einmalige Messungen? Hier ist es noch unerheblich, um welche technischen Datentypen es sich handelt.

- **Experimente:** Hierbei handelt es sich um Daten, die im Prinzip erneut hergestellt werden können (obwohl dies in der Praxis schwierig oder nicht wirtschaftlich sein kann).
- **Modelle oder Simulationen:** Bei einer Simulation kann es wichtiger sein, das Modell und die dazugehörigen Anfangsbedingungen der Simulation zu erhalten, als die damit berechneten (Roh-) Daten.
- **Beobachtungen:** Diese Daten repräsentieren spezifische Phänomene zu einem bestimmten Zeitpunkt oder Ort. Sie enthalten in der Regel eine einzigartige und nicht wiederholbare Aufzeichnung eines Ereignisses.
- **abgeleitete Daten:** Durch die Verarbeitung „roher“ und/oder Verbindung verschiedener Daten werden durch spezielle Methoden neue produziert (die Rechte der Eigentümer der Rohdaten sind zu respektieren!). Hier ist eventuell die Provenienz der Daten und die Dokumentation der Verfahren ebenfalls relevant.

- **kanonische oder Referenzdaten:** Diese Daten beschreiben andere Daten entsprechend gemeinsamer Regeln (lat. *canon* – „Norm, Regel“) oder stellen eine „Übersetzung“ dieser Daten in ein Standardformat dar. Der Übergang zu Metadaten ist fließend.

## Werkzeuge zur Erstellung von Daten, Software

Die Erstellung oder Schaffung unterscheidet sich von der reinen Erfassung von Daten. Um beispielsweise Daten zu reproduzieren, die bei Analysen und Simulationen entstehen, ist es nicht zwangsläufig notwendig, die erzeugten Daten selbst aufzubewahren. Allerdings ist es unumgänglich, die Software und Werkzeuge, mit denen diese Daten geschaffen wurden, zu erhalten und deren Nachnutzung zu thematisieren.

### Erfassung und Speicherung

Zum Zeitpunkt der Datenerfassung gilt es, ausreichend Informationen über die Daten selbst zu erfassen, um eine weitere Nutzung zu ermöglichen (siehe Kap. 10 *Metadaten*, S. 61 ff.). Es ist notwendig, die Kriterien klar zu definieren, unter denen ein Datensatz angelegt wird, und welche zugehörigen Metadaten gesammelt werden sollen.

Für die Speicherung ist es sinnvoll, die erwarteten Datenmengen und Produktionsraten abzuschätzen. Schon bei der Planung der Datenerfassung stellt sich die Frage der Speicherung der Daten auf geeigneten Medien (siehe Kap. 4 *Speicherung und Infrastruktur*, S. 33 ff.). Ein weiterer Punkt ist die wohldefinierte Identifizierung von Dateien und Inhalten, wobei hier neben einer klaren Zuordnung auch die Sicherung der Qualität der Dateien durch eine automatische oder gedankliche Überprüfung der Inhalte gemeint ist. Auch gilt es, einen sicheren Platz für die erfassten Daten (d. h. ein vertrauenswürdiges Archiv) zu finden und sicherzustellen, dass das Archiv diese Daten aufnehmen kann und wird (siehe Kap. 3 *Ingest: Einspeisen und Verantwortungsübernahme*, S. 28 ff.).

## Kriterien für Dateiformate und Standards zur gemeinsamen Nutzung von Daten

Es muss weiter geklärt werden, in welchen Formaten und gemäß welcher Standards Daten erfasst und gespeichert werden sollen.

Die Auswahl eines geeigneten Formats zur Archivierung der Daten ist eine grundlegende Entscheidung, deren Tragweite man sich bewusst sein sollte. Der Austausch und die Wiederverwendung von Daten erfordert deren Interoperabilität; hierzu müssen Standards für die Datenerfassung, Zitierung, Annotation, Klassifizierung, Integration von neuer Software, Darstellung von Inhalten usw. eingehalten werden. Diese Standards müssen identifiziert – oder, falls nicht vorhanden, entwickelt – werden und sollten dann in einem definierten Format darstellbar sein.

Der Übergang von Dateien zu Daten ist im Rahmen dieser Kriterien fließend. Eine Behandlung von Daten durch Client-basierte Daten-Dienste geht über das Konzept einer Datei hinaus. Dienste, die beispielsweise Daten über ein Webportal anbieten, sollten die Möglichkeit der Verifizierung der Quelle etc. anbieten. Die in diesem Zusammenhang zu beachtenden Kriterien sollten ebenfalls in die Planung des Datenmanagements aufgenommen werden.

Die nachstehend aufgeführten Kriterien für Datenmanagement-Standards wurden sowohl unter Gesichtspunkten der Daten-Langzeitarchivierung (\*) als auch im Hinblick auf gemeinsame Datennutzung in kooperativen Forschungsumgebungen (\*\*) gesammelt. Das Domänenmodell aus Abb. 3 auf S. 18 sollte hier Anwendung finden, d. h. die Kriterien sind in den unterschiedlichen Domänen unterschiedlich relevant.

- **Einfachheit<sup>\*,\*\*</sup>:** Technische Komplexität erschwert fehlerfreie Entschlüsselung und Nutzung. Je mehr Wissen zur Nutzung notwendig ist, desto eher kann ein Teil des notwendigen Wissens verloren gehen.
- **Flexibilität<sup>\*\*</sup>:** Große Datenmenge und mehrere Objekte sind in einer Datei speicherbar. Es besteht die Möglichkeit zum Zugriff auf Untereinheiten und zur parallelen Verarbeitung.
- **Nutzbarkeit<sup>\*\*</sup>:** Die Selektion der Daten sollte nach der Verbreitung innerhalb der Community, der Verfügbarkeit von Client-Software, der vorhandenen Anbindung der Daten an Aufbereitungs-Software und deren Anwendbarkeit und Stabilität für verschiedenste Szenarien erfolgen.
- **Standardisierung<sup>\*,\*\*</sup>:** Eine formale Beschreibung/Spezifikation existiert und ist frei verfügbar. Eine Spezifikation ermöglicht es, das Format zu verstehen und eigene Nutzungssoftware zu schreiben.

- **Referenzierbarkeit/Interoperabilität<sup>\*\*\*</sup>**: Die Daten sind klassifizierbar, kommentierbar, mit anderen Daten verknüpfbar und global referenzierbar.
- **Datenintegrität<sup>\*</sup>**: Für die Beurteilung der Integrität der Daten sind die Verifizierbarkeit der Quelle und die Überprüfbarkeit des Inhalts der Datensätze die wichtigsten Kriterien. Eine Möglichkeit zur automatischen Fehlererkennung ist anzustreben.
- **Provenienz<sup>\*\*\*</sup>**: Die Bearbeitungshistorie der Daten ist nachvollziehbar und wird aufgezeichnet.
- **Robustheit<sup>\*\*</sup>**: Das ausgewählte Speicherverfahren weist eine hohe Fehlertoleranz bei hardwareseitigen Fehlern auf.
- **Unabhängigkeit<sup>\*\*\*</sup>**: Die Verarbeitung der Daten ist nicht abhängig von spezieller Hard- oder Software. Die Daten können auch mit verschiedenen Versionen der Software gelesen werden.
- **Schutzmechanismen<sup>\*\*</sup>**: Kopierschutz und Verschlüsselungen sind für die Langzeitarchivierung von Dateien problematisch, da eine Modifikation technisch notwendig werden kann. Gemeinsame Datennutzung macht aber klare Regelungen und Einschränkungen durch Autorisierung und Authentifizierung notwendig.
- **Selbstdokumentation/Datenbanken**: Eine Integration von Metadaten in Daten erleichtert das Verständnis der Daten und verringert die Abhängigkeit von externen Datenquellen, andererseits erleichtert eine getrennte Lagerung von Daten und Metadaten den Zugriff, erhöht aber die Gefahr, dass die Verbindung zwischen Metadaten und Daten langfristig verloren geht. (*Hier kann keine allgemeingültige Richtlinie gegeben werden, es müssen die Vor- und Nachteile der gewählten Vorgehensweise von Fall zu Fall abgewogen werden.*)

## Anwendungsfall Klimaforschung

Die Klimaforschung produziert und nutzt unterschiedliche Daten [Overpeck et al. 2011], vor allem Beobachtungsdaten (z. B. Satellitendaten) und Modellrechnungen. Die gespeicherten Daten werden durch die Klimaforschung selbst, aber auch durch die Klimafolgenforschung genutzt. Ein nicht unerheblicher Teil besitzt gesamtgesellschaftliche Relevanz. So sind die Konsortialrechnungen des IPCC (Intergovernmental Panel on Climate Change [IPCC], eine Unterorganisation der UNO) Grundlage für Empfehlungen an die Politik.

In Projekten von besonderer Relevanz wird schon die Datenproduktion gemeinsam von Produzenten, Archiven und Nutzern geplant. Ein solches Projekt ist CMIP5 (Coupled Model Intercomparison Project, Phase 5 [Meehl et al. 2009]). CMIP ist ein Protokoll zur Analyse von Rechenergebnissen allgemeiner Zirkulationsmodelle (GCM, General Circulation Model) mit gekoppeltem Atmosphären- und Ozeanmodell. CMIP5 liefert eine Infrastruktur für die Diagnose und Validierung, den Vergleich und die Dokumentation solcher Klimamodelle. Es wird erwartet, dass die dabei produzierten Rechenergebnisse in den nächsten Weltklimabericht des IPCC einfließen werden, wie das auch mit den Ergebnissen früherer CMIP-Phasen geschehen ist.

Vor Beginn der Ausführung der Modellrechnungen wurden diese im Detail geplant [Taylor / Stouffer / Meehl 2012], einschließlich deren einheitlicher Benennung für die spätere Speicherung der Ergebnisse. Dateiformat und Metadatenkatalog sind ebenfalls festgelegt [CMIP5 Datenbeschreibung o.J.], und zwar auf NetCDF [NetCDF 2012] und CF [NetCDF CF Metadata Convention 2011]. Eine dreistufige Qualitätskontrolle [CMIP5 Quality Control o.J.] wird Bestandteil des Ingest sein. Für alle Core-CMIP5-Daten – das sind diejenigen, die in [Taylor / Stouffer / Meehl 2012] angefordert worden sind – ist die Veröffentlichung mit DOI-Vergabe und erneuter Qualitätskontrolle vorgesehen (näheres siehe Kapitel 11, S. 67 ff.). Die Planung sieht die Beteiligung weit entfernter Datenzentren vor. So sollen die Core-CMIP5-Daten nicht nur am WDCC [WDCC] archiviert, sondern zweifach repliziert werden, indem sie auch an das PCMDI (Program for Climate Model Diagnosis and Intercomparison, USA) [PCMDI] und das BADC (British Atmospheric Data Centre) [BADC] geschickt werden. Die bei der Replikation ausgetauschten Datenmengen werden so groß sein, dass diese nicht über das Netz transportiert, sondern auf Festplatten verschickt werden sollen. Die Festplatten sollen wiederverwendet werden.

## 2 Auswahl und Aufbewahrungs dauer

### Gründe zur Aufbewahrung

Wissenschaftliche Daten werden aus ganz unterschiedlichen Gründen aufbewahrt:

- Arbeitskopie: Die Daten werden für die aktive Arbeit während des Projektes gesichert.
- Nachweis der guten wissenschaftlichen Praxis: Die Daten sind Grundlage einer Publikation.
- Nachnutzung: Die Daten sind wichtig für spätere Forschung.
- Auflagen und Selbstverpflichtung
- Dokumentation: Die Daten sind gesellschaftlich relevant, z. B. Grundlage einer politischen Entscheidung.

Bei der *Arbeitskopie* handelt es sich oft um ein Zwischenergebnis oder um Vorläuferversionen der Endfassung. Eine Langzeitarchivierung ist in der Regel nicht erforderlich. Der Vertrag über die Archivierung sollte das Recht einschließen, auch den Lesezugriff auf die eigene Arbeitsgruppe beschränken zu können.

Sind die Daten *Grundlage einer Publikation*, sollten die „Regeln zur Sicherung guter wissenschaftlicher Praxis“ [Max-Planck-Gesellschaft 2001] Anwendung finden. In dem Dokument der Max-Planck-Gesellschaft wird für Primärdaten eine Aufbewahrungsduer von – wenn möglich – mindestens zehn Jahren gefordert. Darüber hinaus müssen alle wichtigen Schritte einer Forschungsarbeit durch Protokollierung nachvollziehbar gemacht und die Protokolle ebenfalls mindestens zehn Jahre aufbewahrt werden. Die Deutsche Forschungsgemeinschaft hat sich entsprechende Regeln gegeben [Deutsche Forschungsgemeinschaft 1998]. Gute wissenschaftliche Praxis erhöht die Nachvollziehbarkeit wissenschaftlicher Arbeiten und erleichtert die Aufklärung von Fehlern und Fälschungen. Auch immer mehr Verlage machen eine Veröffentlichung in ihren Medien vom öffentlichen Zugang zu den zugehörigen Forschungsdaten abhängig.

Die Ermöglichung der *Nachnutzung* ist oft ein weiterer Grund für eine Archivierung. Ein Großteil der Forschungsdaten kann nur mit erheblichem Aufwand erstellt werden und viele Daten können überhaupt nicht oder nicht effizient reproduziert werden. Forschungsdaten sollten als Ressource begriffen und nicht dauerhaft zurückgehalten werden, denn häufig eignen sich einmal produzierte Daten für mehrere Forschungszwecke – oft auch solche, an die bei Erzeugung der Daten noch gar nicht gedacht war. Die mühevolle Arbeit der Datenerstellung sollte belohnt werden, indem das Archiv den Nachnutzer vertraglich verpflichtet, in Veröffentlichungen die Herkunft der Daten in Form eines Zitats kenntlich zu machen. Außerdem sollte Datenerzeugern eine angemessene Sperrfrist für die Erstauswertung eingeräumt werden.

Einer gesetzlichen *Auflage* zur Archivierung muss selbstverständlich nachgekommen werden. So schreibt §1 der Gentechnikaufzeichnungsverordnung (GenTAufzV) vor, dass bei gentechnischen Arbeiten oder Freisetzungen Aufzeichnungen zu führen und aufzubewahren sind. Die Röntgenverordnung (RöV) legt in § 28 und die Strahlenschutzverordnung (StrlSchV) in § 85 fest, welche Aufzeichnungen bei der Strahlenanwendung am Menschen angefertigt und aufbewahrt werden müssen. Auch die Landesberufsordnungen für Ärzte enthalten bestimmte Dokumentationspflichten. Eine vertragliche Verpflichtung zur Archivierung kann sich ebenso aus den Anforderungen des Projektträgers oder der Mitgliedschaft in einer Forschungsgemeinschaft ergeben, beispielsweise durch Regeln zur Qualitätssicherung. Im kommerziellen Umfeld können auch Geschäftsregeln, Produkthaftung oder Basel II Anlass zur Archivierung sein.

## Datenauswahl

Die Selektion, welche Daten aufgehoben werden und welche nicht, muss in transparenter und nachvollziehbarer Weise erfolgen [Whyte/Wilson 2010]. Dabei sollte vermieden werden, dass allein die Sichtweise einer Person oder Gruppe zum Tragen kommt. Am besten gibt sich das Projekt selbst ein Regelwerk für die Datenauswahl, in dessen Erstellung neben Datenzentren auch Datenerzeuger und Nachnutzer einbezogen werden sollten. Die Selektionsregeln sollten auch vorgeben, wer welchen Teil der Datenbewertung vornimmt.

Bei der Selektion wird darüber entschieden, ob die zur Aufnahme vorgeschlagenen Daten archivwürdig und archivfähig sind. *Archivwürdig* sind sie, wenn eines der obigen Relevanzkriterien erfüllt ist. Die Archivwürdigkeit kann zusätzlich an bestimmte formale Qualitätskriterien gebunden sein – z. B. daran, dass Folgendes mit den Daten mitgeliefert wird:

- Zitierungen
  - Zitierung der wissenschaftlichen Methode, Normen, Hilfsmittel
  - Zitierung rechtlicher Grundlagen
  - Nachweis von zugehörigen Gegenständen, die in Museen oder Sammlstellen lagern, z. B. Funde, Saatgutproben
- Rohdaten wie z. B. Originalbildmaterial
- Provenienzdaten, in denen die genaue Vorgehensweise protokolliert ist
- Fachgutachten

*Archivfähig* sind Daten, wenn die technischen Voraussetzungen für die Archivierung erfüllt sind. Digitale Forschungsdatenarchive geben häufig Datenformat und Metadaten-Ausstattung vor. Eine Beschränkung der im Archiv erlaubten Datenformate verringert den Umfang der zur Pflege benötigten Kenntnisse und Software und damit Aufwand und Kosten. Zur Pflege-software gehören Standardwerkzeuge zur Formatvalidierung und -konvertierung, deren Zahl direkt von der Zahl der erlaubten Formate abhängt.

Nicht nur neue Daten können einer Selektion unterzogen werden. Es sollte auch in regelmäßigen Abständen überprüft werden, ob Daten, die sich schon lange im Archiv befinden, noch weiter dort aufbewahrt werden sollen; für eine solche Wiedervorlage kann und sollte das Projekt bzw. die Forschungsgemeinschaft verbindliche Regeln aufstellen. Dabei sollte berücksichtigt werden, dass sich die Gründe für die Nachnutzung verändern können und ein anderer als der ursprüngliche Zweck sogar in den Vordergrund des Interesses rücken kann.

## Aufbewahrung

Offene Dateninfrastrukturen haben zur Folge, dass sich Datenerzeuger, Manager und Nutzer nicht mehr unbedingt gegenseitig kennen. Vor diesem Hintergrund erscheint es nicht länger angemessen, die Entscheidung über die weitere Aufbewahrung von Daten allein auf fachinterne Kriterien zu stützen. Natürlich sollten fachbezogene Kriterien weiterhin ein starkes Gewicht haben, für die Entscheidung sollten aber weitere hinzugezogen werden. Ein einfach zu ermittelndes Maß für das Nutzerinteresse ist die Zahl der Abrufe, jedoch sollte dies wegen der hiermit verbundenen Manipulationsmöglichkeiten auch nicht das einzige Kriterium sein. Ein geeigneteres Maß kann die Zahl der Zitierungen sein – wenn das Archiv diese erfasst und sammelt. Außerdem können regelmäßige Analysen der Nutzerzusammensetzung helfen, Trends in den Nutzerinteressen frühzeitig zu erkennen. Wenn gesetzlich oder vertraglich ein Löschdatum festgeschrieben ist, hat das Archiv selbstverständlich keine Wahl und muss dem folgen.

## Weiterführende Literatur

- Für die Auswahl digitaler Objekte allgemein sowie Auswahlkriterien für Netzpublikationen: *nestor Handbuch*, Version 2.3 [Neuroth et al. 2010]:

Kapitel 3.5, Auswahlkriterien (<http://nbn-resolving.de/urn:nbn:de:0008-2010071949>).

## Anwendungsfall Klimaforschung

Die in den Archiven vorgehaltenen Messdaten repräsentieren den Zustand der Umwelt zum jeweiligen Zeitpunkt und können nicht durch Wiederholung der Messung erneut erhoben werden. Ältere Klimamodellrechnungen können nur mit sehr hohem Aufwand wiederholt werden, weil die damalige Hardware nicht mehr existiert und die Programme erst auf die jetzige Hardware portiert werden müssten.

Das World Data Center for Climate (WDCC) [WDCC] ist beschränkt auf verarbeitete Klimadaten. Es handelt sich dabei vorwiegend um Ergebnisse von Modellrechnungen und um solche Beobachtungsdaten, die der Modellvalidierung dienen, z. B. Niederschlagsdaten.

Die Daten dürfen nur in ganz bestimmten Dateiformaten vorliegen, nämlich als ASCII-Textdatei, GRIB [GRIB o.J.] oder NetCDF [NetCDF 2012]. Die beiden letzten sind Binärformate, die Header besitzen und in der Klimaforschung üblich sind. Die Daten sollen außerdem den CF-Standard [NetCDF CF Metadata Convention 2011] erfüllen, der z. B. Koordinatensysteme sowie Namen physikalischer und chemischer Größen vorgibt.

Die Daten werden mindestens zehn Jahre aufbewahrt, eine Höchstdauer ist nicht vorgesehen. Ältere Rechenergebnisse sind durchaus gefragt, da diese wichtige Vergleichsdaten für die Entwicklung neuer Klimamodelle sind.

## 3 Ingest: Einspeisen und Verantwortungsübernahme

Der Begriff *Ingest* bezeichnet den Prozess des Hinzufügens von Daten zu einem Archiv. Zum Ingest gehören alle Vorgänge, die zwischen der Zustimmung für die Aufnahme und dem Ende des Einfüllens ins Archiv liegen. Der Ingest kann gesammelt kurz vor Projektende oder verteilt über die gesamte Projektlaufzeit stattfinden.

## Verfahren

In Anlehnung an Digital Curation 101 [Digital Curation 101 o.J.] gehören zum Ingest die folgenden Arbeitsschritte:

- **Transport** der Daten für den Ingest
- **Vorbereitung** der Daten
  - Vergabe eines internen, archivweit eindeutigen *Identifikators*
  - Test auf *Schadsoftware* in den Daten
  - Übernahme, Extraktion oder Erzeugung der zugehörigen *Metadaten*
  - ggf. *Formatkonvertierung*
  - *Validierung* technischer Details (Daten- und Metadatenformat)
  - Prüfung der Daten und Metadaten auf *Vollständigkeit und Richtigkeit*
  - Aufteilung/Zusammenfassung der Daten in *Containerdateien*
- **Einfüllen** ins Archiv, dabei
  - Erzeugung von *Prüfsummen* zur späteren Prüfung auf ungewollte Veränderungen

Die Arbeitsschritte können je nach Art der Daten sowie Zweck und Aufbau des Archivs unterschiedlich sein. Für *sensible Daten* können z. B. zusätzliche Schritte wie eine Beschränkung des Zugangs und eine Verschlüsselung erforderlich sein. Auch die Reihenfolge der Arbeitsschritte kann variieren. Einige der Arbeitsschritte sollen nun näher beschrieben und diskutiert werden.

Der *Datentransport* kann über das Netzwerk erfolgen oder es werden Datenträger versandt. Wenn die Datenmengen so groß sind, dass eine hohe Beanspruchung des Netzwerks über eine längere Zeit oder sogar ein Abbruch wegen Zeitüberschreitung zu erwarten ist, werden gern Festplatten verschickt. Externe Festplatten besitzen eine hohe Speicherkapazität und lassen sich leicht an bestehende Computersysteme anschließen.

Zur Vorbereitung der Daten gehört die *Zusammenstellung der erforderlichen Metadaten*. Eventuell kann ein Teil der Metadaten maschinell aus den Daten ausgelesen werden (Metadatenextraktion). Die übrigen Metadaten werden meist vom Produzenten geliefert. Das Datenzentrum ergänzt eventuell noch Provenienzinformationen bezüglich des Ingest, d. h. Zusatzinformationen, die den Ablauf des Ingest protokollieren.

Unter *Validierung* soll hier eine Prüfung digitaler Objekte auf die technische Funktionsfähigkeit verstanden werden. Dabei wird untersucht, ob die erforderlichen technischen Spezifikationen erfüllt sind. Häufig wird eine Formatvalidierung durchgeführt, d. h. es wird geprüft, ob Daten bzw. Meta-

daten in einem gültigen Format vorliegen. Bei zusammengesetzten Formaten wie z. B. PDF müssen für eine vollständige Formatvalidierung auch die eingebundenen Objekte auf Gültigkeit ihres Formats geprüft werden.

Eine *Prüfung der Daten auf sachliche Richtigkeit* können nur Fachleute leisten. Eine Möglichkeit ist, die Datenproduzenten diese Prüfung selbst vornehmen zu lassen. Die Produzenten bestätigen nach erfolgter Prüfung die Richtigkeit und Vollständigkeit der Daten gegenüber dem Datenzentrum. Selbstverständlich birgt eine solche Selbstüberprüfung die Gefahr, dass die Produzenten aufgrund der intensiven Beschäftigung mit den Daten eventuell vorhandene durchgängige Fehler bzw. Abweichungen von zuvor festgelegten Anforderungen nicht bemerken. Dieses Risiko kann u. U. durch gezielte Zuordnung von fachkundigen – möglicherweise externen – Gutachtern minimiert werden. Im Falle numerischer Daten ist eventuell eine Plausibilitätskontrolle möglich, welche allerdings auch schon sehr gute Kenntnisse der verwendeten Forschungsmethode und des vorliegenden Datenformats erfordert.

Wissenschaftliche Untersuchungen, Experimente und numerische Rechnungen können nur reproduziert oder rekonstruiert werden, wenn alle wichtigen Schritte nachvollziehbar sind. Beim Ingest sollte deshalb geprüft werden, ob entsprechende Informationen enthalten sind.

Die *Prüfung der Metadaten* auf Vollständigkeit und formale Korrektheit kann anhand eines Katalogs von Pflicht-Metadaten erfolgen, der zuvor in der Community beschlossen worden ist.

Besteht ein Werk oder Dokument aus mehreren zusammengehörigen Dateien, so ist es oft zweckmäßig, diese in eine *Containerdatei* zu packen und als eine Einheit zu archivieren. Containerdateien sollten einen schnellen Zugriff auf die darin befindlichen Objekte ermöglichen, ohne dass der Container erst ganz ausgepackt werden muss.

## **Verantwortungsübernahme**

Schon vor der Übernahme der Verantwortung müssen die wesentlichen rechtlichen Aspekte zwischen Produzent und Datenzentrum geklärt worden sein, um beiden Seiten Rechtssicherheit zu geben. Falls es keine gesetzlich vorgeschriebene Ablieferungspflicht gibt, die für sich genommen schon die Archivierungstätigkeit regelt, muss zumindest eine Übereinkunft (Lizenzver-

einbarung) für den urheberrechtlich wichtigen Bereich getroffen werden [Beinert et al. 2008].

Beim Ingest sollten Produzent und Archiv eine Übernahmevereinbarung abschließen, die die Details der Übernahme der Verantwortung beschreibt und die bisherigen Schritte der Datenvorbereitung dokumentiert. Bestandteile der Übernahmevereinbarung sollten in Anlehnung an nestor [ebd.] insbesondere sein:

- die Liste der zu archivierenden Werke
- die Liste der diese Werke ausmachenden Datenobjekte (z. B. Dateien)
- die zu ihrer Archivierung notwendigen bzw. gewünschten organisatorischen und technischen Rahmenbedingungen (z. B. Aufbewahrungsdauer, Sperrfrist, Zahl der Kopien)<sup>3</sup>
- die erforderlichen Metadaten
- Kostenschätzung
- die rechtlich handelnden Parteien
- Regelungen zu Urheberrecht und Haftung
- Zeitplan für die Durchführung der Informationsübernahme.

Alle wichtigen Arbeitsschritte des Ingest sollten protokolliert werden. Dieses Protokoll sollte ebenso dauerhaft erhalten bleiben wie die gespeicherten Inhalte. Das Protokoll sollte eine Liste der aufgenommenen Datenobjekte, den Namen des Produzenten, alle Transformations- und Validierungsschritte einschließlich der Prüfergebnisse und die Zeitstempel aller wichtigen Schritte enthalten [ebd.]. Datenproduzent und Archiv sollten außerdem vereinbaren, wer im Fehlerfall für welche Schritte zur Fehlerbehandlung verantwortlich ist.

## Weiterführende Literatur

- nestor materialien 10: *Wege ins Archiv. Ein Leitfaden für die Informationsübernahme in das digitale Langzeitarchiv.* Version I ([Beinert et al. 2008], <http://nbn-resolving.de/urn:nbn:de:0008-2008103009>).

---

3 Für eine umfassende Liste organisatorischer und technischer Rahmenbedingungen siehe [Bitstream Preservation].

## Anwendungsfall Klimaforschung

Nur im Ausnahmefall werden Daten durch das World Data Center for Climate (WDCC) [WDCC] vom Produzenten geholt. Im Regelfall stellt das WDCC Platz zur Zwischenspeicherung der Daten zur Verfügung. Der Produzent kopiert die zum Ingest vorgesehenen Daten in diesen zur Verfügung gestellten Bereich. Die Verantwortung für den ordnungsgemäßen Datentransfer liegt beim Produzenten. Das WDCC führt an dieser Stelle keine Prüfsummenkontrolle durch.

Der Produzent ist verpflichtet, Metadaten abzuliefern – und zwar auch dann, wenn dieselben Informationen bereits in den Headern der Datenfiles enthalten sind. Die Metadaten können mithilfe einer Webapplikation online eingetragen und direkt in eine temporäre Datenbank geschrieben werden. Wenn die neu eingetragenen Metadaten die Qualitätskriterien erfüllen, brauchen sie vom DKRZ nur noch in die Produktionsdatenbank übernommen werden. Die Metadaten dürfen aber auch in XML eingebettet als Textdatei abgegeben werden. Eine weitere Möglichkeit ist, XML online mithilfe von GeoNetwork [GeoNetwork o.J.] zu erzeugen. GeoNetwork ist eine Open-Source-Software des OSGeo-Projektes [OSGeo], die auch von der FAO, WHO, UNEP und vielen anderen Organisationen verwendet wird.

Im Rahmen der technischen Qualitätskontrolle wird überprüft, ob versehentlich leere Dateien und somit überhaupt keine Daten geliefert wurden. Wenn die Daten in den Formaten NetCDF [NetCDF 2012] oder GRIB [GRIBo.J.] angeliefert wurden, wird das Format validiert. Je nach Projekt werden weitere Tests durchgeführt, z. B. auf doppelt vorhandene Zeitstempel geprüft (für ein und dieselbe Zeit zwei Datensätze zu haben, deutet auf einen Fehler hin).

Auch die wissenschaftliche Qualitätskontrolle ist stark vom Projekt abhängig, in dessen Rahmen die Daten produziert wurden. In vielen Fällen ist eine Kontrolle der Daten auf Richtigkeit und Vollständigkeit nicht möglich oder seitens der Produzenten nicht gewünscht. Vom Projekt ist abhängig, ob der Wertebereich von Variablen kontrolliert wird, beispielsweise sollen Daten für die relative Feuchte zwischen null und eins liegen, dies ist in der Praxis aber nicht immer der Fall. Messdaten besitzen eine durch die begrenzte Messgenauigkeit bedingte Toleranz, außerdem kann es auf natürliche Weise zur Übersättigung kommen (Werte > 1). Ergebnisse von Modellrechnungen können aufgrund numerischer Ungenauigkeiten ebenfalls außerhalb des eigentlich zulässigen Intervalls liegen, deshalb muss das Modell jedoch nicht

insgesamt schlecht sein. Welche Abweichung toleriert werden kann, können nur Experten entscheiden.

Metadaten werden durch die Ingest-Software auf formale Korrektheit geprüft.

- Metadaten, die aus einer Auswahlliste kommen, müssen einen der erlaubten Werte besitzen. Die erlaubten Werte sind in einer Datenbank abgelegt und beruhen auf Standards.
- Für bestimmte Einträge gibt es Vorgaben bzgl. der Länge.
- Bestimmte Einträge (Datensatznamen) dürfen nicht mehrfach im Archiv vorkommen.
- Ebenfalls wird geprüft, ob das XML valide ist, in dem die Metadaten eingebettet sind.

Am WDCC werden die Daten vor der Einspeisung ins Archiv in Containerdateien gepackt. Die Technik dazu hat das Deutsche Klimarechenzentrum selbst entwickelt, um Lizenzgebühren zu sparen. Der Zugriff auf Daten ist ohne vollständiges Auspacken des Containers möglich.

## 4 Speicherung und Infrastruktur

Die Speicherung von Forschungsdaten ist eine der grundlegendsten Aufgaben im Datenmanagement. Wenngleich organisatorische Aufgaben und Arbeitsabläufe oftmals die größten Schwierigkeiten darstellen und Speicherkapazitäten in der Wahrnehmung vieler Nutzer immer günstiger, einfacher und zuverlässiger werden, so bleibt doch die Speicherung von Forschungsdaten eine Herausforderung.

Grundlegende Faktoren, welche die Speicherung beeinflussen, sind:

- die Größe der Datensätze,
- die Anzahl der Datensätze und
- wie häufig auf die Datensätze zugegriffen werden soll.

Die derzeitigen Entwicklungstendenzen in Bezug auf Datenmengen, Speicherkapazitäten und Netzwerkkapazitäten lassen dies auch nicht als vorübergehende Schwierigkeiten erscheinen. Zwar wachsen die Kapazitäten von typischen Speichermedien exponentiell (das sogenannte Kryders Law in Anlehnung an Moores Law), aber auch die produzierten Datenmengen wachsen durch verbesserte Hard- und Software (wie z. B. die Verbesserung der Bild-

sensoren) in einem ähnlichen oder sogar stärkeren Maße. Die Netzwerkkapazität zum Transport der Daten wächst hingegen nicht unbedingt im gleichen Umfang, sodass es zu einer tendenziellen Verlangsamung des Datenzugriffs kommen kann.

Die Speicherung muss nicht immer durch die Institution, die die Verantwortung für das Forschungsdaten-Management übernimmt, selbst durchgeführt werden, sondern sie kann unter Umständen ausgelagert oder durch einen Verbund von Datenzentren/Archiven geleistet werden. Details zu den Erwägungen, wer die Speicherung übernimmt, finden sich im Kapitel „Management, Organisation und Policies“. Unabhängig davon, wer die Speicherung letztendlich durchführt, werden die wesentlichen Anforderungen durch folgende Faktoren vorgegeben:

- Integrität,
- Vertraulichkeit,
- Verfügbarkeit und Nutzung.

Die Sicherung der Integrität von Forschungsdaten auf der Speicherebene wird Bitstream Preservation genannt. Der prinzipielle Ansatz ist, genügend Kopien der Daten vorzuhalten, die möglichst wenig fehleranfällig und möglichst unabhängig voneinander sind (also z. B. an unterschiedlichen Orten mit unterschiedlichen Technologien gespeichert werden). Wenn die Kopien angemessen häufig auf ihre Integrität überprüft und fehlerhafte Kopien ersetzt werden, kann die Gefahr eines Datenverlusts sehr niedrig gehalten werden, auch wenn immer eine theoretische Verlustmöglichkeit besteht. Die Schwierigkeit besteht darin, eine sinnvolle Balance zwischen Integritätsanforderungen und Aufwand zu finden.

Die Vertraulichkeit sowie die Verfügbarkeit und Nutzbarkeit sind zwar zuerst Fragen des Zugriffs und werden im nächsten Kapitel detaillierter behandelt, aber sie haben direkte Auswirkungen auf die Speicherung und notwendige Infrastruktur. Es ist wichtig, die Nutzungsszenarien realistisch zu planen – insbesondere, wie häufig auf welche Datenbestände zugegriffen wird und zu welchem Zweck. Daten, auf die sehr häufig und in nicht vorhersehbaren Mustern zugegriffen wird und die zudem mit nur geringer Verzögerung bereitstehen müssen, müssen wahrscheinlich eher auf Festplatten („online“) als z. B. auf wesentlich günstigeren Magnetbändern („nearline“, „offline“) gespeichert werden. Die Netzwerk-Infrastruktur und die Übertragungsprotokolle müssen die vom Nutzungsszenario benötigte Transfergeschwindigkeit unterstützen. Gerade bei großen Datenmengen können für die Verarbeitung und einen schnellen Zugriff Grid- und Cloud-Technologien sehr

sinnvoll sein, insbesondere in Szenarien mit einer verteilten Speicher-Infrastruktur. Für spezielle Berechnungen oder Visualisierungen mit diesen Datensätzen kann es außerdem am effektivsten sein, wenn spezialisierte Hardware auf der Seite des Datenzentrums vorhanden ist.

## Weiterführende Literatur

- Ludwig, Jens / Rathmann, Torsten / Enke, Harry & Schintke, Florian (2011): *Bitstream Preservation: Bewertungskriterien für Speicherdiene*ste. WissGrid Arbeitspaket 3: Langzeitarchivierung von Forschungsdaten ([Ludwig et al. 2011], <http://www.wissgrid.de/workgroups/ap3/2011-03-08--bitstream-preservation.pdf>). – hier abgedruckt auf S. 101 ff. –

## Anwendungsfall Klimaforschung

Um die wachsenden Datenmengen bewältigen zu können, wird am World Data Center for Climate (WDCC) [WDCC] ein High Performance Storage System (HPSS) betrieben, d. h. die Daten werden zunächst temporär auf Festplatten geschrieben und später automatisch auf Bandkassetten geschoben. Am WDCC hat jede Bandkassette zurzeit eine Kapazität von einem Terabyte. Abb. 4 zeigt das Innere eines Storage-Containers, der 10.000 Bandkassetten fasst.



Abb 4 Innenleben eines Storage-Containers; auf den Schienen laufen die Tape-Roboter, die die Bandkassetten zu den Lesegeräten bringen

Je drei solcher Storage-Container stehen in zwei getrennten Brandabschnitten. Von allen Daten des WDCC gibt es zwei Kopien: Eine Kopie liegt im ersten, die andere im zweiten Brandabschnitt. Zum Schutz vor Diebstahl ist der Zugang zu den Tape-Libraries auf einige wenige Mitarbeiter beschränkt. Den Schutz vor klimatischen Einflüssen gewährleistet eine Klimaanlage.

Zur Erkennung von Fehlern werden Checksummen geschrieben, bei Bändern auf Blockebene und auf höheren Ebenen. Dort findet gegebenenfalls auch eine Fehlerkorrektur statt, ein End-to-end Checksumming ist im Aufbau. Bei einem Umstieg auf neue Medien, welcher alle drei bis fünf Jahre stattfindet, werden die Daten, die in der Regel unverschlüsselt sind, umkodiert.

## 5 Erhaltungsmaßnahmen und ihre Planung

Um digitale Daten langfristig nutzbar zu halten, sind eine Reihe von Maßnahmen notwendig, die im weiteren Sinne auch alle anderen in diesem Leitfaden behandelten Themen umfassen. Im engeren Sinne sollen in diesem Kapitel die spezifischen Maßnahmen zur Sicherung der technischen und intellektuellen Nachnutzbarkeit behandelt werden.

Erhaltungsmaßnahmen werden notwendig, wenn sich die Anforderungen der Zielgruppe bzw. die Zielgruppe selbst oder die verfügbaren Technologien und Verfahren ändern. Beispiele dafür sind neue Daten- oder Dateiformate, neue Schnittstellen, die von der Zielgruppe für die Arbeit mit neuen Softwareprogrammen oder Arbeitsumgebungen benötigt werden, neue wissenschaftliche Standards oder Arbeitsweisen, die eine Umrechnung in neue Maßeinheiten oder zusätzliche Parameter als Hintergrundinformation erfordern, oder auch die Erweiterung der Zielgruppe auf Laien. Wenn in diesen Zusammenhängen von einem Veralten von z. B. Dateiformaten gesprochen wird, so bedeutet dies in den seltensten Fällen, dass keine funktionierende Nutzungsumgebung mehr verfügbar wäre, sondern dass relativ zu den aktuellen Anforderungen mit den „veralterten“ Mitteln kein effizientes Arbeiten mehr möglich ist. C64-Software und mit ihr erstellte Daten lassen sich üblicherweise gut mit Emulatoren nutzen, aber es entspricht nicht mehr den modernen Erwartungen an Nutzungsumgebungen.

Eine wichtige Aufgabe für die Erhaltung von Daten besteht darin, zunächst überhaupt festzustellen, dass es relevante Änderung in der Zielgruppe oder der Technologielandschaft gibt. Dafür ist die regelmäßige Untersuchung der eingesetzten und neuen Technologien (Technology Watch) und der Anforderungen und des Hintergrundwissens der Zielgruppe (Community Watch), z. B. durch ein Datenarchiv, notwendig. Bereits vor der Übernahme in ein Datenarchiv sollte eine Dokumentation der ursprünglichen Technologien und Anforderungen erfolgen.

Wie mit diesen Änderungen umzugehen ist, muss in einem gründlichen Planungsprozess entschieden werden. Im „Planets“-Projekt wurde zu diesem Zweck ein Verfahren auf Basis der Nutzwertanalyse entwickelt. In einer groben Übersicht sind folgende Schritte durchzuführen:

1. *Anforderungen definieren:* Die Anforderungen an die Erhaltung von Datenbeständen müssen als messbare Eigenschaften definiert werden. Als Leitlinie sollten u. a. Anforderungen an die zu erhaltenden Objekteigenschaften (z. B. Inhalt, Erscheinung, Strukturierung), an die technische Umsetzung der Objekte (z. B. Verbreitung des Dateiformats, einfache Verarbeitbarkeit), an den Erhaltungsprozess (z. B. maximaler Zeitbedarf einer Konvertierung) und an die Infrastruktur (benötigte Hardware, Personal, Kosten etc.) definiert werden.
2. *Alternativen evaluieren:* Die unterschiedlichen Alternativen zur Umsetzung von Erhaltungsmaßnahmen müssen identifiziert und in einem Experiment gemessen werden.
3. *Ergebnisse analysieren:* Anhand der Experiment-Ergebnisse kann gemessen werden, wie gut eine Erhaltungsmaßnahme den verschiedenen Anforderungen entspricht. Durch die Zuordnung von Relevanzfaktoren zu den verschiedenen Anforderungen kann zwischen den Alternativen abgewogen werden.
4. *Erhaltungsplan erstellen:* Schließlich wird aus der Analyse ein Umsetzungsplan generiert.

Typische Maßnahmen zur Sicherung der technischen Nachnutzbarkeit sind die Anpassung der Software-Umgebung (wie z. B. Portierung von Software, Unterstützung weiterer Formate, Emulation) oder die Anpassung der Daten (wie z. B. Formatmigration, Konvertierung) an neue Software-Umgebungen und Anforderungen. Formatmigrationen müssen dabei nicht unmittelbar vorgenommen werden, sondern können auch erst beim erneuten Zugriff auf die Daten erfolgen, wenn entsprechende Konvertierungssoftware vorhanden ist.

Auch die Erhaltung der intellektuellen Nachnutzbarkeit – d. h., dass ein technisch einwandfrei nutzbarer Datensatz auch inhaltlich verstanden werden kann – erfordert Maßnahmen. Diese bestehen oft darin, dass zum Verständnis notwendige Kontextinformationen vor einer Veröffentlichung oder Übernahme in ein Datenarchiv dokumentiert und bei Bedarf aktualisiert werden. Das dafür benötigte Hintergrundwissen verlangt meist eine aktive Kooperation mit der wissenschaftlichen Zielgruppe. Der Bedarf für eine Aktualisierung kann z. B. entstehen, wenn sich in einer Disziplin neue Terminologien oder Verfahren etablieren, um Nutzern das Verhältnis zu den älteren Terminologien und Verfahren nachvollziehbar zu machen. Weitere Maßnahmen zur inhaltlichen Nachnutzbarkeit können die Ergänzung oder Korrektur von Datensätzen sein, sofern sie nachvollziehbar versioniert werden und sofern sie nicht als Nachweis des korrekten wissenschaftlichen Arbeitens dienen und deshalb unverändert bleiben müssen.

Der beste Weg zu der Erhaltung von digitalen Daten ist, spätere Erhaltungsmaßnahmen durch eine gute Planung der Erzeugung von Daten und Qualitätskontrollen im Ingest unnötig zu machen (siehe Kapitel 1 und 3).

## Weiterführende Literatur

- Becker, Christoph et al. (2009), Systematic planning for digital preservation: evaluating potential strategies and building preservation plans. In: *International Journal for Digital Libraries* ([Becker et al. 2009], <http://www.ifs.tuwien.ac.at/~becker/pubs/becker-ijdl2009.pdf>).
- nestor AG – Digitale Bestandserhaltung (2011). nestor Materialien 15: *Leitfaden zur digitalen Bestandserhaltung. Vorgehensmodell und Umsetzung* ([nestor AG – Digitale Bestandserhaltung 2011], <http://nbn-resolving.de/urn:nbn:de:0008-2011101804>).

## Anwendungsfall Klimaforschung

Am World Data Center for Climate (WDCC) werden nicht die Daten migriert, sondern die Software-Umgebung an neue Hardware oder Anforderungen der Nutzer angepasst. Da am WDCC nur wenige Datenformate zugelassen sind, ist dies der bequemere Weg.

## 6 Zugriff und Nutzung

Neben der reinen Erhaltung der Daten gehört die Ermöglichung der Datenutzung zu den vornehmsten Aufgaben der meisten Archive. Das Ziel des Archivs besteht dabei darin, autorisierten Nutzern den Zugang zu den Daten zu verschaffen und zugleich nicht-autorisierten Zugriff zu unterbinden – denn nur, wenn letzterer verhindert werden kann, werden Datenerzeuger mit der Aufbewahrung ihrer Daten im Archiv einverstanden sein. Die meisten Archive sind mit den folgenden Aufgaben konfrontiert:

- Nachnutzung muss möglich sein, insbesondere müssen Daten gefunden werden können.
- Nur autorisierte Nutzer dürfen Zugang erhalten.
- Rechtliche Einschränkungen müssen eingehalten werden.
- Interoperabilität soll ermöglicht werden.

### Nachnutzung und Suchbarkeit

Wenn Daten durch andere als die Produzenten nutzbar sein sollen und ein Zugriff über das Web realisiert werden soll, bietet sich ein Portal an. Ein Portal ist ein Webservice, unter dem weitere Dienste über eine grafische Oberfläche erreichbar sind. Ein bequemer Zugang zu den Daten kann im Portal mit Suchfunktionen, Orientierungshilfen und Nachbearbeitungsschritten zusammen angeboten werden. In der Praxis wichtige Nachbearbeitungsschritte sind die Visualisierung und die Konvertierung der Daten in ein Format, das von der Software des Nutzers gelesen werden kann. Die Nachbearbeitung kann bis hin zu komplexen Postprocessing-Workflows im Grid gehen. Eine Vielzahl solcher und ähnlicher Dienste kann in einem Portal bereitgestellt werden. Da das Portal gemeinsamer Einstiegspunkt im Web ist, muss die Prüfung der Identität des Nutzers (Authentifizierung) nur einmal pro Sitzung erfolgen, auch wenn mehrere Dienste in einer Sitzung genutzt werden. Als Webservice baut ein Portal auf dem HTTP-Protokoll auf.

Für den Datenzugriff außerhalb des Portals können auch andere Protokolle verwendet werden. Diese werden meist über eine Kommandozeile gesteuert. Häufig werden solche Lösungen zusätzlich zum Portal angeboten.

Für alle autorisierten Nutzer sollten die Daten suchbar sein. Ihre Existenz und der Ort ihrer Aufbewahrung können z. B. über Kataloge und Verzeich-

nisse herausgefunden werden. Effektiv und schnell ist die Suche in den Metadaten, sofern zweckmäßige, beschreibende Metadaten vorhanden sind. Wenn in den Daten selbst gesucht werden soll, müssen sich diese auf Medien befinden, auf die schnell zugegriffen werden kann, z. B. Festplatten.

Die gleichzeitige Suche in mehreren Archiven kann ermöglicht werden, wenn die für die Suche erforderlichen Metadaten eine einheitliche Struktur besitzen. Bei dem als *Harvesting* bezeichneten Verfahren werden in regelmäßigen Zeitabständen die für die Suche erforderlichen Metadaten bei den einzelnen Archiven eingesammelt und in eine zentrale Datenbank kopiert, in der dann gesucht werden kann [OAI-PMH 2008].

Ist zu Beginn der Suche unklar, welche Archive überhaupt existieren, können *Registries* helfen. In einer Registry können Archive und Dienste gesucht werden, die dort zuvor registriert worden sind.

## Offener Zugang versus Zugriffsbeschränkungen

Öffentlichkeit und Politik dürfen erwarten, dass die Mittel für die öffentliche Forschung so effizient wie möglich eingesetzt werden. Die Erzeugung von Forschungsdaten ist fast immer mit hohen Kosten verbunden. In der öffentlichen Forschung muss daher vermieden werden, dass die Produktion von gleichartigen Forschungsdaten mehrfach erfolgt und mehrfach bezahlt wird. Ein offener Zugang zu den Daten würde das gewährleisten, denn dann könnten außer den Datenproduzenten auch andere Forscher auf die Daten zugreifen und bräuchten die Daten nicht neu erzeugen.

Mit der „Berliner Erklärung“ [Berliner Erklärung 2003] sind alle wichtigen Organisationen der öffentlichen Forschung Deutschlands eine Selbstverpflichtung eingegangen, den freien Zugang zu Publikationen und allen ergänzenden Materialien zu unterstützen. Zu den Unterzeichnern [Unterzeichner der Berliner Erklärung o.J.] der Berliner Erklärung gehören der Deutsche Bibliotheksverband, die Deutsche Forschungsgemeinschaft, die Fraunhofer-Gesellschaft, die Helmholtz-Gemeinschaft, die Hochschulrektorenkonferenz, die Max-Planck-Gesellschaft, die Leibniz-Gemeinschaft und der Wissenschaftsrat. Dementsprechend wird die Vergabe von Mitteln immer häufiger an die Bedingung geknüpft, Forschungsdaten frei zugänglich zu machen.

So wünschenswert der freie Zugang auch ist: Daten, die einer Geheimhaltungspflicht unterliegen, dürfen nicht öffentlich zugänglich gemacht werden. Dies trifft für personenbezogene Daten zu, aber z. B. auch für Einzel-

daten statistischer Ämter, die zu Forschungszwecken weitergegeben wurden (§ 16 Bundesstatistikgesetz).

Die Notwendigkeit, den Zugang zu beschränken, ergibt sich nicht unbedingt nur aus gesetzlichen Vorschriften. Diejenigen, bei denen Daten zu Forschungszwecken erhoben worden sind, verlangen häufig eine Beschränkung des Zugangs, beispielsweise wenn die Daten Betriebs- oder Geschäftsgeheimnisse enthalten. In solchen Fällen werden die Daten möglicherweise erst zur Verfügung gestellt, wenn die Zugriffsbeschränkung in einem Vertrag verankert ist.

Selbst für Daten, die für die Weitergabe vorgesehen sind, können Beschränkungen gefordert werden. Ein Beispiel hierfür sind kommerziell verwertbare Daten. Hier verlangt der Datenerzeuger häufig eine Gebühr oder eine Erklärung, dass die Daten nur für wissenschaftliche oder nicht-kommerzielle Zwecke verwendet werden.

Ein ganz anderer Grund, Daten zurückzuhalten, ist Unfertigkeit: Daten, an denen noch gearbeitet wird (Arbeitskopien), sollten nur Mitgliedern der Arbeitsgruppe zugänglich sein.

Sensible Daten können durchaus gleichzeitig durch Beschränkung des Zugangs geschützt und gemeinschaftlich für Forschungszwecke genutzt werden. Ist die Nutzung eingeschränkt, müssen Nutzer ihr Einverständnis erklären, bestimmte Nutzungsbedingungen zu beachten, bevor sie Zugang zu den Daten erhalten. Die Bedingungen können die Nutzung auf einen bestimmten Zweck einschränken, z. B. fachbezogene Forschung, oder bestimmte Formen der Nutzung ausschließen, z. B. kommerzielle Nutzung oder die Rückgängigmachung von Pseudonymisierung bzw. Anonymisierung der Daten.

Die Erklärung, die Nutzungsbedingungen zu beachten, kann je nach Erfordernissen elektronisch oder schriftlich bei der Registrierung als Nutzer abgefordert werden. Es können auch strengere Zugangsregeln für sensible Daten festgelegt sein, beispielsweise:

- Einschränkung des Zugangs auf bestimmte Gruppen oder Personen
- Forderung einer Erlaubnis des Eigentümers der Daten
- gesicherter Zugang, über den die Daten nur analysiert, nicht aber kopiert werden können
- Öffnung des Zugangs erst nach Ablauf einer Sperrfrist, d. h. zu einem Termin, ab dem die Vertraulichkeit nicht länger fortbesteht. Über eine Sperrfrist kann Datenerzeugern auch eine angemessene Zeit für die Erstnutzung der Daten eingeräumt werden.

Nutzer müssen sich authentifizieren, bevor ihnen Zugang zu zugriffsbeschränkten Daten gewährt wird. In Computernetzwerken geschieht die Authentifizierung durch Versenden von Zeichenketten, die eindeutig oder nahezu eindeutig einem Nutzer zugeordnet werden können. Sehr häufig werden Benutzername/Passwort, Public-Key-Zertifikate oder OpenID verwendet, seltener Hardware wie Smartcards oder biometrische Daten wie Fingerabdrücke.

Public-Key-Zertifikate beruhen auf einem Schlüsselpaar, bestehend aus einem öffentlichen und einem geheimen Schlüssel. Das eigentliche Zertifikat setzt sich aus dem Namen, einigen weiteren Daten und dem öffentlichen Schlüssel zusammen und wird zur Authentifizierung verschickt. Der Nutzer erhält sein persönliches Zertifikat von einer Certification Authority (CA), nachdem er seinen Personalausweis bei einer Registration Authority (RA) vorgelegt hat, die für die CA die Ausweiskontrolle vornimmt.

Eine OpenID ist eine dem Nutzer zugeordnete Webadresse, die von einem OpenID-Server vergeben wird. Nutzer melden sich einmal pro Sitzung bei einem OpenID-Server mit ihrem Benutzernamen und Passwort an und können sich danach mit ihrer OpenID bei allen das System unterstützenden Webservices authentifizieren.

## Interoperabilität

Immer häufiger wird die Bereitstellung von Diensten erwartet, die Interoperabilität ermöglichen. Interoperabilität ist unverzichtbar für gemeinschaftlich betriebene Informationsarchitekturen. Die Wortbedeutung und praktische Verwirklichung dieses Konzeptes sind jedoch außerordentlich unterschiedlich [Gradmann 2008]: Interoperabilität kann aus einer objektbezogenen oder einer funktionalen Perspektive gesehen werden, aus der Sicht der Institution oder des Nutzers. Darüber hinaus wurde Interoperabilität auf verschiedenen Abstraktionsebenen konzipiert (siehe Abb. 5).

Von der Funktion her betrachtet, können interoperable Dienste einfach digitale Inhalte austauschen. Die Funktionalität kann aber auch weit darüber hinausgehen. Beispielsweise können digitale Objekte zu einer gemeinsamen Inhaltsschicht verknüpft werden. Auch kann über Interoperabilität eine gemeinsame Dienstarchitektur etabliert werden.

Die zusammenwirkenden Elemente können sowohl traditionelle Institutionen (Archive, Bibliotheken, Museen) oder digitale Repositories, E-Science- und E-Learning-Plattformen oder einfach nur Webservices sein. Interope-

rabilität ist also keineswegs auf Institutionen beschränkt, sondern schließt auch Fragen wie die folgende mit ein: Wie können IT-gestützte Tools geeignete Informationen finden, um mit fachfremden oder ungewöhnlich strukturierten Daten arbeiten zu können?

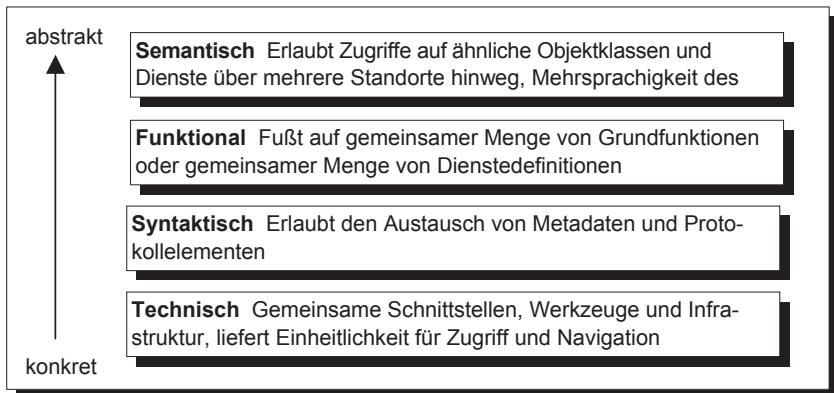


Abb. 5 Abstraktionsstufen der Interoperabilität nach [Gradmann 2008]

## Weiterführende Literatur

- Gradmann, Stefan (2008): *Interoperability: A key concept for large scale, persistent digital libraries*. DigitalPreservationEurope (DPE) Briefing Paper ([Gradmann 2008], <http://www.digitalpreservationeurope.eu/publications/briefs/interoperability.pdf>).
- *nestor Handbuch*, Version 2.3 [Neuroth et al., 2010]: Kapitel 9.3, Retrieval (<http://nbn-resolving.de/urn:nbn:de:0008-2010071949>).

## Anwendungsfall Klimaforschung

Der Zugang zum World Data Center for Climate (WDCC) [WDCC] kann online über grafische Benutzerschnittstellen auf zwei verschiedenen Wegen erfolgen.

Der eine Weg führt über das CERA-Portal [CERA]. CERA steht für „Climate and Environment data Retrieval and Archiving system“. Das CERA-Portal wird wie das WDCC vom Deutschen Klimarechenzentrum betrieben. Über das CERA-Portal sind alle Datensätze des WDCC erreichbar. Gesucht werden kann in den Metadaten, und zwar nach folgenden Strategien:

- über eine Liste der Experimente<sup>4</sup>
- über Begriffe, die aus einer Liste ausgewählt werden können
- über den Namen der Modell-Software (Code-Suche)
- Volltextsuche
- hierarchische Suche in einer Baumstruktur aus Oberbegriffen und Begriffen
- Suche in einer Tabelle mit Autorennamen, Titel und DOI.

Nach erfolgreicher Suche kann auf die Daten per Download zugegriffen werden. Für die Nachbearbeitung stehen Zeit- und Datenformatkonvertierer sowie fachspezifische Berechnungswerzeuge zur Verfügung.

Der zweite Weg zu Daten des WDCC führt über das C3Grid-Portal [C3Grid-Portal]. Über das in Abb. 6 auf S. 45 gezeigte Webformular kann in den Metadaten gesucht werden. Nach erfolgreicher Suche können die Daten per Grid-Job geholt werden. Dabei kommt im C3Grid die Eigenentwicklung GNDMS (Generation N Data Management System) [GNDMS] zum Einsatz, die auch Postprocessing-Workflows steuert. Solche Workflows zur rechnerischen Weiterverarbeitung der Daten können ebenfalls über das C3Grid-Portal gestartet werden. Hierfür sucht sich der Nutzer einen der vorgegebenen, fachspezifischen Workflows aus einer Liste aus und startet den Grid-Job über das Portal. Die Workflow-Software kann nicht über das Portal verändert werden. Zusätzlich benötigte Parameter können aber über ein Webformular mitgegeben werden.

Die Nutzungsbedingungen der Archive werden durchgesetzt, indem der Nutzer zusätzlich zum Benutzerkonto für das C3Grid-Portal künftig auch die Nutzungsberechtigungen für die gewünschten Archive haben muss. Am WDCC muss der Nutzer bei erstmaliger Anmeldung die Nutzungsbedingungen akzeptieren und bekommt bei Aufnahme in den Nutzerkreis ein persönliches Nutzerkonto. Nutzerkonten für Gruppen gibt es nicht. Der Zugang zu Daten, vor deren Nutzung der Nutzer eine Erklärung unterschreiben muss, wird gesondert freigeschaltet. Dies geschieht, indem der Nutzer in die entsprechende Gruppe der Nutzungsberechtigten für diese speziellen Daten eingetragen wird. Technisch werden die Zugriffsbeschränkungen durch Abfrage einer Oracle-Datenbank durchgesetzt. Dort werden die Tabellen mit den Berechtigungengruppen gehalten.

---

<sup>4</sup> „Experiment“ bedeutet hier Modellrechnung. Modellrechnungen sind sozusagen numerische Experimente.



Welcome , Torsten Rathmann [Profile](#) [Home](#) [Logout](#)

[C3 Status](#) [My C3Grid](#) [Search & Download](#) [Workflows](#) [Test Suite](#)

### Data Retrieval

[Free Search](#) [Advanced Search](#) [Browse Catalogs](#) [My Stored Queries](#) [My Stored Downloads](#)

[reset](#) [start search](#)

<b>Free Search</b> <a href="#">?</a> <input type="text"/>	<b>Time Constraints</b> <a href="#">?</a> <input checked="" type="checkbox"/> activate this box Start Date <input type="button" value="after"/> 1900-01-01 12:00 End Date <input type="button" value="before"/> 2100-01-01 12:00
<b>Vertical Constraints</b> <a href="#">?</a> <input type="checkbox"/> activate this box Min Vertical <input type="button" value="1"/> level Max Vertical <input type="button" value="1"/> level Vertical Type <input type="button" value="Column Density"/>	<b>Geographical Constraints</b> <a href="#">?</a> <input checked="" type="checkbox"/> activate this box Min Lat <input type="button" value="-90.00"/> World Max Lat <input type="button" value="90.00"/> Min Lon <input type="button" value="0.00"/> Max Lon <input type="button" value="360.00"/> <input type="button" value="within"/>
<b>Content Constraints</b> <a href="#">?</a> <input type="text"/> 2m temperature FAO data set (sol data flags)#nonCF air_pressure_at_convective_cloud_top (maximum) <b>air_pressure_at_sea_level</b> air_temperature air_temperature (mean per month of four values a day) air_temperature (mean per month) <b>air_temperature-at2m</b> air_temperature-at2m (maximum per ...) air_temperature-at2m (mean per month of maximum) air_temperature-at2m (mean per month of minimum) air_temperature-at2m (mean per month)	<b>Keywords</b> <a href="#">?</a> <input type="text"/> "climate simulation" "scenario run" Arctic River Discharge CMIP Climate Modeling ECHAM4 ECHAM5 ECHO-G Eurasia HOPE Hydrological Cycle ipcc AR4

Abb. 6 Formular zur Datensuche im C3Grid-Portal

Dateneigentümer wollen informiert werden, welche Nutzer ihre Daten heruntergeladen haben. Je nach Wunsch des Dateneigentümers geht diese Information sofort nach dem Download an den Dateneigentümer oder in regelmäßigen Zeitabständen in Form einer zusammenfassenden Liste.

Inhaltlich ist das Datenangebot der Portale verschieden. Über das CERA-Portal sind alle WDCC-Daten und nur diese zugänglich. Über das C3Grid-Portal ist eine Teilmenge der Daten aller am C3Grid beteiligten Institutionen zugänglich. Eine Verpflichtung, den Zugriff auf Daten über das C3Grid zu

ermöglichen, besteht nicht. Welche Daten über das C3Grid zur Verfügung gestellt werden, entscheidet jede Institution für sich.

## **Teil II: Übergreifende Aufgaben des Forschungsdatenmanagements**

Die in jeder Station des Lebenszyklus der Daten vorkommenden Aufgaben (vgl. Abb. 2, S. 16) sind im Wesentlichen nicht IT-bezogenen, sondern beziehen sich auf die Herstellung von geeigneten Rahmenbedingungen, unter denen das Datenmanagement bzw. die Langzeitarchivierung gesichert werden kann.

### **7 Organisation, Management und Policies**

Die Forschungsdaten werden von einzelnen Forschern, Forschungsgruppen innerhalb einer Einrichtung, überinstitutionellen Gruppen sowie Kollaborationen auf nationaler oder internationaler Ebene erzeugt.

#### **Organisation**

Es muss geklärt werden, an welcher Stelle die Daten abgelegt werden können und sollen, wer (welche Personen, Abteilung, Organisation) für die Aufbewahrung zuständig ist und nach welchen Kriterien die Weitergabe der Daten erfolgen soll.

Ein Datenarchiv ist die Organisationseinheit, die die Aufgabe des Datenmanagements in einem festgelegten Bezugsrahmen verantwortlich übernimmt. Ein Repository ist die Realisierung eines Datenspeichers in einem Datenarchiv.

Es gibt verschiedene Formen eines Datenarchivs, die sich in ihrem Bezugsrahmen unterscheiden und damit auch in der Festlegung ihrer Managementstrukturen und Policies unterschiedlich sind.

- **Institutionelles Datenarchiv:** Als Beispiel kann eine Universität dienen, die neben den Diplomarbeiten/Dissertationen/Habilitationen auch die Daten zu diesen Arbeiten speichert. Die Konzeption eines solchen Repository bedarf einer Policy der Universität, in welcher die Form und die Verpflichtung der Abgabe dieser Daten sowie deren Nutzungsbedingun-

gen geregelt sind. Eine solche Policy regelt konzeptuell das Datenmanagement eines Teils der von der Institution erzeugten Daten. Der Datenmanagement-Plan muss darüber hinaus die Implementierung des Repository und die Sicherstellung des Betriebs beinhalten. Die Universität hat hierfür organisatorische Voraussetzungen zu schaffen: Bereitstellung von IT-Infrastruktur, Bereitstellung von Services für den Ingest der Daten und deren Publikation. (Diese Aufgabe ist nicht spezifisch für eine einzelne Universität; die Entwicklung von standardisierten Metadaten und Verfahren hierfür wäre sinnvoll.)

- **Kollaborations-Datenarchiv:** Hierfür lässt sich als Beispiel eine (internationale) Kollaboration zur Nutzung eines Instruments nennen. Solche Kollaborationen entstehen oft aus der Notwendigkeit heraus, knappe Ressourcen optimal auszunutzen. Die Nutzung der Daten wird von den Beteiligten in erster Linie als Eigennutzung konzipiert – und unter diesem Gesichtspunkt werden die Vorgaben für die Datenspeicherung und Nutzung vor allem von den individuellen Interessen der Beteiligten gelehnt.

Die Fördergeber verbinden mit der Vergabe der Mittel jedoch mittlerweile eine – zeitgemäße – Auflage zur Veröffentlichung der Daten. Zudem sind die Größenordnungen dieser Daten auch für eine Auswertung/Speicherung durch die einzelnen Beteiligten meist nicht mehr geeignet. Daher werden in größeren Vorhaben explizit Mittel für ein gemeinsames Datenmanagement bereitgestellt und eine oder mehrere der beteiligten Institutionen stellen die technische Infrastruktur sowie Know-how und Dienste für das Management der Daten des Instruments bereit.

Für die Policy eines solchen Repository sind in erster Linie die Kollaborations-Vereinbarungen bindend. Die langfristige Sicherstellung der Verfügbarkeit der Daten ist in diesen Fällen oft von den Institutionen abhängig, die das Repository betreiben. Charakteristisch sind zeitlich befristete Zugangsbeschränkungen und eine partielle Publikation von Daten; eine Strukturierung der Daten unter Einbeziehung der Gesichtspunkte der späteren Publikation ist daher sinnvoll.

- **Thematicsches Datenarchiv:** In diese Kategorie fallen z. B. Einrichtungen wie das Institut für Deutsche Sprache, das Deutsche Institut für Wirtschaft oder auch eine Gen-Datenbank. Während der Bezugsrahmen durch das Thema vorgegeben ist, werden hier vor allem Datenschutz, Vertraulichkeit und auch wirtschaftliche Interessenkonstellationen einen großen Einfluss haben. Auch hier ist eine Policy erforderlich, welche die thema-

tische Abgrenzung der Daten, die Aufnahme der Daten und deren Publikation bzw. Nutzung regelt.

Die Policies dieser thematischen Repositories sind stark beeinflusst von den Vorgaben der Fördermittelgeber oder der „Datenprovider“ (beispielsweise Statistische Ämter, Sozial- oder Arbeitsämter oder Wirtschaftsverbände). Die Bereitstellung der Daten und deren Pflege ist Daseinszweck dieser Art von Datenarchiv und die Festlegung von Policies für den Ingest, den Zugriff und die Leistungen des Archivs ist ein wesentliches, konstituierendes Element.

## **Management**

Die Strukturierung der Daten nach bestimmten (meist fachlichen) Kriterien sowie die Auswahl von zu verwendenden Metadaten zur Beschreibung von Inhalt und Kontext sind Komponenten des Datenmanagements. Zwar hat jede Domäne (vgl. Abb. 3, S. 18) eigene Notwendigkeiten, jedoch ist es sinnvoll, klare Regelungen zu haben, welche die Aufbewahrung und Weitergabe der Daten betreffen. Die Handhabung der Daten kann durch die Regelungen der Fachgemeinschaft, der Institution, der Kollaboration oder auch des Fördergebers beeinflusst oder vorgegeben sein.

Der Datenmanagementplan regelt die Implementierung und die Sicherstellung des Betriebs des Datenarchivs. Zur Implementierung des Datenmanagements ist eine Analyse des Workflows von der Erzeugung der Daten bis zu deren Nutzung notwendig. Eine Abgrenzung von Daten, die im Repository vorzuhalten sind, und intermediären Daten muss anhand dieser Analyse vorgenommen werden. Zudem sind Regelungen über die zeitliche Dauer der Datenvorhaltung notwendig. Ein weiterer Bestandteil des Datenmanagementplans ist die Qualitätskontrolle, welche den Gehalt der Daten und deren technische Integrität bewertet. Beim Übergang von der privaten zur Gruppendomain ist eine Selektion und Qualitätskontrolle relativ leicht zu realisieren, z. B. in einer Kollaboration, in der die Forscher „live“ mit den Daten arbeiten. Beim Übergang von der Gruppen- in die Public Domain sind adäquate Formen der Qualitätskontrolle und Selektion bisher nur in Ansätzen vorhanden. Eine dieser Formen ist das Data-Release für Kollaborations-Repositories, welches eine wissenschaftliche Bewertung der publizierten Daten beinhaltet. Für thematische oder institutionelle Repositories existieren solche Prozesse derzeit nur bedingt.

Werden Forschungsdaten durch ein internationales Konsortium erzeugt, so wird die Verwendung von Standards für diese Daten geradezu eine unumgängliche Notwendigkeit. Insbesondere, um diese Daten für IT-basiertes Data-Mining zugänglich zu machen, werden die z. B. vom Virtual Observatory in der Astronomie oder dem Open Geospatial Consortium vorgeschlagenen Standards und Tools ein wichtiger Teil der vom Datenmanagement zu berücksichtigenden Komponenten.

Ein wesentliches Charakteristikum des modernen Datenarchivs ist, dass Aufbau und Betrieb kaum mehr als Nebenaufgaben eines oder mehrerer beteiligter Wissenschaftler zu realisieren sind. Dementsprechend gehört auch die Bereitstellung von ausreichenden Personalreserven mit den erforderlichen Qualifikationen zu den Komponenten eines Datenmanagementplans.

## Policies

Policies regeln in Bezug auf das Datenarchiv die grundlegenden Verfahren zur Aufnahme, zur Bereitstellung und zum Zugriff auf die Daten. Solche Policies werden innerhalb eines organisatorischen Rahmens festgelegt und gelten nur innerhalb desselben. Bei überinstitutionellen Zusammenschlüssen (Kollaborationen, Arbeitsgruppen) ist es erforderlich, dass der Betrieb des Repository von bestehenden Organisationen/Institutionen verpflichtend übernommen wird, und dass Regelungen für die Zeit nach Beendigung der Zusammenarbeit getroffen werden. Darüber hinaus wird durch Policies festgelegt, welche Nutzung der Daten vom Archiv als zulässig gewertet wird, ob und in welcher Form Lizenzen, Gebühren etc. erhoben werden, welche Nutzergruppen autorisiert sind usw.

## Anwendungsfall Klimaforschung

Das C3Grid (Collaborative Climate Community Data and Processing Grid) [C3Grid Website] ist ein echtes Datengrid, in dem die Daten über verschiedene Standorte verteilt liegen. Drei ICSU-Welddatenzentren (WDCC [WDCC], WDC-MARE [WDC-MARE], WDC-RSAT [WDC-RSAT]), der Deutsche Wetterdienst (DWD) [Deutscher Wetterdienst] und eine Reihe weiterer Archive kooperieren im C3Grid, um eine einheitliche Plattform für den Zugriff auf Klimadaten anzubieten. Die Entscheidung, welche Daten über das C3Grid-Portal [C3Grid-Portal] zugänglich gemacht werden, liegt

bei den einzelnen Datenzentren. Generell nicht über das Grid zugänglich sind Daten, vor deren Nutzung eine schriftliche Erklärung unterzeichnet werden muss.

Wie wird die Einhaltung der Planung überprüft oder nachgewiesen? Im C3Grid erfolgen Überprüfung und Nachweis der Einhaltung der Planung durch Projektberichte. Am WDCC gibt es drei Nachweis- bzw. Prüfverfahren:

- regelmäßige Reviews (Metadaten und Datenkonsistenz)
- halbjährliche Überprüfung auf nationaler Ebene durch den Wissenschaftlichen Lenkungsausschuss (Verfügbarkeit der WDCC-Dienste für die Community)
- alle fünf Jahre internationale Begutachtung im Rahmen der Rechnerbeschaffung (Ausstattung)

## 8 Kosten

Mit den fallenden Preisen für Speichermedien scheint oftmals der Eindruck entstanden zu sein, dass das Aufbewahren von Daten kaum Kosten und Aufwand verursachen kann. Aber eine der größten Gefahren für den langfristigen Erhalt von Forschungsdaten sind fehlende finanzielle und personelle Ressourcen. Eine Voraussetzung, damit Forschungsinstitutionen mit den meist knappen verfügbaren Mitteln die wichtigsten Aufgaben erfüllen können, besteht darin, den mit den Aufgaben verbundenen Aufwand abschätzen zu können. Bei Entscheidungen und Abschätzungen der benötigten finanziellen und personellen Ressourcen sollten einige grundlegende Faktoren bedacht werden:

- **Teil der Nutzungskosten** Das Aufbewahren und die Pflege von Forschungsdaten-beständen wird nicht um der Tätigkeit selbst willen durchgeführt, sondern weil es möglich sein soll, die Forschungsdaten zu nutzen. Entsprechend wichtig ist es, den Nutzen eines Forschungsdatenbestandes herauszuarbeiten und die Kosten des Datenmanagements nicht als zusätzliche und optionale Kosten, sondern als genauso notwendig für die Nutzung aufzufassen wie die Produktionskosten selbst.<sup>5</sup> Die Kosten

---

<sup>5</sup> Um den Nutzen bei Bedarf genauer auszuarbeiten, bieten sich die im Rahmen der Keeping-Research-Data-Safe-Projekte entwickelten Instrumente an, siehe [KRDS-I2S2-

des Datenmanagements sind somit ein notwendiger Teil der gesamten Nutzungskosten.

- **Höchste Kosten am Anfang** Digitale Forschungsdaten haben oftmals einen langfristigen Wert – aber genauso langfristig müssen auch Aufwände und Investitionen erfolgen, um diesen Wert zu erhalten. Bei einer groben Einteilung der Datenerhaltung in die Übernahme-, Speicher- und Zugriffsphase lassen sich ungefähr die Hälfte der Kosten der Übernahme in das Archiv zuordnen. Die zweitaufwendigste Phase ist der Zugriff, die Speicherphase ist am günstigsten.<sup>6</sup>
- **Warten und Nichtstun ist teuer** Diese am Anfang entstehenden hohen Kosten können kaum aufgeschoben werden, weil das spätere Nacharbeiten noch mehr Kosten verursacht. Ein Beispiel sind die Aufwände für Qualitätskontrolle und Metadaten, die zudem eine höhere Effizienz bei den restlichen Archivabläufen ermöglichen.<sup>7</sup>
- **Personalkosten** Den größten Anteil an den Kosten für ein verlässliches Datenmanagement stellt ausreichend qualifiziertes Personal dar und nicht Hard- oder Software. KRDS gibt eine Größenordnung von 70 Prozent und mehr für Personalkosten an [Beagrie et al. 2011, S. 14].
- **Sinkende jährliche Kosten** Aufgrund der hohen einmaligen Anfangskosten und der zunehmenden Effizienz der Technologien sinken die jährlichen Kosten für die Aufbewahrung eines Datenbestand. Dies hat z. B. zur Entwicklung eines simplen Geschäftsmodells „Pay Once, Store Forever“<sup>8</sup> an der Princeton University geführt, das aber auch nur einen sehr begrenzten Service vorsieht.
- **Anreize** Nicht nur unklare Vorstellungen vom langfristigen Nutzen und mangelnde Mittel können notwendige Maßnahmen verhindern, sondern auch fehlende Anreize. Anders als viele analoge Güter werden Informa-

---

Tools]. Einige grundlegende ökonomische Eigenschaften der Bewahrung digitaler Daten wurden im Abschlussbericht der Blue Ribbon Task Force erläutert, siehe [Blue Ribbon Task Force 2010].

6 Für den Archaeology Data Service wird eine als typisch angesehene Kostenstaffelung von circa 55 Prozent in Outreach/Acquisition/Ingest, circa 31 Prozent in Access und ungefähr 15 Prozent bei Archival Storage und Preservation angegeben, vgl. [Beagrie et al. 2010, S. 79].

7 In Studien wurde abgeschätzt, dass es durchaus eine Größenordnung teurer sein kann, nachträglich Metadaten zu erzeugen, vgl. [Nationale Archief 2005, S. 15].

8 Siehe [Goldstein & Ratliff 2010, S. 1].

tionsgüter nicht durch die Nutzung aufgebraucht. Es reicht daher im Prinzip eine Partei aus, die den Aufwand des Forschungsdaten-Managements treibt, damit beliebig viele andere ohne Aufwand die Daten nutzen können.<sup>9</sup> Gesamtwirtschaftlich betrachtet kann das sehr sinnvoll sein, aber einzelne Wissenschaftler oder Institutionen könnten demotiviert werden, diesen Aufwand zu erbringen, wenn Dritte den Nutzen ohne Ge-genleistung erhalten. Aus diesem Grund sind Erstverwertungsrechte oder das Zitieren von Forschungsdaten wichtige Faktoren im Forschungsdaten-Management, um die notwendige Anerkennung zu gewährleisten.

Zur eigentlichen Bestimmung der Kosten der Bewahrung digitaler Daten haben zwei mehrphasige Projekte Modelle und Fallstudien entwickelt: Keeping Research Data Safe und das LIFE-Projekt. In beiden Fällen orientieren sich die Berechnungsgrundlagen am DCC Curation Lifecycle Model (siehe Abb. 1 *Aufgaben im Lebenszyklus von Forschungsdaten*, S. 15). Eine Kostenplanung kann eine Abschätzung der Kosten – an den einzelnen Phasen orientiert – durchführen. Im KRDS-Modell gliedern sich die Kostenkategorien, in welche die einzelnen Phasen eingesortiert werden, grob wie folgt [Beagrie et al. 2010, S. 14–26]:

- Vorarchiv-Phase: Hier fallen neben den Kosten für die Erschaffung der Daten auch Kosten an für Beratung, Schulung und die Planung des Datenmanagements selbst.
- Archiv-Phase: Die wesentlichen Kostenkategorien in diesem Abschnitt sind die Kosten für alle einzelnen Lebenszyklusphasen, die in dem Modell dieses Leitfadens von Auswahl und Bewertung bis Zugriff und Nutzung reichen. Zusätzlich werden insbesondere Innovationskosten für die Entwicklung von neuen Werkzeugen, Standards etc. darunter verbucht.
- Unterstützungsdiene: Kosten für die Verwaltung aller Aktivitäten und die allgemeine IT-Basisinfrastruktur.
- Gebäude: Aufwände im Zusammenhang mit benötigten Räumen und Gebäuden.

---

<sup>9</sup> “Digital assets are nonrival in consumption and create a free-rider potential” [Blue Ribbon Task Force 2010, S. 24].

## Weiterführende Literatur

- Ayrис, P. et al. (2008): The LIFE2 final project report. LIFE Project, London, UK ([Ayrис et al. 2008], <http://eprints.ucl.ac.uk/11758/1/11758.pdf>).
- Beagrie, Neil et al. (2010): User Guide for Keeping Research Data Safe ([Beagrie et al. 2011], [http://www.beagrie.com/KeepingResearchDataSafe\\_UserGuide\\_v2.pdf](http://www.beagrie.com/KeepingResearchDataSafe_UserGuide_v2.pdf)).
- Blue Ribbon Task Force (2010): Sustainable Economics for a Digital Planet ([Blue Ribbon Task Force 2010], [http://brtf.sdsc.edu/biblio/BRTF\\_Final\\_Report.pdf](http://brtf.sdsc.edu/biblio/BRTF_Final_Report.pdf)).
- Charles Beagrie Ltd / JISC (Hrsg.) (2010): Keeping Research Data Safe Factsheet [Charles Beagrie Ltd / JISC 2010], [http://www.beagrie.com/KRDS\\_Factsheet\\_0910.pdf](http://www.beagrie.com/KRDS_Factsheet_0910.pdf)).

## Anwendungsfall Klimaforschung

C3Grid [C3Grid Website] hat von September 2005 bis August 2008 eine Projektförderung vom Bundesministerium für Bildung und Forschung (BMBF), Referat „Internet“, bekommen. Das Nachfolgeprojekt C3-INAD<sup>10</sup> wird jetzt vom Fachreferat „Globaler Wandel“ des BMBF gefördert. Der Förderungszeitraum reicht von Oktober 2010 bis September 2013.

Das World Data Center for Climate (WDCC) [WDCC] wird am Deutschen Klimarechenzentrum (DKRZ) [Deutsches Klimarechenzentrum] betrieben, dessen Betrieb wiederum von den vier Gesellschaftern (Helmholtz-Zentrum Geesthacht, Max-Planck-Gesellschaft, Freie und Hansestadt Hamburg, Alfred-Wegener-Institut für Polar- und Meeresforschung Bremerhaven) finanziert wird.

Die Archivierung von Daten ist am WDCC für externe Auftraggeber kostenpflichtig. Die Kosten für die Archivierung müssen in der Regel von demjenigen getragen werden, der den Auftrag für den Ingest gegeben hat. Das Abrufen von Daten über das Web ist dagegen kostenfrei, sofern die Daten nur für wissenschaftliche Zwecke verwendet werden. Im Falle von Sonderwünschen, z. B. Bereitstellung von Daten auf CD, werden die Kosten für das Kopieren und Verschicken in Rechnung gestellt.

---

10 INAD steht für „Towards an Infrastructure for General Access to Climate Data“.

Bisher wurden hauptsächlich Klimadaten von Institutionen archiviert, die zugleich DKRZ-Nutzer sind. In diesem Fall werden die Kosten mit den bewilligten Kontingenten verrechnet und die Speicherung ist de facto kostenfrei. In letzter Zeit sind die Archivierungsdienste des WDCC anscheinend auch für externe Kunden interessant geworden, z. B. für Forschungsinstitute, die sich den Aufbau eines eigenen Langzeitarchivs ersparen wollen. Von daher zeichnet sich eine zusätzliche, wenn auch eng begrenzte Einnahmequelle für das Archiv ab. Kunden müssen lediglich einen Selbstkostenbeitrag leisten. Gewinne darf das DKRZ als gemeinnützige GmbH nicht erzielen. Ein höherer als der Selbstkostenpreis widerspricht auch den Regeln [WDC Principles 2012] für ICSU-Welddatenzentren [International Council for Science]. Solange es keine umfassenden Erfahrungen mit den tatsächlich anfallenden Kosten gibt, stellt das DKRZ den Einstellern Schätzkosten nach Tab. 1 in Rechnung. Auch von den zahlenden Kunden werden nur Daten angenommen, die den Regeln für eine Archivierung im WDCC entsprechen.<sup>11</sup>

*Tabelle 1: Kosten für die Datenspeicherung am DKRZ*

	1 Experiment, 1 TB	10 Exp. ähnl. Struktur, 15 TB
Summe Daten-/Metadatenspeicherung	0,30 PM	0,76 PM
LZA (10 Jahre) inkl. Pflege	0,35 PM	1,35 PM
Medien und Betriebskosten für 10 Jahre inkl. 2 Kassetten-Upgrades	400 Euro	6000 Euro
Kosten für DOI-Registrierung (optional)	0,15 PM	0,55 PM

PM = Personenmonate, Experiment steht für Modellrechnung (numerisches Experiment)

## 9 Rechtliche Aspekte von Forschungsdaten

Im wesentlichen lassen sich für Forschungsdaten zwei Bereiche unterscheiden, in denen rechtliche Fragen Bedeutung erlangen. Zum einen ist dies das Feld des Datenschutzes, typischerweise der Schutz personenbezogener Daten vor unbefugtem Zugriff, und zum anderen Fragen des Urheberrechtes. Bei

---

<sup>11</sup> Regeln siehe Abschnitte 2 und 3.

letzterem sind wiederum zwei verschiedene Aspekte zu betrachten, nämlich einerseits die Be- oder Nachnutzung von urheberrechtlich geschützten Werken (z. B. Datenbanken oder Programmen), zum anderen die Erstellung neuer urheberrechtlich geschützter Objekte bzw. die Kontrolle über die bei der Erstellung sich ergebenden Rechte.

## Datenschutz – personenbezogene Daten

Forschungsdaten unterliegen einer Reihe von deutschen und internationalen Gesetzen. Das Bundesdatenschutzgesetz (BDSG) stellt die primäre Referenz der gesetzlichen Bestimmungen über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten dar und betrifft sowohl Behörden als auch nicht-staatliche Institutionen – neben dem Bundesrecht weist jedes der 16 Bundesländer eine eigene Gesetzgebung auf. Personenbezogene Daten dürfen nur erhoben werden, wenn dies gesetzlich zulässig ist (z. B. mittels gerichtlicher Anordnung) oder die betroffene Person eingewilligt hat; in der Regel muss diese Einwilligung schriftlich gegeben werden.

Zweck des BDSGs ist es, Einzelne vor Missbrauch ihrer personenbezogenen Daten zu schützen. Solche Daten umfassen Namen, Geburtsdatum, Patientendaten und andere vertrauliche Informationen. Personen, die mit der Erhebung oder Verarbeitung personenbezogener Daten beschäftigt sind, ist es untersagt, diese Daten ohne Genehmigung zu beschaffen, zu nutzen oder weiterzuverarbeiten – und sie sind verpflichtet, das Datengeheimnis auch nach Ende ihrer Tätigkeit zu wahren.

Das BDSG enthält besondere Bestimmungen zur Verwendung personenbezogener Daten zum Zwecke der Forschung. Es besagt, dass personenbezogene Daten, die zu wissenschaftlichen Zwecken erhoben oder gespeichert wurden, nur im Rahmen dieser Zwecke verarbeitet oder genutzt werden dürfen. Die so erhobenen Daten müssen anonymisiert werden, sobald es der Forschungsprozess erlaubt. Bis zu diesem Zeitpunkt müssen Daten, die einer bestimmten Person zugeordnet sind oder werden können, gesondert aufbewahrt werden und dürfen nur soweit mit anderen Daten kombiniert werden, wie es der Forschungszweck erfordert. Wissenschaftliche Institutionen dürfen personenbezogene Daten nur veröffentlichen, wenn das Einverständnis der entsprechenden Person vorliegt oder die Veröffentlichung der Daten für die Präsentation von Forschungsergebnissen zu aktuellen Ereignissen unverzichtbar ist.

## **Urheberrecht**

Prinzipiell unterliegen Forschungsdaten in Deutschland dem Urheberrecht. Der Urheberschutz greift allerdings erst dann, wenn ein Werk die Erfordernisse des persönlichen Schaffens, der wahrnehmbaren Formgestaltung, des geistigen Gehalts und der eigenpersönlichen Prägung erfüllt.<sup>12</sup> Auf Forschungsdaten trifft dies jedoch nicht immer zu (z. B. bei unstrukturierten Messdaten); sie sind daher oft nicht urheberrechtlich geschützt. Anders verhält es sich, wenn für die Erstellung, Darstellung oder Auswertung der Forschungsdaten eigene Programme entwickelt oder die Daten in einer Datenbank gesammelt werden. Dies kann durchaus einen eigenen Urheberschutz begründen und sollte daher von Projektseite bedacht und gestaltet werden, insbesondere wenn diese Werke in die Speicherung der Forschungsdaten einzbezogen werden.

Wenn das Werk vom deutschen Urheberrecht geschützt ist, sind nur bestimmte Nutzungsarten ohne Zustimmung des Urhebers zulässig. Dazu gehören:

- Vervielfältigung von bloßen Fakten im Rahmen eigener Interpretation oder Wortwahl,
- Vervielfältigungen zum privaten Gebrauch,
- Vervielfältigung, Verbreitung und öffentliche Wiedergabe im Rahmen eines Zitats.

## **Urheberrecht bei fremden Daten**

Grundsätzlich müssen bei wissenschaftlicher Forschung die Rechte an geistigem Eigentum berücksichtigt werden. Ist ein Werk urheberrechtlich geschützt, ist die Einwilligung der Urheber zu dessen Vervielfältigung oder Weiterverbreitung unabdingbar. In diesem Zusammenhang ist zu berücksichtigen, dass Datenbanken<sup>13</sup> nach deutschem Recht einem spezifischen Schutz unterliegen, der den Erstellern der Datenbank das alleinige Recht zu ihrer Verbreitung und Vervielfältigung gewährt. Lediglich die Verwendung eines

---

12 Siehe Lutz, Peter: *Grundriss des Urheberrechts*. C. F. Müller, Heidelberg 2009, Rn. 37–86d, zitiert nach *Wikipedia*, [http://de.wikipedia.org/wiki/Deutsches\\_Urheberrecht](http://de.wikipedia.org/wiki/Deutsches_Urheberrecht).

13 Gemeint sind hier die in Datenbanken gespeicherten Daten, also nicht die Architektur oder Verwaltungssoftware einer Datenbank.

*unwesentlichen* Teils der Datenbank ist ohne Zustimmung des Datenbankherstellers erlaubt; für die Vervielfältigung eines *wesentlichen* Teils einer Datenbank ist eine Einwilligung außerdem dann nicht erforderlich, wenn diese Vervielfältigung zum privaten Gebrauch oder zur Veranschaulichung im Unterricht erfolgt.

Darüber hinaus sind Kopien – sowohl von Datenbanken als auch allgemein von urheberrechtlich geschützten Werken – zum persönlichen wissenschaftlichen Gebrauch<sup>14</sup> zulässig, wenn die Vervielfältigung zu diesem Zweck geboten<sup>15</sup> ist und keinen gewerblichen Zwecken dient. Die Speicherung von urheberrechtlich geschützten Daten durch Forschungseinrichtungen fällt hingegen normalerweise nicht unter diese Regel, da dieser Vorgang üblicherweise auf eine Verfügbarmachung für mehr als eine Person und den Austausch mit anderen Forschern abzielt.

Insofern ist bei der Verwaltung von Forschungsdaten zu bedenken, welche Fremddaten und -programme benutzt wurden und welche Einschränkungen mit deren Verwendung verbunden sind. Insbesondere stellt sich die Frage, ob diese Daten und Programme mit in die Archivierung einbezogen werden dürfen. In Zweifelsfällen sollte eine Klärung mit den Rechteinhabern angestrebt werden, die gegebenenfalls in die Form eines rechtsverbindlichen Vertrages münden sollte.

## Urheberrecht bei eigenen Daten

Nicht nur für den rechtlichen Schutz der verwendeten fremden Daten sollten Überlegungen angestellt werden, sondern auch bezüglich der Rechte an den im Rahmen des Projektes erstellten eigenen Daten – und dazu, wie die Einhaltung dieser Rechte kontrolliert werden kann. Hierbei sollten auch die in Kap. 8 erwähnten Anreize und deren rechtliche Umsetzung beachtet werden.

Zur Festlegung von Nutzungsrechten existiert mittlerweile ein breites Spektrum von möglichen Lizenzierungsmodellen, deren Erläuterung den Rahmen dieses Leitfadens sprengen würde. Wenn keine oder nur spezifische

---

<sup>14</sup> Der „persönliche wissenschaftliche Gebrauch“ umfasst das Kopieren innerhalb einer unzugänglichen Umgebung und den Ausschluss einer Weitergabe an Dritte.

<sup>15</sup> Als „geboten“ kann die Vervielfältigung dann bezeichnet werden, wenn sie die wissenschaftliche Forschung erfordert und der Kauf einer Kopie nicht zumutbar oder problematisch ist.

Restriktionen gewünscht werden, so können diese wohl am einfachsten mit einer geeigneten offenen Lizenz (z. B. GPL oder Creative Commons) versehen werden. Zu beachten sind jedoch Fälle, bei denen in die Erstellung von eigenen Programmen fremde Software eingegangen ist: Hier können die dafür bestehenden Lizenzen die Wahl eigener Lizenzierungsmöglichkeiten einschränken (z. B. durch das „Copyleft-Prinzip“).

Weiterhin zu beachten sind Fälle mit bestimmten Datenarten, in denen das Patentrecht greift. Wenn verwendete oder erzeugte Daten von wissenschaftlichen, technischen oder methodischen Patenten geschützt sind, so sollte ein erfahrener Patentanwalt konsultiert werden, um einen Lizenzvertrags auszuarbeiten oder um Probleme, welche die Daten während deren gesamter Lebensdauer beeinträchtigen können, zu überprüfen.

## Schranken des Urheberrechts

Geschützte (Text-) Daten unterliegen einer Frist, nach der ihre Autoren und andere Rechteinhaber ihre Exklusivrechte verlieren und die Daten gemeinfrei werden (z. B. 70 Jahre nach deren Tod). Es ist möglich, dass diese Zeitspanne während des Aufbewahrungszeitraumes endet oder sich ändert.

Nach Ablauf dieser Frist unterliegen Forschungsdaten nicht mehr dem urheberrechtlichen Schutz und eine weitergehende (oder uneingeschränkte) Nutzung der Daten ist möglich. Zu beachten ist dabei, dass die gesetzlichen Fristen im Urheberrecht in und außerhalb der EU im Fluss sind.<sup>16</sup>

## Weitere Aspekte

Um rechtliche Unklarheiten beim Management von Forschungsdaten zu vermeiden, sollte man Vertrags- und Lizenzentwürfe von einem Anwalt absichern lassen. Insbesondere die z. T. sehr unterschiedlichen Datenschutz- und Urheberrechtsbestimmungen in internationalen Kontexten und die sich daraus ergebende Komplexität der Rechtsansprüche sollte nicht unterschätzt werden. Aufgrund der noch relativ neuen und sich stetig ändernden Rechtslage kann auch ein System zur regelmäßigen Rechtsberatung in Betracht

---

16 in der EU: [http://en.wikipedia.org/wiki/Copyright\\_law\\_of\\_the\\_European\\_Union#Duration\\_of\\_protection](http://en.wikipedia.org/wiki/Copyright_law_of_the_European_Union#Duration_of_protection); in anderen Ländern: [http://en.wikipedia.org/wiki/ List\\_of\\_countries'\\_copyright\\_length](http://en.wikipedia.org/wiki/ List_of_countries'_copyright_length)

gezogen werden, um festzustellen, wie sich zukünftige Gesetzesänderungen auf die vorhandenen oder geplanten Datenarchive auswirken.

## Weiterführende Literatur

- de Cock Buning, Madeleine / van Dinther, Barbara / Jeppersen de Boer, Christina G. & Ringnald, Allard (2011): Report on the Legal Status of Research Data in the Knowledge Exchange partner countries. Centre for Intellectual Property Law (CIER), The Netherlands ([de Cock Buning et al. 2011], <http://www.knowledge-exchange.info/Default.aspx?ID=461>).
- Spindler, Gerald & Hillegeist, Tobias (2009): *KoLaWiss Project: Arbeitspaket 4 – Recht*. Göttingen ([Spindler & Hillegeist 2009], [http://kolawiss.uni-goettingen.de/projektergebnisse/AP4\\_Report.pdf](http://kolawiss.uni-goettingen.de/projektergebnisse/AP4_Report.pdf)).

## Anwendungsfall Klimaforschung

Klimadaten unterliegen keiner gesetzlichen Archivierungspflicht. Das World Data Center for Climate (WDCC) [WDCC] bekennt sich aber zu den Regeln zur Sicherung guter wissenschaftlicher Praxis [Max-Planck-Gesellschaft 2001], aus denen sich eine Selbstverpflichtung ergibt, Primärdaten mindestens zehn Jahre lang aufzuheben. Eine Verpflichtung zur Langzeitarchivierung ergibt sich auch aus den Prinzipien [WDC Principles 2012], denen die ICSU-Welddatenzentren unterliegen. Hier ist z. B. vorgeschrieben, dass die Daten im Falle der Schließung eines Welddatenzentrums an ein anderes Welddatenzentrum weitergegeben werden müssen, außerdem garantieren die WDC-Prinzipien den (fast) kostenfreien Zugang zu den Daten für Wissenschaftler aller Länder.

Dies spiegelt sich auch in den Nutzungsbedingungen [WDCC-Nutzungsbedingungen 2010] wider: Für Forschungszwecke dürfen die Daten des WDCC frei genutzt werden; fließen sie in eine Veröffentlichung ein, muss eine entsprechende Referenzierung erfolgen. Weitergehende Vorschriften der Datenbesitzer müssen allerdings beachtet werden – so wird manchmal von Datenbesitzern die Unterzeichnung einer schriftlichen Erklärung gefordert, dass die Daten nur für Forschungszwecke genutzt werden.

## 10 Metadaten

An jedes wissenschaftliche Projekt wird die Forderung gestellt, die Erstellung und Verarbeitung von Forschungsdaten umfassend so zu dokumentieren, dass die Entstehung der Daten selbst wie auch die daran geknüpften Interpretationen jederzeit inhaltlich nachvollzogen werden können; dazu dienen typischerweise „Metadaten“.

Metadaten sind „(mehr oder weniger) strukturierte Informationen, die das Erstellen, Verwalten und Nutzen von Datensätzen dauerhaft in und zwischen den Bereichen, in denen sie erzeugt wurden, ermöglichen. [Sie] können benutzt werden, um Datensätze und die Personen, Vorgänge und Systeme, die sie erzeugen, verwalten, unterhalten und nutzen, zu identifizieren, zu beglaubigen und in einen Zusammenhang zu stellen“ (paraphrasiert nach „record-keeping metadata“ in [Wallace 2001], S. 255, zitiert nach [Day 2005], S. 8).

Metadaten können aus verschiedenen Perspektiven betrachtet werden – hier als verschiedene „Dimensionen“ beschrieben –, obwohl diese nicht ganz voneinander unabhängig sind. Trotzdem müssen alle diese Aspekte (letztlich gleichzeitig!) in Betracht gezogen werden, wenn es an den Aufbau eines effektiven und nützlichen Metadatensystems geht. Mit „Metadatensystem“ bezeichnen wir hier die Einheit aus den Begriffs- und/oder Felddefinitionen, die für das Projekt relevant sind (das „Datenmodell“), und seiner Verwaltungsinfrastruktur, z. B. einer Datenbank.

### Zweck

Die zentrale Frage vor der Einrichtung eines Metadatensystems ist die Frage nach dem Zweck: Wozu sollen die Metadaten dienen oder benutzt werden? Je nach Arbeitsbereich und Zielgruppe kann die Erstellung und Bereitstellung von Metadaten sehr unterschiedlichen Zwecken dienen, die letztlich bestimmen, wie sie aussehen und was mit ihnen geschieht. Dies kann unterschiedlich klassifiziert und strukturiert werden, hier wird die folgende Gliederung vorgeschlagen:<sup>17</sup>

---

17 Day [Day 2005] zitiert eine Auflistung von Haynes [Haynes 2004]: „Metadaten dienen der Beschreibung, dem Auffinden, der Verwaltung, der Beschreibung von Eigentum und Echtheit sowie der Interoperabilität von Daten.“

- **Datenbestand sichtbar machen:** Viele Metadaten dienen dazu, Datenbestände oder Dokumente verfügbar zu machen. Beispiele sind alle Arten von Katalogen (z. B. Bibliothekskataloge), aber auch Zeitschriften oder Repositories können ihren Inhalt per Metadaten strukturiert anbieten. Typischerweise werden hier Informationen bereitgestellt, die potenziellen NutzerInnen Rückschlüsse auf den Inhalt der beschriebenen Ressourcen ermöglichen.
- **Daten interpretierbar machen:** Oft können Daten nur verstanden werden, wenn die Rahmenbedingungen ihrer Erhebung (Ort, Zeit, Messinstrumente etc.) einerseits und die Bedeutung der Daten (Kategoriensystem, Skalierung etc.) berücksichtigt werden.
- **Daten austauschen:** Metadaten können dem Austausch von Daten zwischen mehr oder weniger eng miteinander assoziierten Partnern dienen, z. B. um einen gemeinsamen virtuellen Korpus zu erzeugen, Daten an bestimmten Punkten zu aggregieren oder zu synchronisieren oder die für den Austausch nötigen Informationen bereitzustellen (z. B. Datumsangaben).
- **Verwaltung und Pflege:** Von zentraler Bedeutung sind stabile Kennzeichen der Daten zu ihrer Identifikation, außerdem Informationen über Zugriffsrechte, etwaige Formataktualisierungen und die (Sicherung der) Echtheit von Daten.
- **Präsentation:** Um Daten (effektiv) zu nutzen, sind oft zusätzliche Informationen nötig, z. B. um Objekte (Bilder, Seiten) zur Darstellung zusammenzuführen, sie mit anderen Informationen zu verknüpfen oder die Darstellung an die NutzerInnen anzupassen (z. B. Sprache).

## Arten der Information

Aus dem Zweck der Metadaten ergibt sich weitgehend, welche *Arten* von Informationen erhoben und verwaltet werden müssen. „Klassisch“ ist die Einteilung in deskriptive, administrative und strukturelle Metadaten, wie sie auch im METS<sup>18</sup> repräsentiert wird.

Auch hier ist das Projektziel von entscheidender Bedeutung. Z. B. spielt in der Dokumentation wissenschaftlicher Forschung die Provenienz von Daten eine große Rolle, da sie nachvollziehbar macht, wie Daten erhoben

---

<sup>18</sup> „Metadata Exchange and Transmission Standard“, siehe <http://www.loc.gov/standards/mets/>

und verarbeitet wurden – und so die Überprüfbarkeit der Forschungsergebnisse gewährleisten soll. In anderen Zusammenhängen wird der Kontext der Daten und Dokumente betont, der insbesondere bei Archiven eine zentrale Rolle spielt.

Unabhängig vom jeweiligen Projekt erscheinen die folgenden Informationen von allgemeiner Bedeutung:

- **Objekte:** Metadaten zur Beschreibung und Identifikation der Objekte, die im Arbeitsprozess entstehen bzw. be- oder verarbeitet werden, sollten vorhanden sein. Ohne eindeutige und dauerhafte Identifikation der beschriebenen Objekte sind alle weiteren Informationen nur noch schwer zuzuordnen und zu nutzen.
- **Akteure:** Als Akteure können Personen, Gruppen und/oder Organisationen, die an der Entstehung und Bearbeitung von Daten beteiligt waren, betrachtet werden; aber auch technische Systeme können als Akteure gefasst werden, wenn sie Aktionen anstoßen oder durchführen. Dies ist vor allem für Abrechnungs- und Sicherheitsanforderungen von Bedeutung.
- **Quellen:** Dokumentation des Entstehungskontexts von Daten, von Ort, Zeit und Umständen, unter denen sie erhoben wurden, und dazu, welche Akteure (Personen oder technische Systeme) daran beteiligt waren.
- **Vorgänge:** Auch eine Dokumentation der Bearbeitungsschritte, denen die Daten unterworfen wurden, von welchen Akteuren welche Aktionen angestoßen wurden, welche Programme und Systeme dabei eingesetzt wurden, und welcher zeitliche Verlauf sich dabei ergab, kann sinnvoll sein.
- **Ergebnisse:** Die Ergebnisdaten, die für die direkte Nutzung vorgesehen und daher von primärer Relevanz für die Nachnutzung sind, müssen durch Metadaten auffindbar gemacht und eventuell für die Präsentation angereichert werden.

Je nach Projekt und geforderter Vollständigkeit kann das Erheben und Verwalten dieser Daten einen nicht unerheblichen Aufwand erfordern – der Umfang der Daten kann durchaus die Masse der Primärdaten erreichen oder überschreiten. Wo irgend möglich, sollten sie automatisch erhoben und gespeichert werden; wenn darüber hinaus menschliche Intervention nötig ist, so muss die korrekte und vollständige Erhebung gesichert werden. In jedem Fall muss eine sorgfältige Abwägung (unter Berücksichtigung der notwendig zu erfüllenden Ansprüche) zwischen dem erwarteten Nutzen und dem dafür notwendigen Aufwand an Ressourcen stattfinden.

## Semantik

Um Metadaten „verstehen“ zu können, muss man die Bedeutung der verwendeten Terme kennen. Ein simples Beispiel ist die Frage, ob unter „Titel“ eine Überschrift oder ein Namenszusatz zu verstehen ist. In historisch gewachsenen Bereichen wie den Bibliothekswissenschaften oder dem Archivwesen haben sich komplexe Begriffssysteme herausgebildet, die den dortigen speziellen Anforderungen entsprechen, z. B. MARC<sup>19</sup> oder ISO 15489 für die Schriftgutverwaltung; ebenso für einige fachspezifische Informationsfelder, z. B. die INSPIRE-Richtlinien zur Geo-Information<sup>20</sup>. Diese sind aber oft nicht einfach auf neuere (digitale) oder andere Objekte übertragbar. Im Gegenzug hat sich mit dem „Dublin Core Metadata Element Set“ (DCMES) [DCMES 2012] ein Minimalstandard etabliert, der mit 15 Elementen eine elementare und mit den 55 „DCMI Metadata Terms“ [DCTerms 2012] eine erweiterte Beschreibung ermöglicht.<sup>21</sup> Es zeigt sich darüber hinaus, dass spezielle Wissensbereiche vor allem zur inhaltlichen Beschreibung zusätzlicher Klassifikationen oder Ontologien bedürfen, die entweder einer Allgemeinklassifikation (z. B. der „Dewey Decimal Classification“ [Dewey Decimal Classification o.J.]) oder einer fachlichen Spezialklassifikation (z. B. der „Mathematical Subject Classification“ [MSC 2010]) entnommen sind.

Insbesondere für Datenaustausch und -zusammenführung können die unterschiedlichen benutzten Begriffs- und Klassifikationssysteme fast unüberwindliche Hindernisse bilden, sodass oft das Zurückfallen auf einen Minimalstandard wie das DCMES die einzige Möglichkeit bildet, eine zumindest minimale Interoperabilität zu erreichen. Daher wird das Dublin Core Model auch als „Pidgin language“ für den „digital tourist“<sup>22</sup> bezeichnet.

Neben fachspezifischen Begriffen, Formaten und Ansprüchen gibt es einen gemeinsamen Kern, der durch das DCMES abgedeckt und noch informativ genug ist, um einen elementaren Datenaustausch zu ermöglichen. Typische Elemente und ihre Zwecke sind dabei:

---

19 <http://www.loc.gov/marc/>

20 <http://inspire.jrc.ec.europa.eu/>

21 Zur Anwendung siehe <http://dublincore.org/specifications/>.

22 Siehe Glossareintrag „digital tourist“ unter <http://dublincore.org/documents/usaguide/glossary.shtml#>.

- der **Identifikator** (das Kennzeichen), der erlaubt, auf das Objekt zuzugreifen;
- eine **Bezeichnung** (Titel, Label, Etikett), damit man das Objekt bezeichnen und darüber reden kann;
- das **Datenformat** (evtl. eine Referenz auf eine Formatedatenbank), damit das Objekt präsentiert bzw. gelesen werden kann;
- **beteiligte Akteure** (Personen, Körperschaften, Programme, Prozesse), damit klar ist, wer Aktionen angestoßen hat bzw. sie verantwortet;
- **thematische Informationen** (Schlagwörter, Klassifikation, Ontologie), damit potenzielle NutzerInnen die Relevanz für sich beurteilen können.

Über diesen Kern hinaus wird es vielfältige verschiedene Zusatzinformationen geben, die jenseits des gegebenen Faches oder Kontextes aber nicht genutzt oder interpretiert werden können.<sup>23</sup>

## Syntax

Metadaten werden typischerweise innerhalb eines Datei- oder Datenbanksystems gespeichert und verwaltet. Dazu wird ein Datenmodell benötigt, das reichhaltig genug ist, um alle gewünschten Informationen aufzunehmen. Dies wird von den einzelnen Projekten auf mehr oder weniger individuelle Weise gelöst und ist für sich genommen unproblematisch. Wichtig ist aber die Frage, wie der Austausch von Daten ermöglicht wird; dazu muss natürlich zunächst die oben erwähnte Semantik der Partner zueinander passen. Der *Inhalt* von Datensätzen kann auf verschiedene Weise „verpackt“ werden, z. B. regelt ISO 19139 eine XML-Verpackung der Geoinformation nach ISO 19115 oder MARC XML ein „framework for working with MARC data in a XML environment“ [MARC-XML 2008]. Das Ziel ist hierbei immer, die Daten so transportabel zu machen, dass möglichst keine Informationen verloren gehen. Gleichzeitig sollen die entstehenden Datenpakete möglichst universell und ohne großen technischen Aufwand interpretiert werden können.

Innerhalb enger Partnerschaften kann man natürlich ein beliebiges Austauschformat wählen, z. B. auch Datenbankformate (bibliografisch oder relational). Wegen möglicher technischer Komplikationen bei der Übertragung werden aber üblicherweise textbasierte Formate bevorzugt, welche die Daten

---

<sup>23</sup> Vgl. dazu auch das Schalenmodell in [Krause 1996], das auf einer elementarerer Ebene die Qualitäten von Metadaten differenziert.

mehr (z. B. XML) oder weniger (z. B. CSV) strukturiert bereitstellen. Darüber hinaus gibt es mit RDF die Möglichkeit, komplexere Sachverhalte zu beschreiben. In Kurzform lassen sich die genannten Formate grob wie folgt zusammenfassen.<sup>24</sup>

- interne (Datenbank-) Formate: effektiv, aber auf engen Nutzerkreis beschränkt,
- CSV: einfaches Textformat, eher für einfache Strukturen geeignet, recht kompakt,
- XML: vielfältige Möglichkeiten, auch komplexe Strukturen abzubilden, relativ großer Überhang an Text,
- RDF: Möglichkeit, komplexe Zusammenhänge abzubilden, Standard für „Semantic Web“,
- Graphen: stärker visuell orientiert, noch wenig eingesetzt.

## Weiterführende Literatur

- Baca, Murtha (Ed.) (2008): *Introduction to Metadata Version 3.0*, Getty Publications, Los Angeles ([Baca 2008], digitale Ausgabe: [http://www.getty.edu/research/publications/electronic\\_publications/intro\\_metadata/](http://www.getty.edu/research/publications/electronic_publications/intro_metadata/)).
- Day, M. (2005): Digital Curation Manual: Instalment on “Metadata” ([Day 2005], <http://www.dcc.ac.uk/sites/default/files/documents/resource/curation-manual/chapters/metadata/metadata.pdf>).
- Powell, A. & Johnston, P. (2011): Metadata Guidelines for the Resource Discovery Taskforce ([Powell & Johnston 2011], <http://rdtfimetadata.jiscpress.org/>).
- PREMIS (Preservation Metadata: Implementation Strategies) Editorial Committee (2011): PREMIS Data Dictionary for Preservation Metadata, version 2.1 ([Committee 2011], <http://www.loc.gov/standards/premis/v2/premis-2-1.pdf>).

---

<sup>24</sup> Mehr zur Präsentation von RDF findet sich z.B. zu JSON unter <http://www.json.org/>, zu Turtle unter <http://www.w3.org/TeamSubmission/turtle/>, zu Graphen in [http://portal.acm.org/ft\\_gateway.cfm?id=1060835&type=pdf](http://portal.acm.org/ft_gateway.cfm?id=1060835&type=pdf).

## Anwendungsfall Klimaforschung

Für Metadaten gibt es im World Data Center for Climate (WDCC) [WDCC] Regeln, die im CERA-2-Datenmodell [CERA2-Datenmodell 2008] zusammengefasst sind. Das CERA-2-Datenmodell ist konform mit dem internationalen Metadaten-Standard ISO 19115/19139.

Das WDCC enthält drei verschiedene Datenarten, von denen zwei unterschiedliche Kategorien deskriptiver Metadaten sind:

1. Metadaten des Experimentes (Zusammenfassung von Datensätzen): Hier finden sich alle Metadaten zum Experiment, z. B. Titel und Autoren.
2. Metadaten der einzelnen Datensätze
3. Datensätze selbst

Von großer Bedeutung sind die Standardnamen, die in Metadaten und Daten verwendet werden und physikalische bzw. chemische Größen benennen, z. B. „air\_temperature“. Diese erleichtern die Arbeit mit den Daten und entsprechen der in der Klimaforschung international anerkannten CF-Namensliste.<sup>25</sup>

## 11 Identifikatoren und Informationsobjekte

Identifikatoren sind ein wichtiges Querschnittsthema im Datenmanagement. Sie sind ein fundamentales Instrument, um sich auf Informationsobjekte zu beziehen. Es ist zwar möglich, sich auf Informationsobjekte durch relative Angaben und Eigenschaften zu beziehen, wie z. B. „der Datensatz, der unter Adresse X gespeichert ist“ oder „der Datensatz, der am Datum Y erzeugt wurde“. Dies wird aber schnell unpraktisch und für eine vereinfachte und robustere Verarbeitung ist es notwendig, Daten eigene und eindeutige Identifikatoren zuzuweisen.

Prinzipiell kann man alles identifizieren, seien es einzelne Dateien, eine bestimmte Menge von Dateien, die durch die Dateien repräsentierten abstrakten Inhalte, Teile von digitalen Objekten, dynamische Objekte, Funktionalitäten von Webservices, analoge Gegenstände, Personen oder beliebige andere

---

<sup>25</sup> CF steht für „Climate and Forecast“ und ist eine Konkretisierung des Standard-Datenformates NetCDF [NetCDF] für die Bedürfnisse der Klimaforschung. Die Namensliste ist ein Anhang zur CF-Konvention [NetCDF CF Metadata Convention].

Objekte. Es muss deshalb explizit definiert werden, was das Informationsobjekt ist, das ein Identifikator bezeichnen soll, und wie der Identifikator aufgelöst werden soll. Diese Entscheidung hängt von dem jeweiligen Anwendungsfall und den Nutzungsszenarien ab. Es kann Fälle geben, in denen Daten in einer bestimmten technischen Version mit immer derselben Bitfolge benötigt werden, z. B. um die Integrität automatisch zu prüfen. Ein entsprechend technisch definierter Identifikator verweist immer auf dieselbe Bitfolge. In anderen Fällen können hingegen nur die Inhalte relevant sein – unabhängig davon, ob sie durch eine CSV-, eine *Excel*-Datei oder ein anderes Dateiformat ausgedrückt werden. Ein entsprechend inhaltlich definierter Identifikator könnte dieselben Inhalte in den jeweils benötigten, unterschiedlichen Datenformaten liefern. Beide Identifikatoren können unter Umständen sogar die gleiche Datei liefern, obwohl sie unterschiedliche Informationsobjekte als identisch betrachten.

Das PILIN-Projekt hat eine Reihe von Leitfragen formuliert, um auf Basis eines Informationsmodells bei der Entscheidung zu helfen, wie Identifikatoren in einem Forschungsprojekt vergeben werden sollten [PILIN Transition Project 2008].

- **Was für Dinge existieren?** Der erste Schritt ist, sich darüber klar zu werden, welche Dinge im Forschungsbereich existieren, d. h. welche analogen oder digitalen Objekte, welche Akteure, Funktionalitäten, Relationen etc. Hierfür gibt es zum Teil domänenspezifische Standards oder Ontologien.
- **Welche Dinge basieren auf anderen?** Einige Objekte sind von anderen abgeleitet und je nach Anwendungsfall können die Ursprungsobjekte oder die resultierenden Elemente wichtiger sein. Z. B. kann es sich um Ausschnitte aus einem größeren Datensatz, inhaltlich überarbeitete Versionen oder in einem anderen Format gespeicherte Präsentations- oder Arbeitsversionen handeln.
- **Welche Dinge sind wichtig?** Manches muss mit Identifikatoren versehen werden, anderes nicht. Dinge, die außerhalb des Entstehungskontext referenziert werden sollen, wie z. B. ein publizierter Datensatz, sollten üblicherweise Identifikatoren erhalten. Hingegen müssen einzelne Teile von schon mit Identifikatoren versehenen Objekten oftmals nicht neue Identifikatoren bekommen, da sie über relative Angaben adressiert werden können, wie z. B. Zeitabschnitte in Videos oder Seiten in Dokumenten.

- **Wie werden Identifikatoren aufgelöst?** Es ist nicht von vornherein klar, was mit einem Identifikator gemacht werden kann. Häufig ist die Erwartung, dass das Objekt herunterladbar ist. Wenn aber z. B. abstrakte Objekte identifiziert werden, die in verschiedenen Formaten oder Versionen vorliegen, ist festzulegen, welches Format oder welche Version ausgeliefert wird. Unter Umständen wird auch nicht das Herunterladen angeboten, sondern es sind nur andere Funktionalitäten über den Identifikator ansprechbar, wie z. B. die Darstellung von Metadaten, Service-Operationen etc. Diese sind insbesondere bei nicht als Dateien repräsentierten Objekten wie z. B. Webservices oder analogen Objekten zu definieren.
- **Wann werden Dinge identifiziert?** Der Zeitpunkt der Identifikation muss festgelegt werden. Je nach Szenario kann es sinnvoll sein, sie gleich bei der Erzeugung, erst nach einer Qualitätskontrolle oder erst bei der Publikation zu vergeben.

Es gibt eine Reihe von Schemata für Identifikatoren für unterschiedlichste Zwecke und viele Domänen haben ihre eigenen Standards. An dieser Stelle wird nur auf die sogenannten *Persistent Identifier* eingegangen, die eine besonders dauerhafte Identifizierung ermöglichen sollen, wie sie zum Beispiel zur Zitation benötigt wird. Dies sind u. a. DOI, Handle, URN und PURL. Persistent Identifier werden generiert und in einem Verzeichnisdienst (Resolver) mit Informationen wie der Zugriffsadresse (z. B. URL) gespeichert. Die Identifikatoren selbst werden nicht mehr geändert und bei Veränderungen der Zugriffsadresse oder weiterer Informationen werden nur die Daten im Resolver aktualisiert. Dadurch, dass für einen Zugriff zuerst vom Resolver die aktuellen Zugriffsinformationen abgefragt werden, können der Identifikator konstant gehalten und für den Zugriff wechselnde Speicherorte benutzt werden. Zitate und Referenzen, die den persistenten Identifikator anstelle der URL benutzen, werden bei Veränderungen der Speicheradresse nicht ungültig.

Bei Persistent Identifiern ist es wichtig zu bedenken, dass sie nicht automatisch persistent sind. Dass die Verknüpfung zwischen dem Identifikator und dem identifizierten Informationsobjekt persistent ist, hängt von einer fortwährenden Pflege der Informationen im Resolver und des Informationsobjekts ab. Persistent Identifier sind nur ein Hilfsmittel. Auch ein mit einem DOI versehener Datensatz kann verloren gehen oder nicht mehr zugreifbar sein, weil er z. B. nur auf einem Arbeitsplatzrechner ohne professionelles

Backup gespeichert war oder es versäumte wurde, die Zugriffsadressen im Resolver nachzutragen.

## Weiterführende Literatur

- Einführungen zu Persistent Identifiern bietet der Australian National Data Service (ANDS) auf verschiedenen Niveaus an (2009):
  - Persistent Identifiers Guide Awareness Level ([Australian National Data Service 2009a], <http://ands.org.au/guides/persistent-identifiers-awareness.pdf>),
  - Persistent Identifiers Guide Working Level ([Australian National Data Service 2009b], <http://ands.org.au/guides/persistent-identifiers-working.pdf>),
  - Persistent Identifiers Guide Expert Level ([Australian National Data Service 2009c], <http://ands.org.au/guides/persistent-identifiers-expert.pdf>).
- Kunze, John A. (2003): Towards Electronic Persistence Using ARK Identifiers ([Kunze 2003], <https://confluence.ucop.edu/download/attachments/16744455/arkcdl.pdf>).
- PILIN, Information Modelling Guide for Identifiers in e-research (2008). University of Southern Queensland ([PILIN Transition Project 2008], <http://resolver.net.au/hdl/102.100.272/6R22YGTRH>).

## Anwendungsfall Klimaforschung

Das GeoForschungsZentrum Potsdam [GeoForschungsZentrum] und die drei ICSU-Welddatenzentren WDCC [WDCC], WDC-MARE [WDC-MARE] und WDC-RSAT [WDC-RSAT] bieten an, in deren Archiven vorhandene Daten mit den Persistent Identifiern DOI (Digital Object Identifier) und URN (Uniform Resource Name) zu versehen. Damit verbunden ist ein Eintrag im GetInfo-Katalog [GetInfo-Katalog], welcher der Suche in den Beständen der Technischen Informationsbibliothek, der Deutschen Zentralbibliotheken für Medizin und Wirtschaftswissenschaften sowie der Suche in weiteren Fachdatenbanken dient.<sup>26</sup> Den Eintrag im GetInfo-Katalog nimmt die Technische Informationsbibliothek (TIB) [Technische Informationsbibliothek] mit Sitz

---

26 Nach DOI bzw. URN gesucht werden kann unter <http://nbn-resolving.de/>.

in Hannover vor. Die TIB gehört zu einem weltweiten Netz von Registrierungssagenturen, die der Internationalen DOI-Foundation (IDF) [International DOI Foundation] angeschlossen sind.

Wie alle Persistent Identifier erleichtern DOI und URN die Zitierung, indem der Identifikator einfach als Referenz benutzt wird. Beispiel für ein Zitat mit URN: Zahn, M. (2010), Climate Simulation with CLM, Scenario A1B run no.1, North Atlantic region, *WDCC*, urn:nbn:de:tib-10.1594/WDCC/CLM\_A1B\_ZS9.

Der zugehörige DOI hat die folgende Gestalt: 10.1594/WDCC/CLM\_A1B\_ZS. Am WDCC wird der DOI zusammengesetzt aus

- dem Zahlencode 10., der den String als DOI kennzeichnet,
- einer vom IDF für WDCC-Daten fest vergebenen Nummer (1594),
- der Zeichenkette /WDCC und
- einem vom WDCC selbst für die spezielle Veröffentlichung vergebenen Teil.

Der URN ist mit einem Vorspann und am Ende zusätzlich mit einer Prüfziffer versehen. Das nbn im Vorspann steht für „National Bibliography Number“ (RFC 3188), ein international verwalteter Namensraum der Nationalbibliotheken [Neuroth et al. 2010].

Am WDCC ist die DOI/URN-Vergabe in einen Qualitätssicherungs-Workflow eingebunden [WDCC-Qualitätssicherung o.J.]. Der Datenproduzent ist für die wissenschaftliche Qualitätskontrolle allein und für die technische Qualitätskontrolle gemeinsam mit dem WDCC verantwortlich. Von Seiten des WDCC werden die folgenden technischen Eigenschaften überprüft:

- Die Zahl der Datensätze ist korrekt und nicht 0.
- Die Größe eines jeden Datensatzes ist nicht 0.
- Die zu den Datensätzen gehörigen Metadaten sind vorhanden und zugreifbar.
- Der Gesamtumfang der Daten ist korrekt.
- Die in den Metadaten angegebenen Zeiten (Start- und Stoppdatum, Zeitschritt) sind mit den Daten konsistent. Im Falle von Beobachtungsdaten können einzelne Zeitstempel jedoch fehlen, wenn zu den betreffenden Zeiten nicht gemessen werden konnte.
- Das Datenformat ist valide.
- Variablenbeschreibungen und Daten sind konsistent.

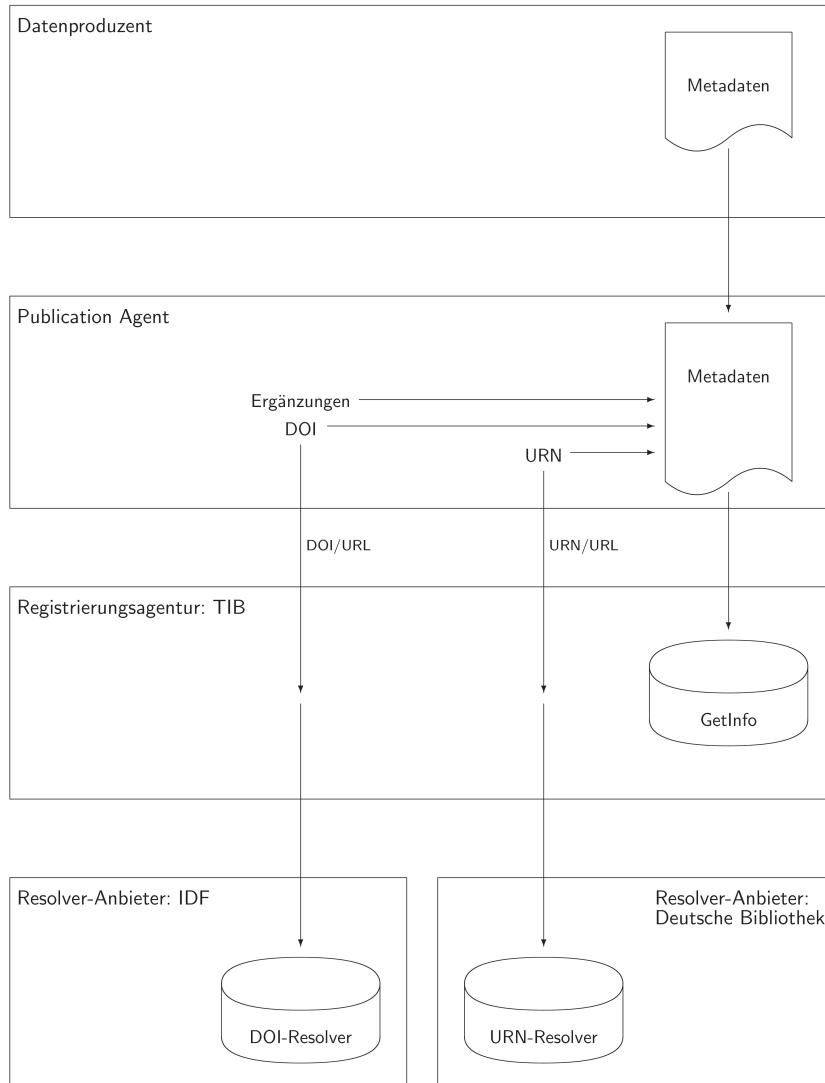


Abb. 7 Workflow zur DOI- und URN-Vergabe  
(Qualitätssicherung nicht mit dargestellt)

Der Workflow für die eigentliche Publikation ist in Abb. 7 dargestellt. Der Datenproduzent liefert Metadaten wie `Creator` und `Title`, die dann vom

Publication Agent durch weitere Metadaten ergänzt werden. Zu den Ergänzungen gehört der Publisher (WDCC) und der DOI und URN selbst.

Die in XML überführten Metadaten<sup>27</sup> werden an die TIB geschickt und dort in den GetInfo-Bibliothekskatalog [GetInfo-Katalog] integriert. DOI/URN und die zugehörige URL werden von der TIB an die Resolver-Anbieter weitergeleitet, welche diese in ihre Resolver aufnehmen.

Nach der DOI-Vergabe dürfen die Daten und diejenigen Metadaten, die Teil des Zitates sind, nicht mehr verändert werden. Im Gegensatz dazu kann die zugehörige URL aber jederzeit durch eine neue ersetzt werden. Dies muss sogar geschehen, wenn sich die Webadresse geändert hat und die alte URL nicht mehr länger besteht.

---

27 Die erforderlichen und optionalen Metadaten sind in [DataCite-Metadatenschema 2011] aufgeführt und erfüllen den Standard ISO 690-2 für bibliografische Referenzen. Die Metadaten können auf Dublin Core [DCMI] abgebildet werden, sowohl auf das Simple Dublin Core Metadata Element Set [DCMES] als auch auf Qualified Dublin Core.



# Anhang: Urheberrecht

## Einführung

Mit der zunehmenden Verbreitung digitaler Medien ergeben sich umfangreiche neue Möglichkeiten der Verbreitung und Nutzung von Informationen kultureller Äußerungen aller Art. Datenspeicherung geht immer mit rechtlichen Fragestellungen einher. So hat der Gesetzgeber für den Abruf von gespeicherten Daten zwar bereits einige Maßnahmen getroffen (§ 52b UrhG für elektronische Leseplätze und § 137I UrhG für neue Nutzungsarten und retrospektive Digitalisierung). Doch bleiben einige Grauzonen im Bereich langfristiger Datenhaltung bislang ungeklärt.

Um aber auch in Zukunft ihrem gesetzlichen Auftrag nachkommen zu können, sind Gedächtnisorganisationen bei der Sammlung und Erhaltung digital aufgezeichneter kultureller Äußerungen in immer stärkerem Maße auf Langzeitarchivierungsstrategien angewiesen. Um digitale Daten über lange Zeiträume für eine Nutzung zu erschließen und persistent lesbar zu erhalten, bedarf es jedoch neben dem üblichen Vorgang des Datensammelns auch verschiedener Maßnahmen der Datenbearbeitung. Hierbei werden Archive, Museen und Bibliotheken jedoch vor einige juristische Schwierigkeiten gestellt, sobald sie in der Erfüllung ihres Auftrags mit dem Urheberrecht konfrontiert werden. Vom Blickwinkel des Urheberrechtsgesetzes (UrhG) aus gesehen unterscheidet sich die Haltung digitaler Daten signifikant von analogen Daten wie dem klassischen Buch – stellt doch jede elektronische Aktivierung wie Download, Ausdruck etc. im Gegensatz zum bloßen Aufschlagen eines Buches bereits ein Akt der Vervielfältigung dar.

Im Gegensatz zu klassischen Verfahren der Buchrestauration erfolgt die Erhaltung digitaler Daten im Rahmen der üblichen Sicherungsstrategien ausschließlich über die Herstellung von Kopien (Backups), die als Eingriff in die urheberrechtlich geschützte Integrität des Datensatzes interpretiert werden kann und der Zustimmung des Rechtehalters (Urhebers) bedarf. Es stellt sich demnach die Frage, inwiefern die geltenden Bestimmungen auf den Umgang mit digitalen Daten angewandt werden können.

## Rechtliche Situation

Grundsätzlich generiert das UrhG keinen Automatismus, der sämtliche existierenden Daten unter Schutz stellt sowie Zugriff und Verbreitung reglementiert. Vielmehr bedarf es ggf. der Einzelfallprüfung, ob betroffene Datensätze durch ihre Schöpfungshöhe einen geistigen Wert darstellen, der gesetzlichen Schutz genießen kann. So stellt eine Ansammlung gänzlich ungeordneter wissenschaftlicher Rohdaten (z. B. Klimamessdaten) nicht zwangsläufig ein schutzwürdiges Werk sui generis dar. Desgleichen greift der urheberrechtliche Schutz nicht bei gemeinfreien Werken wie amtlichen Bekanntmachungen (§ 5 UrhG) oder Texten, deren Schutzfrist abgelaufen ist – üblicherweise ist dies 70 Jahre nach dem Tod des Urhebers der Fall.

Allerdings bewegt sich jede Gedächtnisorganisation im Umgang mit verwaisten Werken („orphan works“) bereits in einer rechtlichen Grauzone: Wie sind Werke zu bewerten, die nicht mehr aufgelegt oder vergriffen sind und deren urheberrechtliche Situation somit nicht mehr zu ermitteln ist? Unterliegen bestimmte Werke aber dem bisher geltenden Urheberrecht, werfen sich sogleich Fragen des Bestandsaufbaus, der Datensicherung, Datenbearbeitung und Haftung auf.

## Bestandsaufbau und Datensammlung

Zur Erweiterung ihres Bestandes sammeln Archive und Bibliotheken Daten, um sie Nutzern zugänglich zu machen. Bei der Aufnahme und Erschließung neuer Werke im Bestand ist die Rechtslage eindeutig: Eine Erschließung ohne vorherige Einwilligung ist ausgeschlossen. Da die Zahl der im Internet frei zugänglichen Daten – insbesondere im Bereich wissenschaftlicher Publikationen – in den letzten Jahren stark zugenommen hat, werden Gedächtnisorganisationen zusehends auch auf diese Bestände zugreifen müssen, um ein möglichst breites Spektrum anbieten zu können. Ein gängiges Verfahren zur Datengewinnung stellt hierbei das Web-Harvesting dar.

Auch im Zeitalter digitaler Netzwerke und des Web Publishing bedeutet die Publikation im Internet noch keinen Blankscheck für eine ungehinderte Weiterverbreitung oder Vervielfältigung der frei zugänglichen Inhalte. Dies wird vor allem dann relevant, wenn, wie oft zu beobachten, Anbieter der Daten und Urheber nicht identisch sind. Automatisierte Abfragen von Web-Inhalten stoßen an Ausschließlichkeitsrechte von Urhebern, die auch nicht

durch Schrankenregelungen des Urheberrechts (§ 53 Abs. 2 UrhG, s. u.) gedeckt sind.

Daher unterliegen Internetpublikationen sehr häufig speziellen Lizenzvereinbarungen wie GNU, GPL oder Creative Commons, die nicht nur das Verhältnis zwischen Anbieter und Urheber regeln, sondern auch eindeutige Passagen zu ihrer Vervielfältigung enthalten. Diese Verträge haben in der Regel Vorrang vor anderen urheberrechtlichen Bestimmungen. Anders als in den Vereinigten Staaten, wo die Auswertung von Internetangeboten bereits als rechtmäßig gilt, wenn der Urheber eine Nachnutzung nicht ausgeschlossen hat oder ihr nachträglich widerspricht, bedarf nach deutschen Recht eine Auswertung digital publizierter Daten oder eine Vervielfältigung durch Harvesting gewonnener Daten grundsätzlich immer der Zustimmung des Urhebers. Seltene Ausnahmen können sich bisweilen für bestimmte Gedächtnisinstitutionen wie Pflichtexemplarbibliotheken (Deutsche Nationalbibliothek oder Bundesarchiv) ergeben, die der Spezialrechtsprechung des Bundes-/Landespflichtexemplar- und Archivrechts unterliegen.

Ebenfalls unproblematisch nimmt sich die Übernahme gemeinfreier Daten aus, die digitalen Quellen entnommen wurden. Dennoch ergibt sich hier das Dilemma, dass es selbst Pflichtexemplarbibliotheken nicht gestattet ist, jenseits ihres gesetzlichen Auftrages selbstständig zu sammeln und beispielsweise verwaiste Werke in ihren Bestand aufzunehmen. Auch die vom Gesetzgeber angestrebten Änderungen (aktueller Gesetzentwurf zum UrhWahrnG für die Nutzung verwaister und vergriffener Werke siehe: BTDS 17/3991 vom 30.11.2010) betreffen lediglich entsprechend der Archivschranke des § 53 Abs. 2 UrhG verwaiste Werke, die sich bereits im Bestand des Archivs befinden. Frei verfügbare, etwa im Internet publizierte Daten, deren urheberrechtliche Situation unklar ist, können so nicht erfasst werden. Den Archiven fehlen somit treffsichere Schrankenregelungen, die eine Erfüllung ihres gesetzlichen Sammlungsauftrages gewährleisten.

## **Bestandserhaltung und Kopien**

Vergleichsweise komplexer ist die Situation bei der Handhabung bereits im Archiv befindlicher Bestände. Zur Erhaltung des Bestandes an digitalen Daten einer Gedächtnisorganisation ist die regelmäßige Anfertigung von Kopien unabdingbar, will man nicht Gefahr laufen, die Daten aufgrund eines veralteten, nicht mehr lesbaren Dateiformats unwiederbringlich zu verlieren.

Prinzipiell liegt die Entscheidung über die Vervielfältigung von geschützten Werken stets bei deren Urheber.

Urheberrechtlich vergleichsweise unproblematisch gestaltet sich die Anfertigung von Archivkopien – Vervielfältigungen also, die an ohnehin bereits im Bestand einer Gedächtnisorganisation befindlichen Primärwerken zum Zwecke der Bestandswahrung vorgenommen werden: Die Archivschanke des § 53 Abs. 2 Satz 1 UrhG erlaubt die Übernahme von bereits vorhandenen Archivkopien (analog/digital) in eben dasselbe Archiv zum Zweck der Sicherung oder der internen Nutzung, sofern sie nicht zur Erweiterung des eigenen Bestandes vorgenommen wurde. Grundvoraussetzung ist das Vorhandensein einer originalen und rechtmäßig erworbenen Vorlage eines eigenen Werkstücks im Besitz des Archivs. Einschränkend gilt diese Regelung jedoch nur für Archive, deren Tätigkeit in öffentlichen Interesse liegt.

Für den Umgang mit digitalen Daten im Archiv kennt das Gesetz indes einige Spezialfälle, die das Anfertigen von Kopien im Einzelfall regeln. So unterliegen Datenbankwerke nach § 87a Abs. 1 UrhG oder Computerprogramme (§ 69d UrhG; Ausnahme: Fehlerbeseitigung, Sicherungskopie des Besitzers) strengen Restriktionen und dürfen grundsätzlich nicht kopiert werden (§ 53, Abs. 5 UrhG). Hierunter fallen somit auch komplexe Webseiten sowie systemisierte oder elektronisch erschlossene Datensammlungen. Besteht weiterhin ein technischer Kopierschutz an einem digitale Daten bewahrenden Speichermedium (CD-ROM etc.), so darf dieser keinesfalls überwunden oder umgangen werden (§ 95a UrhG). Allerdings ist der Urheber des so gesicherten Materials gesetzlich verpflichtet, einem Archiv, dem er die Anfertigung einer Archivkopie zur Vermehrung des Bestandes eingeräumt hat, die Mittel zur Beseitigung an die Hand zu geben (§95b UrhG).

Bei der Sicherung digitaler Daten ist es – ganz ähnlich dem natürlichen Verschleiß von Bucheinbänden – grundsätzlich unvermeidbar, dass Speichermedien und -formate dem technischen Verfall unterliegen und mit der Zeit veralten. Eine überzeugende LZA-Strategie schließt daher notwendigerweise auch Eingriffe in die technische Integrität der digitalen Bestände ein, um eine nachhaltige Lesbarkeit des Datenmaterials zu gewährleisten. Gängige Verfahren hierzu wie Emulation, Migration und Konversion stellen stets Interpretationsprozesse unlesbarer Datensätze dar, wobei der informationshaltige Kernbestand der Daten weitgehend unberührt bleiben sollte.

Digitale Datenträger unterscheiden sich aber von analogen Speichermitteln in ihrer deutlich kürzeren Haltbarkeit. Technische Eingriffe in digitale Datenspeicher fallen demnach u.U. wesentlich früher an als die Restaurierung

eines Buches. Juristisch ist dies insofern von Belang, als Eingriffe in den inhaltlichen Bestand eines Datensatzes einer urheberrechtlichen Schutzfrist unterliegen. Da diese erst 70 Jahre nach dem Tode des Urhebers verstreckt, die meisten technischen Eingriffe in Speichermedien aber deutlich früher anstehen, ist es unabdingbar die nach wie vor umstrittene Frage eindeutig zu regeln, ob in einem solchen Verfahren juristisch eine Veränderung im Sinne von § 23 UrhG zu sehen ist oder eine bloße Vervielfältigung nach § 16 UrhG vorliegt.

Verfechter der Hypothese, eine Migration stelle einen Akt der Vervielfältigung dar, führen das Argument ins Feld, dass derartige Maßnahmen zwar den technischen Träger von Daten manipulieren, als solche aber als rein mechanischer Akt zu verstehen wären und die dem eigentlichen Schaffensprozess des Urhebers entspringenden Daten davon nicht betroffen seien. Als Vergleich wird der Austausch eines Bucheinbandes zu Restaurationszwecken herangezogen, der die äußere Hülle der Schrift intakt lässt und die den Informationsgehalt tragenden Seiten weder in Zahl, Reihenfolge noch Aussagekraft manipuliert.

Trifft dies zu, bleiben Verfahren wie Migration und Emulation – sofern § 53 Abs. 2 UrhG eintritt, der die Parameter für die Anfertigung einer Archivkopie definiert – durch das Urheberrecht abgedeckt. Folgt man dieser Sichtweise, bedürfen lediglich Eingriffe in den originalen Informationsbestand der Daten des Einverständnisses ihres jeweiligen Urhebers. Weiterhin ungeklärt bleibt selbst bei dieser Interpretation der Sachverhalt bei ausgesprochen sensiblen Daten, wie etwa dem Aktenbestand medizinischer Archive über die Behandlung von Patienten.

Kritiker dieser Sichtweise halten die Schrankenregelung des UrhG für digitale Daten für gänzlich unzureichend. Demnach reichen Änderungen an der digitale Daten erschließende Software über eine bloße Restauration des rasch veraltenden Datenträgers hinaus – stellen doch Anpassungen am Format des Informationsgehalts bereits einen hinreichenden Eingriff in die Integrität des Datensatzes dar. Fallen solche Maßnahmen fernerhin noch in die bereits angesprochene Schutzfrist des UrhG, wären sie demzufolge durch die bereits existierende Archivschranke nicht gedeckt, wodurch sich zumindest eine zweideutige Rechtslage ergibt.

Zusammenfassend lässt sich feststellen, dass sich insbesondere Forschungsinstitutionen angesichts dieser ungeklärten Rechtslage zusehends mit einem Kostenaufwand für Lizenzien urheberrechtlich geschützter Forschungsdaten konfrontiert sehen, die zum Zwecke der Verifizierbarkeit, Re-

plizierbarkeit und Nachnutzung wissenschaftlicher Arbeit gehalten werden. Dass das UrhG ausschließlich natürliche Personen als Urheber ausweist, kommt für juristische Personen wie Forschungsinstitutionen erschwerend hinzu. Folglich können urheberrechtliche Ansprüche von institutionalisierten wie nicht-institutionalisierten Forschungsverbünden und -einrichtungen auf unter ihrer Ägide entstandene Daten nicht geltend gemacht werden und müssen ggf. durch den verantwortlichen Einzelwissenschaftler nachträglich eingeraumt werden.

## **Zugriffsrechte**

Rein urheberrechtlich gesehen definiert § 53 Abs. 2 UrhG Archive als Gedächtnisorganisationen, denen als zentrale Aufgabe das Sammeln, Bewahren und Sichern ihrer Bestände obliegt. Da die Erschließung von Beständen für Nutzer als wesentlicher Teil im Selbstverständnis der meisten Archive liegt, sind sie von den Privilegierungen des Urheberrechts streng genommen ausgeschlossen, was eine nachhaltige LZA verunmöglicht, sobald sie die Einsichtnahme in den gespeicherten Datenbestand umfasst. Zu den bisher vorgesehenen drei Nutzungsvarianten zählen daher ausschließlich die interne, die eingeschränkte und die offene Nutzung.

Die interne Nutzung sieht lediglich den Zugriff auf Daten durch Mitarbeiter der Gedächtnisorganisation vor, die zu Archivzwecken (Metadatenanreicherung, Katalogisierung, Sicherung etc.) Einsicht in die jeweiligen Inhalte nehmen müssen. Sobald aber, wie im Falle digitaler Daten oft notwendig, der Zugriff mittels Download oder Computerausdruck erfolgt, muss das Archiv gewährleisten, dass die Einsichtnahme nur zu wissenschaftlichen Zwecken geschieht (§ 53 Abs. 2 S. 1 Nr. 1 UrhG).

Um die zuvor angesprochene Problematik der fehlenden Regelungen zur Einsichtnahme in digitale Daten zu kompensieren, hat der Gesetzgeber mit § 52b UrhG eine Möglichkeit geschaffen, digitale Inhalte in eingeschränkter Nutzung über öffentliche Bildschirmleseplätze einzusehen, die sich in den Räumlichkeiten des Archivs befinden. Gedeckt wird auch die Darstellung von Digitalisaten zuvor analog gespeicherter Medien. Obgleich diese Regelung eine deutliche Erleichterung für Gedächtnisorganisationen darstellt, greift diese Privilegierung auch in diesem Falle nur für Archive, wenn ihre Sammelaktivitäten in öffentlichem Interesse liegen. Schul- oder universitäre

Institutsbibliotheken sowie kommerzielle Archive bleiben von dieser Verbeserung ausgeschlossen.

Erfolgt die Zugriffnahme an den öffentlich zugängigen Stellen wiederum über Download oder Ausdruck, muss auch hier das Kriterium der Nutzung zu wissenschaftlichen Zwecken nachweislich erfüllt sein. Sollten aber bestimmte Umstände dazu führen, dass § 53b UrhG nicht greift, kann eine Gedächtnisorganisation ihre Bestände ausschließlich auszugsweise für einen relevanten und eng begrenzten Personenkreis erschließen, welcher die Einsichtnahme zu wissenschaftlichen Zwecken vornimmt (§ 52a UrhG).

Die offene Nutzung digitaler Daten hängt hingegen gänzlich von der Zustimmung des Urhebers ab: Solange ein Urheber die von ihm geschaffenen Daten nicht freigibt, dürfen sie von keiner Gedächtnisorganisation ortsungebunden publiziert werden.

## **Haftung**

Neben rein urheberrechtlichen Fragestellungen unterliegt die langfristige Speicherung digitaler Daten weiteren juristischen Kriterien. So ist von jeder Gedächtnisorganisation darauf zu achten, dass keine Daten mit volksverhetzenden, pornografischen, ehrverletzenden oder gegen Bestimmungen des Patentrechts verstörenden Inhalten gespeichert werden. Die §§ 7–10 des Telemediengesetzes (TMG) unterscheiden in Fragen der Haftung von Archiven zwischen eigenen und fremden Inhalten. Für die Zuweisung zu der einen oder anderen Kategorie ist die Nutzersicht ausschlaggebend: Sollte ein Nutzer bei der Einsicht in einen Datensatz auf rechtswidrige Inhalte stoßen und diese urheberrechtlich eindeutig als Eigentum der jeweiligen Gedächtnisorganisation erkennen (Archivzeitschriften, Kataloge etc.), werden die fraglichen Daten als dem Archiv eigen klassifiziert. Dies hat zur Folge, dass das Archiv für evtl. resultierende Rechtsverletzungen haftbar gemacht werden kann.

Um in solchen Fällen eine eindeutige Rechtslage herzustellen, ist es jeder Gedächtnisorganisation angeraten, eigene Inhalte deutlich als solche auszuweisen und einen Haftungsausschluss für Daten aus externen Quellen zu formulieren. Sollten dennoch gesetzeswidrige Inhalte in Archiven entdeckt werden, unterliegt jede Gedächtnisorganisation einer Sorgfaltspflicht (§ 7 Abs. 2 TMG), die ihr eine Sperrung von Daten evident rechtswidrigen Inhalts auferlegt. Hierbei genügt es – ohne eine endgültige Löschung vorzunehmen –,

die Nutzung und Zugänglichkeit solcher Daten zu verwehren, um einem Haftungsanspruch zu entgehen.

## **Fazit**

Angesichts der beschriebenen Komplexität der juristischen Situation sind Gedächtnisorganisationen mit dem aktuellen juristischen Handwerkszeug zwar imstande, ihrem Auftrag zur Sammlung analoger Daten nachzukommen, sehen sich jedoch kaum in der Lage, eine rechtlich abgesicherte LZA-Strategie für digitale Daten zu verfolgen. Zur Klärung der Situation warten sie vielmehr auf einen Satz an griffigen Schrankenbestimmungen, welche die digitale Langzeitarchivierung jenseits vervielfältigender Maßnahmen zur Bestandserhaltung um Möglichkeiten der Bearbeitung und Umgestaltung von Dateiformaten und des Bestandsaufbaus ergänzen (Web Harvesting). Es bleibt festzuhalten, dass das Ausbleiben solcher Instrumente, die neben den bisher privilegierten Pflichtexemplarbibliotheken dem ganzen Spektrum an öffentlichen Gedächtnisorganisationen zugute kommen, eine umfassende und zuverlässige Dokumentation digital fixierter kultureller Äußerungen auf absehbare Zeit verhindern könnte.

# Checkliste zum Forschungsdaten-Management



# **Vorwort: Anleitung zur Benutzung der Checkliste**

Um digitale Forschungsdaten langfristig nutzen zu können und den Anforderungen an die gute wissenschaftliche Praxis gerecht zu werden, ist es notwendig, eine Reihe von Vorkehrungen und Maßnahmen zu treffen. Ohne ausreichende Dokumentation und Metadaten können Forschungsdaten nicht verstanden und verwaltet werden, ohne Finanzierung und Personal können sie nicht aufbewahrt und gepflegt werden und ohne definierte Arbeitsabläufe für das Datenmanagement können nur geringe Datenmengen mit unklarer Qualität gesichert werden. Das sind nur wenige Beispiele der Aufgaben, die idealerweise schon bei der Planung eines Forschungsvorhabens berücksichtigt werden sollten.

Diese Checkliste soll Vorhaben helfen, zusammen mit Infrastruktureinrichtungen wie Rechenzentren oder Datenarchiven den Umgang mit Forschungsdaten zu planen, wie es z. B. in DFG-Anträgen gefordert ist. Einführungen in die einzelnen Themengebiete und weiterführende Literaturhinweise finden sich in dem Leitfaden des WissGrid-Projekts zur Langzeitarchivierung von Forschungsdaten (S. 11–82). Einen Überblick der Aufgaben des Forschungsdatenmanagements geben die Abbildungen 1 (S. 93) sowie 2 (S. 99).



# Teil I: Aufgaben im Lebenszyklus von Forschungsdaten



Abb. 1 Der Lebenszyklus von Forschungsdaten

## 1 Planung und Erstellung

### 1.1 Allgemeine Angaben zu den Rahmendaten des Vorhabens

- Wie lautet der Name/die Bezeichnung des Forschungsvorhabens?
- Was sind die Ziele des Projekts?
- Wer sind der/die Projektträger oder Finanzgeber?
- Was ist die angestrebte/genehmigte Laufzeit des Projekts?
- Welche Organisationen sind an dem Forschungsvorhaben beteiligt (Projektpartner)?
- Welche Organisation oder Person fungiert als Projektverantwortlicher/Leiter/Koordinator?

## 1.2 Vorhandene Daten

1. Können bereits existierende Datensätze benutzt werden? Wurde nach Datenbeständen im Besitz der eigenen Institution und von Dritten recherchiert?
2. Welche Bedeutung haben die vorhandenen sowie die erzeugten Daten für das Vorhabensziel? Wieso sind die Daten wichtig? (*z. B. Dokumentation, Publikation, Nachnutzung, ...*)
3. Wie wird die Integration zwischen den bereits bestehenden und den neuen Daten organisiert? Wie wird z. B. Herkunft und Qualität der Daten dokumentiert?

## 1.3 Arten von Daten

- a) Welche Datenarten werden verwendet bzw. erzeugt? (*z. B. Beobachtungsdaten, Simulationsdaten, Video-Interviews, ...*)
- b) Inwieweit sind die Daten reproduzierbar?
- c) Wie werden Daten erfasst oder erstellt? (*z. B.: welche Instrumente, Technologien und Verfahren werden benutzt und anhand welcher Kriterien wird entschieden, ob ein Datensatz erzeugt wird?*)
- d) Wie groß ist die geschätzte Datenmenge/Produktionsrate?
- e) Welche Maßnahmen werden zur Qualitätssicherung bzw. für das Qualitätsmanagement ergriffen? (*z. B. Dokumentation, Kalibrierung, Validierung, Überwachung, Transkriptionsmetadaten, Peer-Review*)
- f) In welchen Dateiformaten werden die Daten vorliegen? Mit welchen Datenformaten wird gearbeitet?

## 2 Auswahl und Aufbewahrungsduer

### 2.1 Gründe für die Aufbewahrung

Wieso müssen welche Daten ganz oder teilweise aufbewahrt werden? (*mehrere Antworten möglich*)

- a) Arbeitskopie: Sollen die Daten für die aktive Arbeit während des Vorhabens gesichert werden?

- b) Nachweis der guten wissenschaftlichen Praxis: Sind die Daten Grundlage einer Publikation?
- c) Nachnutzung: Sind die Daten für spätere Forschung wichtig und nicht effizient reproduzierbar?
- d) Auflagen: Unterliegen die Daten rechtlichen oder vertraglichen Auflagen bzgl. ihrer Aufbewahrung? Welchen?
- e) Dokumentation: Sind die Daten gesellschaftlich bzw. politisch relevant?

## 2.2 Datenauswahl

- a) Zu welchem Zeitpunkt erfolgt die Selektion?
- b) Wer ist für die Auswahl verantwortlich?
- c) Welche Hilfsmittel (z. B. Software) werden für die Selektion verwendet?
- d) Welche Kriterien werden für die Auswahl festgelegt?

## 2.3 Aufbewahrung

- a) Wie lange sollen welche Daten aufbewahrt werden? (*z. B. bis zum Ende des Projekts, zehn Jahre nach Ende des Projekts, bis zu einem bestimmten Ereignis, unbefristet, ...*)
- b) Wie ist das Verfahren, wenn Daten ggf. nicht mehr aufbewahrt werden sollen? Werden die Produzenten benachrichtigt?

# 3 Ingest: Einspeisen und Verantwortungsübernahme

## 3.1 Verfahren

- a) Wann werden die Daten übergeben (in welcher Projektphase und wann innerhalb des Ingest-Workflows)?
- b) Wie werden die Daten übertragen?
- c) Wann und von wem werden welche Metadaten erfasst?
- d) Wie werden Daten und Metadaten auf technische/formale Korrektheit und Vollständigkeit überprüft (Validierung)?
- e) Wie werden sensible Daten behandelt?

### 3.2 Verantwortungsübernahme

- a) Sind die Rechte und Pflichten der Datenproduzenten und des Datenarchivs/Repository geklärt? Wer ist für welchen Teil des Ingest verantwortlich?
- b) Gibt es eine Übernahmevereinbarung?
- c) Wird der Ingest protokolliert?
- d) Ist ein Vorgehen für die Fehlerbehandlung definiert?

## 4 Speicherung und Infrastruktur

### 4.1 Datensicherung

- a) Wer ist während des Projekts und wer ist nach dem Projekt verantwortlich für die Speicherung der Daten?
- b) Mit welchen Technologien werden die Daten gespeichert?
- c) An welchen Orten werden die Daten gespeichert?
- d) Werden regelmäßig zusätzliche Sicherheitskopien erstellt und überprüft?

### 4.2 Infrastruktur

- a) Wie hoch wird die erwartete Datenmenge sein (pro Jahr oder in der Gesamtdauer des Projekts)?
- b) Welche Netzwerk-Bandbreite ist für den Datentransfer und Zugriff erforderlich?
- c) Welche Formen des Zugriffs sind vorhersehbar? Wie häufig und intensiv wird auf die Daten zugegriffen? Müssen die Daten online sein, oder reichen auch Nearline- oder Offline-Speicher (Band)?
- d) Gibt es spezielle Anforderungen durch besondere Dienste zur Datennutzung? (z. B. *Grafikkarten bei Visualisierung, Rechenkapazität für Datenextraktion, ...*)

## 5 Erhaltungsmaßnahmen und ihre Planung

- a) Sind die eingesetzten Technologien und Abhängigkeiten von anderen Datensätzen oder Diensten dokumentiert?
- b) Sind die Nutzungszielgruppe und die Anforderungen an die Nutzung der Daten dokumentiert?
- c) Wird regelmäßig überprüft, ob sich diese Anforderungen sowie die verfügbaren Technologien oder Abhängigkeiten verändert haben?
- d) Gibt es eine Neubewertung der Aufbewahrungswürdigkeit nach einem definierten Zeitraum/Ereignis?
- e) Gibt es eine Nachfolgeregelung für den Fall, dass die aufbewahrende Institution die Aufgabe abgeben muss?

## 6 Zugriff und Nutzung

### 6.1 Nachnutzung und Suchbarkeit

- a) Können prinzipiell die Daten auch von Anderen innerhalb oder außerhalb des Projekts genutzt werden?
- b) Gibt es Gründe, die Daten prinzipiell nicht zu freizugeben? (*z. B. Datenschutz, Geheimhaltung etc.*)
- c) Gibt es eine Verpflichtung, die Daten freizugeben? (*z. B. durch den Geldgeber*)
- d) Welche Einrichtungen bzw. Gruppen werden voraussichtlich an den Daten interessiert sein?
- e) Wie ist das Verfahren, um Zugriff auf die Daten zu bekommen?
- f) Sind die Daten suchbar?
- g) Wie werden die Daten veröffentlicht bzw. bekannt gemacht?
- h) Was sind die beabsichtigten oder vorhersehbaren Verwendungen der Daten? Mit welchen Diensten/Programmen werden die Daten üblicherweise genutzt?

## 6.2 Offener Zugang versus Zugriffsbeschränkungen

- a) Gibt es ein Recht auf Erstnutzung durch den Ersteller der Daten? Ab wann dürfen auch Andere auf Daten bzw. Metadaten zugreifen (Sperrfristen)?
- b) Unterliegen die Daten Nutzungseinschränkungen oder Lizenzbedingungen?
- c) Wird der Zugang gebührenpflichtig sein?
- d) Wie werden die Zugriffsbedingungen durchgesetzt und technisch implementiert? Wer ist für die Durchsetzung verantwortlich?

## 6.3 Interoperabilität

- a) Sind fremde Dienste oder Archive interoperabel zu eigenen Datendiensten?
- b) Auf welchen Ebenen/in welcher Hinsicht wird Interoperabilität gefordert/gewährleistet/angestrebt?

## Teil II: Übergreifende Aufgaben des Forschungsdaten-Managements

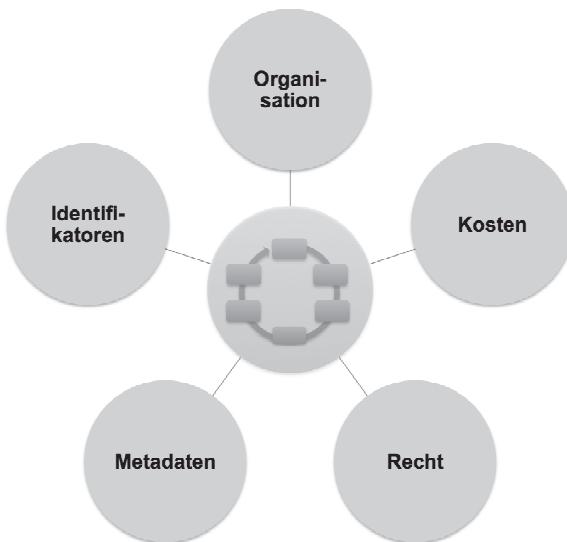


Abb. 2 Übergreifende Aufgaben des Forschungsdaten-Managements

## 7 Organisation, Management und Policies

### 7.1 Organisation und Management

- Werden die Daten in einem institutionellen, kollaborativen oder thematischen Repository aufbewahrt?
- Ist der Bezugsrahmen national oder international? Erwachsen daraus besondere Anforderungen?
- Welche Organisationseinheit ist zuständig für das Datenmanagement?
- Welche Institutionen sind am Datenmanagement beteiligt?

- e) Sind die beteiligten Institutionen, Organisationen, Personen benannt und informiert? Sind deren Beiträge definiert? Liegt deren Einwilligung vor?
- f) Ist der Workflow für das Datenmanagement beschrieben?
- g) Liegt eine Beschreibung und Abschätzung von Personal- und anderen Ressourcen vor?

## 7.2 Policies

- a) Welche Anforderungen und Vorgaben bestehen
  - von Seiten der Finanzgeber,
  - von den beteiligten Institutionen oder Forschungsgruppen,
  - von der Fachgemeinschaft,
  - von relevanten internationalen Vorhaben
  - von anderen Seitenzum Datenmanagement der Daten?
- b) Welche Auflagen liegen ggf. von Seiten eines Datengebers vor?
- c) Welche Policies müssen für die Datenaufnahme, den Betrieb und die Nutzung des Repository erstellt/durchgesetzt werden? Wer ist hierfür verantwortlich?
- d) Welche Selektionsverfahren für die Daten sind definiert? Gibt es Prozesse innerhalb der Fachgemeinschaft, die zur Selektion der Daten dienen können?

## 7.3 Einhaltung der Vorgaben und Planung

- a) Wie, wann und von wem wird die Einhaltung der Planung überprüft oder nachgewiesen?
- b) Wie, wann und von wem wird diese Checkliste bei Bedarf aktualisiert?

## 8 Kosten

### 8.1 Kosten- und Aufwandsabschätzung

- a) Sind die Kosten und der Personalaufwand abgeschätzt worden? (*z.B. anhand von Vergleichswerten, einer Lebenszyklus-Analyse, etc.*)
- b) Welche Kosten entstehen während der Projektlaufzeit und welche danach?
- c) Wer übernimmt die Kosten? Wie hoch ist das im Projekt veranschlagte Budget für Datenmanagement?

### 8.2 Anreize

- a) Sind den Beteiligten die Gründe für das Management von Forschungsdaten klar? (*siehe Frage 2.1*)
- b) Ist es notwendig, den individuellen und allgemeinen Nutzen herauszuarbeiten oder Anreizsysteme einzuführen?
- c) Sind die Kosten für das Datenmanagement ins Verhältnis zu den Kosten der Datenerzeugung gesetzt worden?

## 9 Rechtliche Aspekte von Forschungsdaten

*Die rechtliche Absicherung erfordert unter Umständen das Hinzuziehen von Fachleuten wie z.B. Juristen. Es ist jedoch notwendig, eine angemessene Balance zwischen rechtlicher Absicherung und pragmatischer Forschungspraxis zu finden. Untätigkeit in diesen Fragen aufgrund gesetzlicher Überforderung soll vermieden werden.*

### 9.1 Datenschutz – personenbezogene Daten

- a) Unterliegen die Forschungsdaten dem Datenschutz? Handelt es sich bei den Forschungsdaten um „personenbezogene Daten“ im Sinne des Bundesdatenschutzgesetz (BDSG) §3?

- b) Welche Anstrengungen wurden unternommen, um den Anforderungen des Datenschutzes zu genügen?
- c) Gibt es ethisch, kommerziell oder in anderer Hinsicht sensible Daten?
- d) Welche Maßnahmen werden zum Schutz dieser Daten getroffen?

## 9.2 Urheberrecht

*Die Frage des Urheberrechts an Forschungsdaten ist juristisch nicht abschließend geklärt und auch das Urheberrecht selbst unterliegt Veränderungen. Es ist sinnvoll, diese Fragen mit den Rechteinhabern explizit zu klären bzw. Urheber- und Nutzungsrechte vertraglich zu regeln.*

- a) Werden fremde Forschungsdaten oder Software verwendet, welche dem Urheberrecht, dem Patentrecht oder anderen geistigen Eigentumsrechten unterliegen? Wenn ja, wer besitzt die Rechte?
- b) Unterliegen eigene Forschungsdaten oder Software dem Urheberrecht, dem Patentrecht oder anderen geistigen Eigentumsrechten? Wenn ja, wie werden sie lizenziert und welche Nutzungsrechte werden eingeräumt? (z. B. Einschränkungen oder Verzögerungen der Datenverfügbarkeit)
- c) Wenn entsprechende Rechte an den Forschungsdaten bestehen, werden alle notwendigen Maßnahmen zum Zwecke des Datenmanagements eingeräumt?
- d) Existieren Schutzfristen für die Forschungsdaten, welche während des Aufbewahrungszeitraumes enden? Wie wird mit diesen Daten verfahren?

## 10 Metadaten

- a) Welchem *Zweck* dient die Einrichtung eines Metadatensystems; wozu sollen die Metadaten dienen oder benutzt werden? (z. B.: *Daten sichtbar machen, Interpretation, Austausch, Verwaltung/Pflege, Präsentation*)
- b) Welche *Informationen* sollen durch Metadaten beschrieben werden? (z. B. *Objekte, Akteure, Quellen, Vorgänge, Ergebnisse*)
- c) In welchem Rahmensystem werden die Metadaten erfasst, welche Bedeutungen sollen bzw. können darin abgebildet werden? Welcher *Semantik* unterliegen die Metadaten? Gibt es einen bestimmten (fachspezi-

- fischen oder universellen) Standard, der angewandt werden kann (z. B. ISO 19115 oder Dublin Core)?
- d) In welchem Format werden die Metadaten gespeichert und ausgetauscht, in welcher *Syntax* werden sie präsentiert?
  - e) Welche Metadaten können *automatisch* erhoben werden, wer organisiert die vollständige und korrekte Erfassung der anderen?
  - f) Welche Voraussetzungen bestehen hard- und softwaretechnisch für die Verarbeitung dieser Metadaten?
  - g) Welche Vorkenntnisse/Fachkenntnisse sind zum Verständnis / für die Verarbeitung dieser Metadaten erforderlich?

## 11 Identifikatoren und Informationsobjekte

### 11.1 Zu identifizierende Informationsobjekte

- a) Wie sind die Informationsobjekte definiert und in welchen Verhältnissen stehen sie zueinander? (*z.B.: Werden Daten aus anderen Daten erzeugt oder gibt es logische Beziehungen zwischen ihnen? Sind diese Verhältnisse in einem Informationsmodell oder einer formalen Ontologie dokumentiert?*)
- b) Welche Informationsobjekte sind so zentral, dass sie eigene Identifikatoren benötigen?
- c) Für welche Informationsobjekte ist es wichtig, dass die Identifikatoren persistent bzw. dauerhaft zitierfähig sind?

### 11.2 Identifikatoren

- a) Welche Identifikatoren werden benutzt (Standards, Syntax etc.)? Sind sie projektübergreifend definiert?
- b) Wo werden die Identifikatoren nachgewiesen/aufgelöst? Wird ein externer Resolver-Anbieter in Anspruch genommen?
- c) Wer wird die Aktualisierung und Pflege von Identifikatoren während des Projektes/nach Projektende vornehmen?

## Kurzfassung

### 1. Planung und Erstellung

- 1.1 Sind alle Rahmendaten des Projekts dokumentiert (Name, Ziele, Finanzgeber, Laufzeit, Partner, Leiter)?
- 1.2 Wie können bereits existierende Daten integriert/nachgenutzt werden?
- 1.3 Welche Bedeutung haben die Daten für das Vorhabensziel?
- 1.4 Wie lassen sich die verwendeten/erzeugten Daten charakterisieren (Datenarten, Formate, Reproduzierbarkeit)?
- 1.5 Wie werden die Daten erfasst/erstellt?
- 1.6 Wie groß ist die Datenmenge/Produktionsrate?
- 1.7 Wie erfolgt die Qualitätssicherung?

### 2. Auswahl und Aufbewahrungsdauer

- 2.1 Wieso müssen welche Daten aufbewahrt werden?
- 2.2 Wann, durch wen und womit erfolgt die Datenauswahl?
- 2.3 Wie lange müssen die Daten aufbewahrt werden?
- 2.4 Was geschieht bei Ablauf der Aufbewahrungsdauer?

### 3. Ingest: Einspeisen und Verantwortungsübernahme

- 3.1 Wann und wie werden die Daten übergeben/übertragen?
- 3.2 Wann und von wem werden welche Metadaten erfasst?
- 3.3 Wie werden Daten und Metadaten validiert?
- 3.4 Wie wird mit sensiblen Daten umgegangen?
- 3.5 Sind Rechte und Pflichten von Datenproduzent und -archiv geklärt (Protokollierung, Fehlerbehandlung)?

### 4. Speicherung und Infrastruktur

- 4.1 Wer ist während des Projekts und danach für die Speicherung der Daten verantwortlich?
- 4.2 Mit welchen Technologien und an welchen Orten werden die Daten gespeichert?
- 4.3 Werden regelmäßig Sicherheitskopien erstellt und überprüft?
- 4.4 Wie hoch ist die erwartete Datenmenge?
- 4.5 Gibt es besondere Infrastruktur-Anforderungen für Datentransfer, -zugriff und -nutzung? (Netzwerk-Bandbreite, Hardware etc.)

*5. Erhaltungsmaßnahmen*

- 5.1 Sind die eingesetzten Technologien sowie Abhängigkeiten, Nutzungszielgruppe und -anforderungen dokumentiert?
- 5.2 Wird regelmäßig überprüft, ob sich die Anforderungen, verfügbaren Technologien oder Abhängigkeiten verändert haben?
- 5.3 Wird die Aufbewahrungswürdigkeit regelmäßig überprüft?
- 5.4 Gibt es eine Nachfolgeregelung bei einem Wechsel der aufbewahrenden Institution?

*6. Zugriff und Nutzung*

- 6.1 Können die Daten auch von Anderen innerhalb oder außerhalb des Projekts genutzt werden?
- 6.2 Gibt es Verpflichtungen, Daten freizugeben oder nicht freizugeben?
- 6.3 Welche Einrichtungen/Gruppen werden an den Daten interessiert sein?
- 6.4 Wie werden Veröffentlichung, Suchbarkeit und Zugriff realisiert?
- 6.5 Zu welchem Zweck und mit welcher Software werden die Daten voraussichtlich genutzt?
- 6.6 Wie werden ggf. Erstnutzungsrecht, Nutzungsbeschränkungen oder Lizenzbedingungen durchgesetzt?
- 6.7 Spielt Interoperabilität eine Rolle?

*7. Management, Organisation und Policies*

- 7.1 In welcher Art von Repository werden die Daten aufbewahrt?
- 7.2 Ist der Bezugsrahmen national oder international?
- 7.3 Welche Institutionen sind für das Datenmanagement zuständig oder daran beteiligt?
- 7.4 Haben alle Beteiligten eingewilligt und sind deren Beiträge definiert?
- 7.5 Ist der Workflow des Datenmanagements beschrieben?
- 7.6 Sind alle Ressourcen beschrieben und abgeschätzt?
- 7.7 Welche Anforderungen/Auflagen/Policies müssen berücksichtigt/umgesetzt werden? Von wem?
- 7.8 Wie wird die Einhaltung der Planung überprüft?

*8. Kosten*

- 8.1 Wie hoch sind die Kosten und der Personalaufwand für das Datenmanagement während des Projektes / nach dem Projekt?
- 8.2 Wer übernimmt die Kosten?

- 8.3 Stehen alle Verantwortlichen und Beteiligten hinter den Plänen zum Datenmanagement?
9. *Rechtliche Aspekte von Forschungsdaten*
- 9.1 Sind die Daten aufgrund des Datenschutzes oder aus anderen Gründen sensibel?
  - 9.2 Werden fremde Daten oder Software verwendet, welche dem Urheberrecht, dem Patentrecht o.Ä. unterliegen?
  - 9.3 Unterliegen eigene Daten oder Software dem Urheberrecht/Patentrecht und sind die Nutzungsbedingungen und Rechte geklärt?
  - 9.4 Werden alle notwendigen Maßnahmen zum Datenmanagement eingeräumt?
  - 9.5 Sind evtl. auslaufende Schutzfristen zu berücksichtigen?
10. *Metadaten*
- 10.1 Wozu sollen die Metadaten dienen oder benutzt werden?
  - 10.2 Was soll durch Metadaten beschrieben werden?
  - 10.3 Welche Semantik und Syntax wird verwendet?
  - 10.4 Inwieweit können die Metadaten automatisch erstellt werden?
  - 10.5 Welche Voraussetzungen bestehen für die Verarbeitung und das Verständnis der Metadaten?
11. *Identifikatoren und Informationsobjekte*
- 11.1 In welchem Verhältnis stehen die Informationsobjekte zueinander?
  - 11.2 Für welche Informationsobjekte werden dauerhafte Identifikatoren benötigt?
  - 11.3 Welche Identifikatoren werden benutzt?
  - 11.4 Wie werden die Identifikatoren nachgewiesen?
  - 11.5 Wer wird die Aktualisierung und Pflege von Identifikatoren vornehmen?

## **Formale Informationen zur Checkliste**

Erstellungsdatum

An Erstellung beteiligte Personen

# **Bitstream Preservation: Bewertungskriterien für Speicherdiene**



## 1 Einleitung

Die Langzeitarchivierung digitaler Daten umfasst verschiedene Aufgabenbereiche, um die Nutzbarkeit von digitalen Daten langfristig sicherzustellen. Grundlegend ist, dass Daten hierfür auf der Speicherebene sicher vorgehalten werden müssen. Andere Aufgaben umfassen z.B. Bereiche wie Dateiformate, die veralten können, Kontextmetadaten, die zur Wiederverwendung benötigte Hintergrundinformationen angeben, oder organisatorische und finanzielle Fragen. Die Kompetenz und Verantwortung für diese Aufgaben verteilt sich oftmals über mehrere Akteure [WissGrid Langzeitarchivierungsarchitektur 2010, S. 6–8, 48 ff.].

Im Folgenden werden nur Anforderungen und Bewertungskriterien für einen Teilaspekt der Langzeitarchivierung, der sogenannten Bitstream Preservation, definiert. Bitstream Preservation stellt sicher, dass Bits eines Datenobjekts sich nicht unbeabsichtigt verändern, zugreifbar bleiben und vor dem Ausfall, Verfall und Veralten der Speichermedien und -technologien bewahrt werden.

### Warum Bitstream-Preservation?

Die Notwendigkeit zur Bitstream Preservation ist sicherlich jedem Nutzer digitaler Medien einsichtig, aber sie wird für Forschungsdaten auch von Forschungsförderern explizit verlangt.<sup>28</sup> Allerdings ist diese Aufgabe als nicht trivial einzustufen, auch wenn scheinbar Speicherplatz immer günstiger und zuverlässiger wird. Aber zu oft werden die vollen Betriebskosten eines Speicherdienstes vernachlässigt und theoretisch ermittelten Herstellerangaben wie MTTDL oder MTBF (Mean Time To Data Loss bzw. Mean Time Between Failure) wird zu viel Vertrauen geschenkt (vgl. z.B. [Rosenthal 2010]). Als Beispiel sei nur das Problem der latenten oder versteckten Speicherfehler angeführt, dass Speichermedien nicht nur vollständig und unmittelbar offensichtlich versagen, sondern dass Fehler durch den gesamten Hard- und Software-Stack entstehen können und unter Umständen auch erst beim Auslesen entdeckt werden. Beispielsweise hat das CERN Anfang 2007 die Fehlerrate eines CERN-Raid-Diskpools empirisch gemessen und in

---

<sup>28</sup> Siehe Empfehlung Nummer 7 in [Deutsche Forschungsgemeinschaft 1998] und [Deutsche Forschungsgemeinschaft 2009].

einem Datenbestand von ungefähr neun Terabyte 22 nicht abfangbare Checksumendifferenzen festgestellt [Panzer-Steindel 2007].

## Warum Bewertungskriterien?

Im Folgenden werden Kriterien aufgeführt, die es Nutzern und Anbietern von Speicherdiestleistungen ermöglichen sollen, eine Bewertung unter dem Gesichtspunkt der Bitstream Preservation durchzuführen.<sup>29</sup> Ziel der Kriterien ist es nicht, mit ihnen absolute und unrealistische Sicherheitsgarantien zu formulieren, sondern Integritätsanforderungen und Kosten in ein sinnvolles Verhältnis zu bringen und Vergleichbarkeit zu fördern.<sup>30</sup> Es wäre wünschenswert, dass Daten-/Rechenzentren ihre Speicherdiestangebote entsprechend der Kriterien beschreiben und die Nutzer bei der Bewertung unterstützen. Auch wenn nicht immer verbindliche Aussagen zu einzelnen Kriterien getroffen werden können, so ist eine rein informative Beschreibung des gegenwärtigen Stands bzw. des üblichen Erfüllungsgrades hilfreich. Die WissGrid-Arbeiten sind in Kooperation mit dem SLA4D-Grid-Projekt in eine Vorlage für Service-Level-Agreements (SLAs) eingearbeitet worden [SLA4D 2011] – für die Fälle, in denen Kriterien vertraglich verbindlich definiert werden sollen.

Für Bitstream Preservation kann zwischen allgemeinen Speicherkriterien und den spezifischen, stärker auf Minimierung des Verlustrisikos ziellenden Integritätskriterien unterschieden werden. In einer idealen Welt wäre (sofern es überhaupt Datenverlust gäbe) für den Nutzer nur ein Integritätskriterium wichtig, das die maximale Verlustwahrscheinlichkeit angibt, dass eine definierte Datenmenge in einem definierten Zeitraum verloren geht. Durch welche Technik die Integrität gesichert würde, ob sie durch viele Kopien oder durch besonders robuste Speichertechnologien erzielt würde, wäre für den Nutzer unerheblich. Da aber in der Praxis derzeit kein solcher Wert ermittelt werden kann, wird eine Sammlung von Integritätskriterien im Kapitel 3 vor gestellt. Eine Übersicht über allgemeine Kriterien wird in Kapitel 2 gegeben und Kriterien zur Vertraulichkeit von Daten finden sich im Kapitel 4.

---

29 Neben eigenen Erwägungen und den zitierten Quellen entstammen die Kriterien auch [Baker et al. 2006].

30 Siehe auch [Wright et al. 2009]. Ein Verfahren zur Evaluation von Alternativen zur Bitstream Preservation wird vorgestellt in [Zierau et al. 2010].

## Weitere Aspekte

Über die unten aufgeführten Kriterien hinaus sind weitere vertragliche Regelungen und Angaben für den vertrauenswürdigen Betrieb von Speicherdieneleistungen notwendig. Exemplarisch seien hier Angaben zu den Datenbesitzern/Verantwortlichen und Aktualisierungen des Angebots erwähnt. Ein Datenzentrum muss den Besitzer der Daten kontaktieren können, z.B. aus juristischen Gründen oder um über Zwischenfälle zu informieren. Auch ob und wie eine Weitergabe der Verantwortung erfolgt (z.B. aufgrund eines Arbeitsplatzwechsels des ursprünglichen Datenbesitzers), sollte geklärt sein. Da sich die eingesetzten Technologien und die Rahmenbedingungen eines Datenzentrums schnell ändern können, ist davon auszugehen, dass eine anfängliche Beschreibung des Speicherdienvtes während der Speicherdauer eines Datenbestandes ihre Gültigkeit verliert. Dies mag keine nennenswerte Relevanz haben, wenn es sich nur um Erweiterungen oder einfache Verbesserungen des Angebots handelt, es kann aber gerade bei Sicherheitstechnologien wichtig sein, Aktualisierungen vorzunehmen und alte Verfahren auslaufen zu lassen. Es sollte vorab geklärt sein, wie mit Änderungen und Aktualisierungen des Speicherdienvtes umgegangen wird.

## Hinweis zur Notation

Die Kriterien wurden nach ihrer Wichtigkeit für eine Einschätzung von Speicherdienvten für die Langzeitarchivierung im Bereich der öffentlich geförderten Forschung in die Kategorien „wichtig“ und „weniger wichtig“ eingeteilt. Die nach Auffassung der Autoren zentralen Kriterien sind mit dem Symbol ★ gekennzeichnet. Zu diesen Kriterien sollten Speicherdienvstanbieter in jedem Fall Angaben machen.

## 2 Allgemeine Service-Level-Kriterien für Speicherdiene

1. ★ **Datenvolumen:** das bereitgestellte/benötigte Datenvolumen Einheiten: GB/TB/PB/...
2. ★ **Speicherdauer:** der Zeitraum, für den der Speicherdiene mindestens zur Verfügung gestellt wird/genutzt werden soll  
Einheiten: Zeitdauer oder absoluter Zeitpunkt
3. ★ **Löschermin:** Ist ein Löschermin vorgegeben, müssen die betreffenden Daten an diesem Termin gelöscht werden. Maximale Aufbewahrungszeiträume oder Löschermine sind in einigen Fällen durch den Gesetzgeber vorgeschrieben, insbesondere bei personenbezogenen Daten.  
Einheiten: Zeitdauer oder Zeitpunkt
4. ★ **Sperrfrist:** In einigen Anwendungsfällen werden die Daten erst nach Ablauf einer Sperrfrist für die Öffentlichkeit bzw. die Fachöffentlichkeit zugänglich. Während der Sperrfrist können die Daten nur vom Produzenten bzw. von der Gruppe des Produzenten gelesen werden. Für Forschungsdaten räumen viele Datenzentren den Produzenten der Daten eine Sperrfrist ein, damit eine Erstverarbeitung in Ruhe möglich ist.  
Einheiten: Zeitdauer oder Zeitpunkt
5. ★ **Zugriffsverfahren:** Über welche Arten von Zugang (Protokolle) kann/soll auf Daten/Dateien zugegriffen werden?  
Einheiten: Auflistung der unterstützten Zugriffsprotokolle, z. B. HTTP, SCP, GridFTP ...
6. **Datenanforderungen:** Welche Größen können Daten/Dateien haben? Gibt es eine Limitierung der Anzahl? (z.B. um ein Bandspeichersystem nicht durch zu viele kleine Dateien zu belasten)  
Einheiten: max. MB/GB/TB/PB/..., min. MB/GB/TB/PB/..., max. Anzahl
7. **Zugriffsgrößen:** Wie lange dauert es von der Anfrage nach einer Speicheroperation bis zu ihrem Beginn maximal bzw. im Mittel? Wie viele Zugriffe auf archivierte Daten sind erlaubt/geplant? Wie groß ist die maximal abrufbare/abgerufene Datenmenge in Summe, pro Zugriff und pro Datei?  
Einheiten: Maximalzahl Zugriffe/Zeiteinheit, maximale Datenmenge/Zeiteinheit (Ggf. sind diese Einheiten auf bestimmte Zeiträume bezogen, z. B. wenn in weniger oder stärker nutzungsintensiven Zeiträumen, intensive oder geringere Anforderungen erfüllt werden können.)

8. *Transfersgeschwindigkeiten*: Wie schnell können Daten gelesen und geschrieben werden?  
Einheiten: min./max. Datenmenge pro Zeiteinheit
9. *Verfügbarkeit*: Wie häufig ist das System nicht nutzbar?  
Einheiten: „9s“, Prozentangabe
10. *Maintenance/Service*: Wie ist die Reaktionszeit bei Problemen?  
Einheiten: Zeitdauer nach Problemeingang, ggf. auf verschiedene Zeiträume (z.B. Wochenende vs. Wochentag) bezogen.

### 3 Spezifische Bitstream-Preservation-/Integritätskriterien

Die folgenden Angaben beziehen sich jeweils nur auf den dauerhaften, langfristigen Speicherort. Eigenschaften von Kopien in temporären Zwischenspeichern (z. B. Plattencache/SAN vor einer Tape-Library) können für die Bitstream Preservation vernachlässigt werden.

11. ★ *Kopienanzahl*: Werden Kopien der Daten dauerhaft gespeichert? Je mehr Kopien dauerhaft gespeichert werden, desto unwahrscheinlicher ist es, dass alle Kopien defekt sind. In der derzeitigen Praxis ist es fast nur die Kopienanzahl, die bei unterschiedlichen Angeboten eines Dienstleisters tatsächlich variiert wird.  
Einheiten: Anzahl identischer Kopien
12. *Kopienunabhängigkeit*: Wie unabhängig sind die Kopien unter verschiedenen Gesichtspunkten? Erst die Unabhängigkeit der Kopien voneinander sichert, dass die Kopien nicht vom selben Fehler oder Ereignis betroffen sind.
  - 12.1 *geografisch*: Die geografische Unabhängigkeit ist z. B. für lokale Unfälle, Unglücksfälle, Naturereignisse, etc. relevant und kann nicht nur als Distanz, sondern auch durch Kategorisierungen wie unterschiedliche Räume, unterschiedliche Gebäude/Gefahrenzonen bis hin zu unterschiedlichen Regionen/Ländern/Kontinenten ausgedrückt werden.  
Einheiten: z. B. unterschiedliche Räume, Gebäude, Gefahrenzonen und Entfernung in km

- 12.2 *organisatorisch*: Unter organisatorischer Unabhängigkeit ist die Unabhängigkeit von denselben Personen, Arbeitsabläufen, Institutionen oder auch rechtlich-politischen und finanziellen Rahmenbedingungen zu verstehen.  
Einheiten: z. B. unterschiedliche Administratoren, unterschiedliche Institutionen/Unterauftragnehmer und ggf. unterschiedliche Gesetze/Länder
- 12.3 *technologisch*: Viele Fehler entstehen durch Probleme mit einem bestimmten Typ, einer Version oder Produktionsreihe der verwendeten Speichermedien, Hardware oder Software. Das Risiko dieser Art von Fehlern lässt sich durch eine kontrollierte Heterogenität der eingesetzten Technologien vermindern.  
Einheiten: jeweils (Produktionscharge, Modell, Hersteller, Technologie) für Speichermedien, -Hardware und -Software
13. *Fehlerhäufigkeit der Kopien*: Angaben zu der Fehlerhäufigkeit von Kopien sollten idealerweise auf empirisch gemessenen Daten und nicht nur auf theoretischen Hochrechnungen, wie z.B. den Herstellerangaben zur Speichermedienhaltbarkeit, beruhen.
- 13.1 *Ausfallrate Speichermedien*: unmittelbar sichtbares Versagen eines kompletten Datenträgers  
Einheit: möglichst die empirische Austauschrate (annual replacement rate, ARR), falls nicht möglich, dann Hersteller-MTTF/-MTBF (mean time to/between failure) pro Speicherkapazität in MB/GB/TB/PB
- 13.2 *Bitfehlerrate*: die Häufigkeit latenter/verborgener Fehler auf Bit- oder Blockebene.  
Einheit: Mean time to latent fault
- 13.3 *Gegenmaßnahmen*: Maßnahmen, um die Fehlerhäufigkeit zu reduzieren, Lesbarkeit zu gewährleisten und Alterungsprozessen der Datenspeicherung entgegenzuwirken, z.B. Häufigkeit des Umkopierens der Daten auf andere Medien.  
Einheiten: Freitext
14. *Integritätstests*: Integritätstests sind ein Mittel, um latente/verborgene Fehler zu entdecken.
- 14.1 *Häufigkeit*: Je häufiger ein Integritätstest durchgeführt wird, desto schneller können Fehler entdeckt und die Integrität wieder hergestellt werden.  
Einheit: Dauer zwischen zwei Tests

- 14.2 *Verfahren:* Unterschiedliche Integritätstests sind unterschiedlich zuverlässig, z.B. CRC- vs. MD5-Checksummen.  
Einheit: Verfahren, Checksummenalgorithmus
- 14.3 *Integrität der Checksummenkopien:* Prinzipiell sind auch Checksummen Datenobjekte, die verloren gehen können und nicht nur als einfache Kopie vorliegen sollten.  
Einheit: Verfahren
15. *Integritätswiederherstellung:* Idealerweise stellt ein Speicherdiest im Fehlerfall die Integrität wieder her, allerdings besteht eine gewisse Gefahr, dass Fehler repliziert werden.
- 15.1 *Verfahren:* Existiert ein Mechanismus zur Integritätswiederherstellung?  
Einheiten: ja/nein, eingesetztes Verfahren
- 15.2 *Dauer:* Je schneller die Integrität wiederhergestellt wird, desto kürzer herrscht eine erhöhte Verlustwahrscheinlichkeit, allerdings kann ein gleichzeitiger Produktivbetrieb verlangsamt werden.  
Einheiten: durchschnittliches Datenvolumen pro Zeiteinheit

## 4 Sicherheit und Vertraulichkeit

16. *AAI-Verfahren:* Beschränkung des Datenzugriffs im Rahmen von AAI-Verfahren
- 16.1 *Authentifizierungsverfahren:* Nach welchem Verfahren wird sichergestellt, dass nur Berechtigte Zugang haben?  
Vokabular: Username/Passwort, OpenID, Zertifikat
- 16.2 *Autorisierungsverfahren:* Nach welchem Verfahren werden Zugriffsrechte vergeben?  
Vokabular: XACML, Unix, NTFS
17. *Beschränkung des externen Datenzugriffs:* Auf welche Art wird der Zugang zu den Daten generell sicherheitstechnisch eingeschränkt – beispielsweise, um sich gegen ein Aushebeln der AA-Infrastruktur zu schützen? Andere mögliche Maßnahmen können sein: separater virtueller Server je Kunde, IP-adressbasierter Zugriff (Whitelist, Firewall), Sichtbarkeit nur der jeweils vom authentifizierten Nutzer zugreifbaren Daten oder die Verschlüsselung von Daten.
- Einheit: Freitext

18. *Beschränkung des internen Datenzugriffs:* Auf welche Weise werden Zugriffe des Speicherdiensleisters auf die Daten eingeschränkt? Wie viele Personen haben beim Speicherdiestanbieter Zugriff auf die Daten? Wie viele Personen haben physikalisch Zugriff auf die Speichergeräte? Ist z. B. beim Zugriff auf die Daten beim Speicheranbieter ein Vier-Augen-Kontroll-Prinzip realisiert? Werden Daten verschlüsselt?

Einheit: Freitext

19. *Schutz der Kopien vor äußeren Einflüssen:* Werden gesonderte Sicherungsmaßnahmen ergriffen, die die Zuverlässigkeit der Datenspeicher erhöhen, wie zum Beispiel konstante Luftfeuchtigkeit und Raumtemperatur, Absicherung gegen Umweltkatastrophen, Feuer, Diebstahl, etc.

Einheit: Freitext

## 5 Checkliste

Kriterium	Anbieter	Kunde
allgemeine Service-Level-Kriterien		
Datenvolumen	★	
Speicherdauer	★	
Löschermin	★	
Sperrfrist	★	
Zugriffsverfahren	★	
Datenanforderungen		
Zugriffsgrößen		
Transfergeschwindigkeiten		
Verfügbarkeit		
Maintenance/Service		
spezifische Bitstream-Preservation-/Integritätskriterien		
Kopienanzahl	★	
Kopienunabhängigkeit		
geografisch		
organisatorisch		
technologisch		
Fehlerhäufigkeit der Kopien		
Ausfallrate Speichermedien		
Bitfehlerrate		
Gegenmaßnahmen		
Integritätstests		
Häufigkeit		
Verfahren		
integrierte Checksummenkopien		
Integritätswiederherstellung		
Verfahren		
Dauer		
Sicherheit und Vertraulichkeit		
AAI-Verfahren		
Authentifizierung		
Autorisierung		
externer Datenzugriff		
interner Datenzugriff		
äußerer Einfluss		



# Quellen

*Hinweis des Verlages:* Als zusätzlicher Service befindet sich ein Verzeichnis der Quellen mit verlinkten URLs auf dem Verlagsserver unter <http://www.vwh-verlag.de/vwh/?p=814>. Alle Links wurden letztmalig am 20.12.2012 abgerufen.

## Literaturverzeichnis

- Australian National Data Service (2009a). Persistent Identifiers Guide Awareness Level. URL: <http://ands.org.au/guides/persistent-identifiers-awareness.pdf>.
- Australian National Data Service (2009b). Persistent Identifiers Guide Working Level. URL: <http://ands.org.au/guides/persistent-identifiers-working.pdf>.
- Australian National Data Service (2009c). Persistent Identifiers Guide Expert Level. URL: <http://ands.org.au/guides/persistent-identifiers-expert.pdf>.
- Ayris, Paul / Davies, Richard / McLeod, Rory / Miao, Rui / Shenton, Helen & Wheatley, Paul (2008). The LIFE<sup>2</sup> Final Project Report. URL: <http://eprints.ucl.ac.uk/11758/1/11758.pdf>.
- Baca, Murtha (Ed.) (2008). *Introduction to Metadata Version 3.0*. Getty Publications. URL: [http://www.getty.edu/research/publications/electronic\\_publications/intrometadata/index.html](http://www.getty.edu/research/publications/electronic_publications/intrometadata/index.html).
- Baker et al. (2006). A Fresh Look at the Reliability of Long-term Digital Storage. In: *EuroSys '06. Proceedings of the 1st ACM SIGOPS/EuroSys European Conference on Computer Systems* (April 18–21, 2006, Leuven, Belgium). New York, NY: ACM, 221–234. URL: <http://www.hpl.hp.com/research/ssp/papers/longtermBaker2006.pdf>.
- Beagrie, Neil / Lavoie, Brian & Woppard, Matthew (2010). Keeping Research Data Safe 2. URL: <http://www.jisc.ac.uk/media/documents/publications/reports/2010/keepingresearchdatasafe2.pdf>.
- Beagrie, Neil / Palaiologk, Anna / Charles, Daphne / Beagrie, Rachel / Beagrie, Rob & Lavoie, Brian (2011). User Guide for Keeping Research Data Safe, Version 2, July 2011. URL: [http://www.beagrie.com/KeepingResearchDataSafe\\_UserGuide\\_v2.pdf](http://www.beagrie.com/KeepingResearchDataSafe_UserGuide_v2.pdf).
- Becker, Christoph / Kulovits, Hannes / Guttenbrunner, Mark / Strodl, Stephan / Rauber, Andreas & Hofman, Hans (2009). Systematic planning for digital preservation: evaluating potential strategies and building preservation plans. In: *In-*

- ternational Journal on Digital Libraries*, 10, 2009. DOI: 10.1007/s00799-009-0057-1. URL: <http://www.ifs.tuwien.ac.at/~becker/pubs/becker-ijdl2009.pdf>.
- Beinert, Tobias / Büchler, Georg / Graf, Sabine / Huth, Karsten / Keitel, Christian / Ludwig, Jens / Rödig, Peter & Steinke, Tobias (2008). nestor-materialien 10: *Wege ins Archiv / Ein Leitfaden für die Informationsübernahme in das digitale Langzeitarchiv, Version I.* nestor – Kompetenznetzwerk Langzeitarchivierung und Langzeitverfügbarkeit Digitaler Ressourcen für Deutschland, Koblenz. URL: <http://nbn-resolving.de/urn:nbn:de:0008-2008103009>.
- Berliner Erklärung (2003). URL: <http://oa.mpg.de/lang/de/berlin-prozess/berliner-erklärung/>.
- Blue Ribbon Task Force (2010). Sustainable Economics for a Digital Planet. Ensuring Long-Term Access to Digital Information. URL: [http://brtf.sdsc.edu/biblio/BRTF\\_Final\\_Report.pdf](http://brtf.sdsc.edu/biblio/BRTF_Final_Report.pdf).
- CERA2-Datenmodell (2008). URL: <http://www.mad.zmaw.de/wdc-for-climate/cera-data-model>.
- Charles Beagrie Ltd / JISC (Eds.) (2010). Keeping Research Data Safe Factsheet. URL: [http://www.beagrie.com/KRDS\\_Factsheet\\_0910.pdf](http://www.beagrie.com/KRDS_Factsheet_0910.pdf).
- CMIP5 Datenbeschreibung (o. J.). Appendix 1.1 Experiment Controlled Vocabulary. URL: [http://cmip-pcmdi.llnl.gov/cmip5/docs/cmip5\\_data\\_reference\\_Appendix1-1.pdf](http://cmip-pcmdi.llnl.gov/cmip5/docs/cmip5_data_reference_Appendix1-1.pdf).
- CMIP5 Quality Control (o. J.). CMIP5 – QC and ESG. URL: [https://redmine.dkrz.de/collaboration/projects/cmip5-qc/wiki/Qc\\_esg](https://redmine.dkrz.de/collaboration/projects/cmip5-qc/wiki/Qc_esg).
- DataCite-Metadatenschema (2011). DataCite Metadata Scheme for the Publication and Citation of Research Data. URL: [http://schema.datacite.org/meta/kernel-2.0/doc/DataCite-MetadataKernel\\_v2.0.pdf](http://schema.datacite.org/meta/kernel-2.0/doc/DataCite-MetadataKernel_v2.0.pdf).
- Day, Michael (2005). Digital Curation Manual. Instalment on “Metadata”. Version 1.1. URL: <http://www.dcc.ac.uk/sites/default/files/documents/resource/curation-manual/chapters/metadata/metadata.pdf>.
- DCMES (2012): The Dublin Core Metadata Element Set, Version 1.1. URL: <http://dublincore.org/documents/dces/>.
- DCTerms (2012): The DCMI Metadata Terms. URL: <http://dublincore.org/documents/dcterms/>.
- de Cock Buning, Madeleine / van Dinther, Barbara / Jeppesen de Boer, Christina G. & Ringnalda, Allard (2011). Report on the Legal Status of Research Data in the four partner countries. URL: <http://www.knowledge-exchange.info/default.aspx?id=461>.
- Deutsche Forschungsgemeinschaft (Hrsg.) (1998). *Vorschläge zur Sicherung guter wissenschaftlicher Praxis: Empfehlungen der Kommission „Selbstkontrolle in der*

- Wissenschaft“.* Denkschrift. Weinheim: Wiley-VCH. URL: [http://www.dfg.de/download/pdf/dfg\\_im\\_profil/reden\\_stellungnahmen/download/empfehlung\\_wiss\\_praxis\\_0198.pdf](http://www.dfg.de/download/pdf/dfg_im_profil/reden_stellungnahmen/download/empfehlung_wiss_praxis_0198.pdf).
- Deutsche Forschungsgemeinschaft (2009). Empfehlungen zur gesicherten Aufbewahrung und Bereitstellung digitaler Forschungsprimärdaten. Januar 2009. URL: [http://www.dfg.de/download/pdf/foerderung/programme/lis/ua\\_inf\\_empfehlungen\\_200901.pdf](http://www.dfg.de/download/pdf/foerderung/programme/lis/ua_inf_empfehlungen_200901.pdf)
- Dewey Decimal Classification (o.J.): Dewey® Services at a glance. URL: <http://www.oclc.org/dewey/about/default.htm>.
- DFG-Antrag (2012). Leitfaden für die Antragstellung – Projektanträge. DFG-Vordruck 54.01 – 10/12. URL: [http://www.dfg.de/formulare/54\\_01/54\\_01\\_de.pdf](http://www.dfg.de/formulare/54_01/54_01_de.pdf).
- Digital Curation 101 (o.J.): Ingest. URL: <http://www.dcc.ac.uk/training/train-trainer/disciplinary-rdm-training/ingest/ingest>.
- GeoNetwork (o.J.): GeoNetwork opensource: a standards based Geographic Data and Information Management System for the web. Project Info Sheet. URL: <http://www.osgeo.org/geonetwork/>.
- Goldstein, Serge J. & Ratliff, Mark (2010). DataSpace: A Funding and Operational Model for Long-Term Preservation and Sharing of Research Data. URL: [http://dspace.princeton.edu/jspui/bitstream/88435/dsp01w6634361k/1/DataSpace\\_FundingModel\\_20100827.pdf](http://dspace.princeton.edu/jspui/bitstream/88435/dsp01w6634361k/1/DataSpace_FundingModel_20100827.pdf).
- Gradmann, Stefan (2008). Interoperability. A key concept for large scale, persistent digital libraries. In: *DigitalPreservationEurope (DPE) Briefing Paper*. Digital-PreservationEurope. URL: <http://www.digitalpreservationeurope.eu/publications/briefs/interoperability.pdf>.
- GRIB (o.J.). GRIdded Binary (GRIB). PART II. A GUIDE TO THE CODE FORM FM 92-IX Ext. GRIB. Edition 1. URL: <http://www.wmo.int/pages/prog/www/WDM/Guides/Guide-binary-2.html>.
- Haynes, D. (2004). *Metadata for information management and retrieval*. Facet Publishing.
- Krause, Jürgen (1996). *Informationserschließung und -bereitstellung zwischen Deregulation, Kommerzialisierung und weltweiter Vernetzung – Schalenmodell*. IZ-Arbeitsbericht Nr. 6, IZ Sozialwissenschaften, Bonn. URL: [http://www.gesis.org/fileadmin/upload/forschung/publikationen/gesis\\_reihen/iz\\_arbeitsberichte/ab6.pdf](http://www.gesis.org/fileadmin/upload/forschung/publikationen/gesis_reihen/iz_arbeitsberichte/ab6.pdf).
- KRDS-I2S2-Tools (2011). KRDS/I2S2 Digital Preservation Benefit Analysis Tools Project. URL: <http://beagrie.com/krds-i2s2.php>.
- Kunze, John A. (2003). Towards Electronic Persistence Using ARK Identifiers. URL: <https://confluence.ucop.edu/download/attachments/16744455/arkcdl.pdf>.

- Ludwig, Jens / Rathmann, Torsten / Enke, Harry & Schintke, Florian (2011): *Bitstream Preservation: Bewertungskriterien für Speicherdienste*. WissGrid Arbeitspaket 3: Langzeitarchivierung von Forschungsdaten. URL: <http://www.wissgrid.de/workgroups/ap3/2011-03-08--bitstream-preservation.pdf>.  
– In diesem Band abgedruckt auf S. 100 ff. –
- MARC-XML (2008): MARC in XML. URL: <http://www.loc.gov/marc/marcxml.html>.
- Max-Planck-Gesellschaft (Hrsg.) (2001). *Verantwortliches Handeln in der Wissenschaft. Analysen und Empfehlungen*. Max-Planck-Gesellschaft.
- Meehl, Gerald A. et al. (2009). Decadal Prediction. Can It Be Skillful? In: *Bulletin of the American Meteorological Society*, 90 (19), 1467–1485. URL: <http://journals.ametsoc.org/doi/pdf/10.1175/2009BAMS2778.1>.
- MSC 2010: Zentralblatt MATH. The Mathematical Subject Classification 2010. URL: <http://www.zentralblatt-math.org/msc/data/msc2010.pdf>.
- Nationaal Archief (2005). Costs of Digital Preservation. URL: <http://www.nationaal-archief.nl/sites/default/files/docs/kennisbank/codpv1.pdf>.
- nestor AG – Digitale Bestandserhaltung (2011). nestor Materialien 15: *Leitfaden zur digitalen Bestandserhaltung. Vorgehensmodell und Umsetzung*. URL: <http://nbn-resolving.de/urn:nbn:de:0008-2011101804>.
- NetCDF (2012). Network Common Data Form. The NetCDF Users Guide. URL: [http://www.unidata.ucar.edu/software/netcdf/docs/user\\_guide.html](http://www.unidata.ucar.edu/software/netcdf/docs/user_guide.html).
- NetCDF CF Metadata Convention (2011). NetCDF Climate and Forecast (CF) Metadata Convention. Version 1.6, 5 December, 2011. URL: <http://cf-pcmdi.llnl.gov/documents/cf-conventions/1.6/cf-conventions.html>.
- Neuroth, Heike / Oßwald, Achim / Scheffel, Regine / Strathmann, Stefan & Huth, Karsten (Hrsg.) (2010). *nestor Handbuch*, Version 2.3. URL: <http://nestor.sub.uni-goettingen.de/handbuch/> [gedruckt: Version 2.0 (2009), Verl. Werner Hülsbusch].
- OAI-PMH (2008). The Open Archives Initiative Protocol for Metadata Harvesting (OAI-PMH). URL: <http://www.openarchives.org/OAI/openarchivesprotocol.html>.
- Overpeck, Jonathan T. / Meehl, Gerald A. / Bony, Sandrine & Easterling, David R. (2011). Climate Data Challenges in the 21st Century. In: *Science*, 331 (6018): 700–702. URL: <http://www.sciencemag.org/content/331/6018/700.full>.
- Panzer-Steindel (2007). Data integrity. Cern, Draft 1.3, 8. April 2007. URL: <http://indico.cern.ch/getFile.py/access?contribId=3&sessionId=0&resId=1&materialId=paper&confId=13797>.
- PILIN Transition Project (2008). Information Modelling Guide for Identifiers in e-research. URL: <http://www.linkaffiliates.net.au/pilin2/files/infomodellingere-search.pdf>.

- Powell, Andy & Johnston, Pete (2011). Metadata guidelines for the UK RDTF. Resource Discovery Taskforce. URL: <http://rdtfmetadata.jiscpress.org/>.
- PREMIS (Preservation Metadata: Implementation Strategies) Editorial Committee (Ed.) (2011). *PREMIS Data Dictionary for Preservation Metadata*, version 2.1. URL: <http://www.loc.gov/standards/premis/v2/premis-2-1.pdf>.
- Rosenthal, David S. H. (2010). Keeping Bits Safe: How Hard Can It Be? In: *Communications of the ACM*, Vol. 53, No. 11, pp. 47–55.
- SLA4D (2011). VERSION II der Architektur der SLA-Schicht, D 2.3, Version 1.0, März 2011. URL: [http://www.sla4d-grid.de/sites/default/files/SLA4D-Grid\\_Version-II\\_Architektur.pdf](http://www.sla4d-grid.de/sites/default/files/SLA4D-Grid_Version-II_Architektur.pdf).
- Spindler, Gerald & Hillegeist, Tobias (2009). KoLaWiss Projekt. Arbeitspaket 4: Recht. URL: [http://kolawiss.uni-goettingen.de/projektergebnisse/AP4\\_Report.pdf](http://kolawiss.uni-goettingen.de/projektergebnisse/AP4_Report.pdf).
- Taylor, K. E. / Stouffer, R. J. & Meehl & G. A. (2012): An Overview of CMIP5 and the experiment design. In: *Bulletin of the American Meteorological Society*, 93, pp. 485–498. URL: <http://journals.ametsoc.org/doi/pdf/10.1175/BAMS-D-11-00094.1>.
- Treloar, Andrew & Harboe-Ree, Cathrine (2008). Data management and the curation continuum: how the Monash experience is informing repository relationships. URL: [http://www.valaconf.org.au/vala2008/papers2008/111\\_Treloar\\_Final.pdf](http://www.valaconf.org.au/vala2008/papers2008/111_Treloar_Final.pdf).
- Unterzeichner der Berliner Erklärung (o. J.). URL: <http://oa.mpg.de/lang/de/berlin-prozess/signatoren/>.
- Wallace, D. (2001). Archiving metadata forum: report from the Recordkeeping Metadata Working Meeting, June 2000. In: *Archival Science*, Vol. 1, Issue 3: 253–269.
- WDCC-Nutzungsbedingungen (2010): Nutzungsbedingungen für WDCC-Daten. URL: <http://cera-www.dkrz.de/WDCC/ui/docs/TermsOfUse.html>.
- WDCC-Qualitätssicherung (o. J.): Standard Procedure (Objectives). URL: <http://um-welt.wikidora.com/wikidora/wiki/Standard%20Procedure%20%28Objectives%29>.
- WDC-Principles (2012). Constitution of the International Council for Science World Data System (ICSU WDS), Apr. 2012, URL: [http://icsu-wds.org/images/files/WDS\\_Constitution\\_04\\_04\\_12.pdf](http://icsu-wds.org/images/files/WDS_Constitution_04_04_12.pdf).
- Whyte, Angus & Wilson, Andrew (2010). Appraise & Select Research Data for Curation. URL: <http://www.dcc.ac.uk/resources/how-guides/appraise-select-research-data>.
- WissGrid Langzeitarchivierungsarchitektur (2010). Generische Langzeitarchivierungsarchitektur für D-Grid. URL: <http://www.wissgrid.de/publikationen/deliverables/wp3/WissGrid-D3.1-LZA-Architektur-v1.1.pdf>.
- Wright, Richard / Miller, Ant & Addis, Matthew (2009). The Significance of Storage in the ‘Cost of Risk’ of Digital Preservation. In: *The International Journal of*

- Digital Curation*, Vol. 4, No. 3, pp. 104–122. URL: [http://www.prestoprime.org/docs/training/Cost\\_of\\_risk\\_RW.pdf](http://www.prestoprime.org/docs/training/Cost_of_risk_RW.pdf).
- Zierau, Eld / Kejser, Ulla Bøgvad & Kulovits, Hannes (2010). Evaluation of Bit Preservation Strategies. In: *7th International Conference on Preservation of Digital Objects (iPRES2010)* (Sept. 19–24, 2010, Vienna, Austria). URL: <http://www.ifs.tuwien.ac.at/dp/ipres2010/papers/zierau-31.pdf>.

## Websites

- BADC: British Atmospheric Data Centre (BADC). URL: <http://badc.nerc.ac.uk/>.
- C3Grid Website. Collaborative Climate Community Data and Processing Grid Webseite. URL: <https://verc.enes.org/c3web>.
- C3Grid-Portal. URL: <http://www.c3grid.de/portal/>.
- CERA: Climate and Environment data Retrieval and Archiving system (CERA). URL: <http://cera-www.dkrz.de/CERA/>.
- DCMI: The Dublin Core Metadata Initiative. URL: <http://dublincore.org/>.
- Deutscher Wetterdienst (DWD). URL: <http://www.dwd.de/>.
- Deutsches Klimarechenzentrum (DKRZ). URL: <http://www.dkrz.de/>.
- GeoForschungsZentrum Potsdam. URL: <http://www.gfz-potsdam.de/>.
- GetInfo-Katalog: GetInfo-Katalog für die Suche in den Beständen der Technischen Informationsbibliothek, der Deutschen Zentralbibliotheken für Medizin und Wirtschaftswissenschaften sowie in weiteren Fachdatenbanken. URL: <https://getinfo.de/>.
- GNDMS: Generation N Data Management System. URL: <http://gndms.zib.de>.
- International Council for Science. URL: <http://www.icsu.org/>.
- International DOI Foundation (IDF). URL: <http://www.doi.org/>.
- IPCC: Intergovernmental Panel on Climate Change (IPCC). URL: <http://www.ipcc.ch>.
- OSGeo: The Open Source Geospatial Foundation. URL: <http://www.osgeo.org>.
- PCMDI: Program of Climate Model Diagnosis and Intercomparison (PCMDI). URL: <http://www-pcmdi.llnl.gov>.
- Technische Informationsbibliothek, Hannover. URL: <http://www.tib-hannover.de>.
- WDCC: Word Data Center for Climate (WDCC). URL: <http://www.mad.zmaw.de/wdc-for-climate>.
- WDC-MARE: World Data Center for Marine Environmental Sciences. URL: <http://www.wdc-mare.org>.
- WDC-RSAT: World Data Center for Remote Sensing of the Atmosphere. URL: <http://wdc.dlr.de>.

## Weitere Titel aus dem vwh-Programm

**Langzeitarchivierung von Forschungsdaten** Eine Bestandsaufnahme  
hrsg. v. Heike Neuroth, Stefan Strathmann, Achim Oßwald, Regine Scheffel,  
Jens Klump, Jens Ludwig 2012, ISBN 978-3-86488-008-7, 382 S., 29,90 €  
mit einem Vorwort von Prof. Dr.-Ing. Matthias Kleiner, Präsident der DFG

Forschungsdaten und der langfristige Zugriff auf sie sind für Wissenschaftler aller Disziplinen von großer Bedeutung: als Nachweis des Forschungsprozesses und seiner Ergebnisse, zur Nachnutzung im Rahmen inner- und interdisziplinärer Kooperationen oder im Hinblick auf vergleichende Analysen, bei denen mit neuen Methoden oder unter veränderten Rahmenbedingungen geforscht wird. Dies alles ist nur möglich, wenn Forschungsdaten gesichert, für eine langfristige Nachnutzung archiviert und zur Verfügung gestellt werden. Angesichts rasant anwachsender digitaler Datens Mengen ist die Langzeitarchivierung von Forschungsdaten für alle Wissenschaftsdisziplinen eine begleitende Infrastrukturaufgabe. In der vorliegenden Bestandsaufnahme haben WissenschaftlerInnen aus elf Fachdisziplinen – Geistes- und Sozialwissenschaften, Psycholinguistik, Pädagogik, Altertums- und Geowissenschaft, Klimaforschung, Biodiversität, Teilchenphysik, Astronomie und Medizin – systematisch den Stand und die aktuelle Praxis im Umgang mit der Langzeitarchivierung von Forschungsdaten in ihrer jeweiligen Disziplin aufgearbeitet.

**nestor Handbuch** Eine kleine Enzyklopädie der digitalen Langzeitarchivierung  
Version 2.0, hrsg. v. Heike Neuroth, Achim Oßwald, Regine Scheffel, Stefan  
Strathmann, Mathias Jehn 2009, ISBN 978-3-940317-48-3, 620 S., nur 24,90 €

### Reihe „Schriften zur Informationswissenschaft“

M. Heckner: Tagging, Rating, Posting  
2009, 27,90 €, ISBN 978-3-940317-39-1

S. Mühlbacher:  
Information Literacy in Enterprises  
2009, 32,90 €, ISBN 978-3-940317-45-2

M. Maßun: Collaborative Information Management in Enterprises  
2009, 28,90 €, ISBN 978-3-940317-49-0

T. Memmel: User Interface Specification for Interactive Software Systems  
2009, 33,90 €, ISBN 978-3-940317-53-7

A. Ratzka: Patternbasiertes User Interface Design für multimodale Interaktion  
2010, 33,90 €, 978-3-940317-62-9

M. Prestipino: Die virtuelle Gemeinschaft als Informationssystem  
2010, 30,90 €, ISBN 978-3-940317-69-8

A. Warta: Kollaboratives Wissensmanagement in Unternehmen  
2011, 30,90 €, ISBN 978-3-940317-90-2

J. Griesbaum, T. Mandl, C. Womser-Hacker (Hg.): Information und Wissen: global, sozial und frei? Proceedings  
ISI 2011 2011, 36,50 €, 978-3-940317-91-9

M. Görtz: Social Software as a Source of Information in the Workplace  
2011, 31,90 €, ISBN 978-3-86488-006-3

C. Carstens: Ontology Based Query Expansion Retrieval Support for the Domain of Educational Research  
2012, 34,90 €, ISBN 978-3-86488-011-7

A. Köstlbacher: Eine Informations-system-Infrastruktur für das Therapeutische Drug Monitoring  
2012, 27,90 €, ISBN 978-3-86488-019-3

S.-J. Untiet-Kepp: Adaptives Feedback zur Unterstützung in kollaborativen Lernumgebungen  
2012, 30,90 €, ISBN 978-3-86488-023-0

### Reihe „Web 2.0“

H. Frohner: Social Tagging  
2010, 26,90 €, ISBN 978-3-940317-03-2

R. Bauer: Die digitale Bibliothek von Babel Über den Umgang mit Wissensressourcen im Web 2.0  
2010, 26,90 €, ISBN 978-3-940317-71-1

J. Jochem: Performance 2.0 Zur Mediengeschichte der Flashmobs  
2011, 24,90 €, ISBN 978-3-940317-98-8

G. Franz: Die vielen Wikipedias Vielsprachigkeit als Zugang zu einer globalisierten Online-Welt  
2011, 27,50 €, ISBN 978-3-86488-002-5

R. Sonnberger: Facebook im Kontext medialer Umbrüche  
2012, 29,50 €, ISBN 978-3-86488-009-4

## **Reihe „E-Learning“**

- T. Strasser: Moodle im Fremdsprachenunterricht 2011, 28,50 €, ISBN 978-3-940317-92-6  
M. Nagl: Game-Assisted E-Learning in der Umweltbildung 2011, 28,50 €, ISBN 978-3-940317-94-0  
D. Schirmer et al.: Studieren als Konsum Veralltäglichung und Degendering von E-Learning 2011, 27,90 €, 978-3-940317-83-4  
C. Biel: Personal Learning Environments als Methode zur Förderung des selbstorganisierten Lernens 2011, 24,90 €, ISBN 978-3-86488-001-8  
A. Blessing: Personalisiertes E-Learning 2012, 29,90 €, 978-3-86488-007-0  
I. Zorn: Konstruktionstätigkeit mit Digitalen Medien Eine qualitative Studie als Beitrag zur Medienbildung 2012, 36,50 €, ISBN 978-3-86488-012-4  
K. Himschl-Gutermann: E-Portfolios in der universitären Weiterbildung 2012, 30,90 €, ISBN 978-3-86488-014-8  
M. Beißwenger/N. Anskeit/A. Storrer (Hg.): Wikis in Schule und Hochschule 2012, 36,90 €, ISBN 978-3-86488-017-9  
P. Bettinger: Medienbildungsprozesse Erwachsener im Umgang mit sozialen Online-Netzwerken 2012, 25,90 €, ISBN 978-3-86488-020-9  
C. Lehr: Web 2.0 in der universitären Lehre Ein Handlungsrahmen für die Gestaltung technologiegestützter Lernszenarien 2012, 27,90 €, 978-3-86488-024-7  
J. Wagner/V. Heckmann (Hg.): Web 2.0 im Fremdsprachenunterricht Ein Praxisbuch für Lehrende in Schule und Hochschule 2012, 27,50 €, ISBN 978-3-86488-022-3  
E. Blaschitz et al. (Hg.): Zukunft des Lernens Wie digitale Medien Schule, Aus- und Weiterbildung verändern 2012, 23,50 €, ISBN 978-3-86488-028-5

## **Reihe „Game Studies“**

- B. Sterbenz: Genres in Computerspielen – eine Annäherung 2011, 24,50 €, ISBN 978-3-940317-99-5

## D. Appel u. a. (Hg.):

Welt|Kriegs|Shooter  
Computerspiele als realistische Erinnerungsmedien? 2012, 28,50 €, 978-3-86488-010-0

- S. Felzmann: Playing Yesterday  
Mediennostalgie im Computerspiel 2012, 22,50 €, ISBN 978-3-86488-015-5  
M. Breuer (Hg.): E-Sport – Perspektiven aus Wissenschaft und Wirtschaft 2012, 26,90 €, ISBN 978-3-86488-026-1

## **Reihe „Medientheorie“**

- W. Drucker: Von Sputnik zu Google Earth Über den Perspektivenwechsel hin zu einer ökologischen Weltansicht 2011, 25,90 €, ISBN 978-3-940317-82-7  
S. Brugner: Über die Realität im Zeitalter digitaler Fotografie 2012, 23,90 €, ISBN 978-3-86488-018-6

## **Reihe „Medienwirtschaft“**

- J.-F. Schrape: Gutenberg-Galaxis Reloaded? Der Wandel des deutschen Buchhandels durch Internet, E-Books und Mobile Devices 2011, 17,90 €, 978-3-940317-85-8  
B. Blaha: Von Riesen und Zwergen Zum Strukturwandel im verbreitenden Buchhandel in Deutschland und Österreich 2011, 24,90 €, ISBN 978-3-940317-93-3  
J. Stiglhuber: Macht und Ohnmacht der Unabhängigen Independent-Verlage und ihre Verortung 2011, 26,90 €, ISBN 978-3-86488-003-2

## **Kleine Schriften**

- M. Pankow: In kurzen Sätzen zur weiten Welt Eine funktionale Analyse des Phänomens Twitter [Softcover] 2010, 12,80 €, ISBN 978-3-940317-65-0  
J.-F. Schrape: Wiederkehrende Erwartungen Visionen, Prognosen und Mythen um neue Medien seit 1970 [Softcover] 2012, 11,90 €, ISBN 978-3-86488-021-6

*weitere Reihen im vwh-Programm  
(s. [www.vwh-verlag.de](http://www.vwh-verlag.de)):*

- Typo|Druck
- AV-Medien
- Multimedia
- E-Business
- E-Collaboration
- E-Humanities
- Schriften des Innovators Club



Aktuelle Ankündigungen, Inhaltsverzeichnisse und Rezensionen  
finden sie im vwh-Blog unter [www.vwh-verlag.de](http://www.vwh-verlag.de).

Das komplette Verlagsprogramm mit Buchbeschreibungen sowie eine direkte Bestellmöglichkeit im vwh-Shop finden Sie unter [www.vwh-verlag-shop.de](http://www.vwh-verlag-shop.de).

## Über dieses Buch

Digitale Forschungsdaten sind eine unverzichtbare Grundlage moderner Wissenschaft. Mit ihnen sind aber eine Reihe von notwendigen Datenmanagement-Aufgaben verbunden, damit sie in der aktiven Forschung bestmöglich eingesetzt werden können und die gute wissenschaftliche Praxis eingehalten wird.

Wie lange sollen die Daten aufbewahrt werden? Welche Kontextinformationen müssen erfasst werden, um die Daten zu einem späteren Zeitpunkt noch sinnvoll benutzen zu können? Wie viel kostet die Aufbewahrung?

Dieses Buch kann diese Fragen nur aufwerfen, nicht beantworten. Denn ohne auf Details der jeweiligen Disziplin, Forschungsdaten und Projekte einzugehen, lassen sich diese Fragen nicht allgemein-verbindlich klären.

Was dieses Buch jedoch mit einem Leitfaden und einer Checkliste bereitstellt, ist ein einfaches Instrument für fachwissenschaftliche oder Infrastruktur-Einrichtungen, um die wichtigsten Aufgaben und Fragen im Forschungsdaten-Management strukturiert beantworten und effizient planen zu können.

## Die Autoren

Harry Enke, Leibniz-Institut  
für Astrophysik Potsdam

Norman Fiedler  
Institut für Deutsche Sprache

Thomas Fischer  
Niedersächsische Staats- und  
Universitätsbibliothek Göttingen

Timo Gnadt  
Niedersächsische Staats- und  
Universitätsbibliothek Göttingen

Erik Ketzan  
Institut für Deutsche Sprache

Jens Ludwig  
Niedersächsische Staats- und  
Universitätsbibliothek Göttingen

Torsten Rathmann  
Deutsches Klimarechenzentrum

Gabriel Stöckle  
Zentrum für Astronomie der  
Universität Heidelberg

Florian Schintke  
Konrad-Zuse-Institut für  
Informationstechnik Berlin

[www.vwh-verlag.de](http://www.vwh-verlag.de)

15,80 € (D)

16,24 € (A)

19,50 CHF

**vwh** Verlag Werner Hülsbusch  
Fachverlag für Medientechnik und -wirtschaft

In Kooperation mit dem  Universitätsverlag Göttingen

ISBN 978-3-86488-032-2



9 783864 880322