

Elisabeth Steiner

Zertifizierung von Repositorien

Handbuch Repositorienmanagement, Hg. v. Blumesberger et al., 2024, S. 369–379
<https://doi.org/10.25364/978390337423220>



Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung 4.0 International Lizenz, ausgenommen von dieser Lizenz sind Abbildungen, Screenshots und Logos.

Elisabeth Steiner, Universität Graz, ZIM-ACDH, elisabeth.steiner@uni-graz.at | ORCID iD: 0000-0001-9116-0402

Zusammenfassung

In einer sich rasant wandelnden digitalen Welt stehen Repositorien für verlässliche und langzeitverfügbare Informationen und Ressourcen, die Forschungsergebnisse transparent und nachvollziehbar machen und so auch als Grundlage für neue wissenschaftliche Forschung dienen. Schon früh wurde der Bedarf für eine Qualitätskontrolle und eine Bescheinigung dieser Stabilität und „Vertrauenswürdigkeit“ erkannt, was sich in unterschiedlichen Zertifizierungsinitiativen niederschlug. Der Beitrag erläutert das Konzept des „Trust“ und gibt einen Überblick über Kriterienkataloge und Zertifizierungsrichtlinien, die besonders im geisteswissenschaftlichen und bibliothekarischen Bereich zur Anwendung kommen.

Schlagwörter: Repository; Zertifizierung; Vertrauenswürdigkeit

Abstract

Certification of Repositories

In a rapidly changing digital world, repositories stand for reliable and long-term available information and resources that make research results transparent and comprehensible, thus serving as a basis for new scientific research. Early on, the need for quality control and certification of this stability and “trustworthiness” was recognized, which was reflected in various certification initiatives. The contribution outlines the concept of “trust” and gives an overview of criteria and certification guidelines that are especially used in the humanities and the library sectors.

Keywords: Repository; certification; trust

1. Einleitung

Repositorien folgen bei der Erfüllung ihrer Aufgaben Richtlinien und Standards. Die theoretische Grundlage des digitalen Archivs bildet das OAIS-Referenzmodell¹. Ergänzend dazu stehen zahlreiche andere Empfehlungen oder Best-Practice-Vorgaben zur Verfügung, die sich auf unterschiedliche Teilbereiche oder praktische Anforderungen beziehen. Dazu zählen beispielsweise die FAIR-Prinzipien², die COAR-Prinzipien³ oder die Empfehlungen von Plan S⁴.

Die Einhaltung solcher Richtlinien kann durch Akkreditierungsgremien in Form einer Zertifizierung bestätigt werden. Bei der Auswahl von Archivierungspartnern durch Forschende oder Fördergeber stellt die unabhängige Bewertung durch eine externe Begutachtung eine wichtige Entscheidungshilfe dar.

Für Repositorien kommen dabei einerseits Verfahren in Frage, die nicht direkt mit der Aufgabe als Repository zusammenhängen, z. B. Zertifikate aus dem Bereich IT-Sicherheit, Datenschutz oder andere Akkreditierungen aus den Normen der International Organization for Standardization (ISO) oder des Deutschen Instituts für Normung (DIN). Andererseits stehen bereits spezielle Verfahren für den Aufgabenbereich von Repositorien und digitalen Archiven zur Verfügung, die der Gegenstand dieses Beitrags sind.

2. Qualitätssicherung für Repositorien

Als exemplarische Möglichkeit zur Qualitätssicherung in Repositorien sei hier das DINI-Zertifikat vorgestellt.

Das DINI-Zertifikat für Open-Access-Publikationsdienste wird von der Deutschen Initiative für Netzwerkinformation e.V. vergeben.⁵ Der Kriterienkatalog legt Mindestanforderungen und Empfehlungen fest, was zur Verbesserung der Infrastruktur und der Qualität sowie zu einer Stärkung des Open-Access-Gedankens führen soll. Das Gütesiegel richtet sich in erster Linie an Repositorien, die elektronische Publikationen zur Verfügung stellen, nicht an Forschungsdatenrepositorien oder virtuelle Sammlungen. Weite Verbreitung findet es daher im Bibliotheksbereich.

-
- 1 The Consultative Committee for Space Data Systems: Reference Model for an Open Archival Information System (OAIS). (2012). Vgl. auch den Beitrag in diesem Band.
 - 2 Wilkinson, M. D. et al. (2016)
 - 3 Confederation of Open Access Repositories: COAR Community Framework for Best Practices in Repositories. (2020)
 - 4 Plan S: Technical Guidance and Requirements, https://www.coalition-s.org/technical-guidance_and_requirements
 - 5 Die Beantragung ist kostenpflichtig und liegt je nachdem, ob die Institution DINI-Mitglied ist oder nicht, bzw. ob sie kommerziell arbeitet oder nicht, zwischen 100 und 500 Euro.

Bisher konnten sich nur deutsche Institutionen zertifizieren lassen, doch mit dem Request for Comments 2022⁶ werden die Richtlinien erstmals für österreichische Institutionen angepasst. Die Kriterien beziehen sich teilweise auf allgemeinere Punkte, z. B., dass eine öffentlich zur Verfügung stehende Policy den Dienst beschreiben soll, andererseits auch sehr konkret auf die Implementierung bestimmter Metadatenstandards und technischer Services. Langzeitarchivierung liegt explizit nicht im Fokus des DINI-Zertifikats, allerdings soll die Mindestverfügbarkeit der Publikationen mit Metadaten fünf Jahre nicht unterschreiten.⁷ Nach Ausfüllen eines Fragebogens werden die Angaben von zwei externen Gutachter:innen überprüft und bei erfolgreicher Evaluierung darf der Dienst das Zertifikatslogo führen und sich als zertifizierter Open-Access-Publikationsdienst bezeichnen.

Ein anderes Beispiel stellt die Akkreditierung von Forschungsdatenzentren durch den Rat für Sozial- und Wirtschaftsdaten (RatSWD) in Deutschland dar. Zentren stellen einen Akkreditierungsantrag, der vom RatSWD geprüft und bei Einhaltung der Standards und Kriterien positiv bewertet wird.⁸

Auf den Aspekt der Vertrauenswürdigkeit wird zwar im DINI-Zertifikat mehrfach hingewiesen, allerdings zielt die Evaluierung nicht primär auf die Bescheinigung dieser Eigenschaft. Zu diesem Zweck stehen andere Verfahren zur Verfügung, die gemeinsam mit dem grundlegenden Konzept der Vertrauenswürdigkeit von digitalen Archiven im Folgenden vorgestellt werden.

3. Das Konzept der Vertrauenswürdigkeit in Repositorien

Bereits bei der Entwicklung des OAIS-Referenzmodells wurde das Konzept der Vertrauenswürdigkeit (engl. trust/trustworthiness) implizit eingebunden. Besonders hervorzuheben ist hier die Verbindung zur Authentizität des (digitalen) Objektes: „Authentizität: Das Ausmaß, in dem eine Person (oder System) ein Objekt als das ansieht, was es vorgibt zu sein. Authentizität wird auf der Basis von Evidenz beurteilt.“⁹

6 Vgl. Becker, P. et al. (2022)

7 Vgl. DINI AG Elektronisches Publizieren (E-Pub) (2019)

8 Zur Akkreditierung siehe hier <https://www.konsortswd.de/datenzentren/akkreditierung>

9 nestor: Referenzmodell für ein Offenes Archiv-Informationssystem. Deutsche Übersetzung 2.0. 2013. (nestor-materialien 16), S. 9.

Im englischen Original: “Authenticity: The degree to which a person (or system) regards an object as what it is purported to be. Authenticity is judged on the basis of evidence.” (The Consultative Committee for Space Data Systems: Reference Model for an Open Archival Information System (OAIS). 2012, <https://public.ccsds.org/pubs/650x0m2.pdf>, S. 1-9).

Ein vertrauenswürdiges Repository stellt seiner Zielgruppe nicht nur digitale Objekte zur Verfügung, sondern gleichzeitig auch die Evidenz, um die Qualität und die Provenienz der Information zu beurteilen. Diese Vertrauenswürdigkeit spiegelt sich auf mehreren Ebenen in Repositorien und unter den beteiligten Akteur:innen, besonders auch mit Hinblick darauf, wie Nutzer:innen (digitalen) Ressourcen vertrauen können: “How users trust the documents provided to them by a repository”¹⁰. Hier sind digitale Anbieter im Vergleich zu etablierten (analogen) Institutionen unter Zugzwang, weil diese bereits Jahrhunderte an ihrer Vertrauenswürdigkeit gearbeitet haben, qualitätssichernde Maßnahmen entwickelt und so das Vertrauen der Zielgruppe erworben haben (z. B. Peer Review). Publiizierte Bücher in Bibliotheken haben in der Regel einen bekannten Prozess von der Entstehung bis zur Publikation und Aufnahme in den Bibliotheksbestand durchlaufen, weshalb Nutzer:innen sich bis zu einem gewissen Grad darauf verlassen können, dass hier eine grundlegende Qualitätskontrolle der Inhalte stattgefunden hat.

In der sich schnell wandelnden digitalen Welt geht diese Vertrauenswürdigkeit wie auch die vertrauten Abläufe der Publikation von Daten bzw. Information verloren. Nutzer:innen fällt es oft schwer, den Überfluss an Information zu selektieren und zu bewerten. Deswegen kommt in der virtuellen Welt dem Erhalt der verlässlichen Erreichbarkeit und Zugänglichkeit (im Sinne der wissenschaftlichen Zitierbarkeit) und der Seriosität (im Sinne der wissenschaftlichen Qualität) besondere Bedeutung zu. Vor allem gilt das für Forschungsdaten im engeren Sinne (Messdaten, Rohdaten etc.) im Vergleich zu Publikationen wie Monographien oder Zeitschriftenartikeln, die auch im digitalen Medium einem ähnlichen Muster folgen wie im vertrauten analogen Umfeld.

Die 2020 publizierten TRUST Principles nehmen das Konzept der Vertrauenswürdigkeit erneut auf und fassen die damit verbundenen Empfehlungen für digitale Archive plakativ zusammen¹¹:

10 Research Libraries Group (RLG): Trusted Digital Repositories: Attributes and Responsibilities. (2002), S. 9.

11 Lin, D. et al. (2020)

Principle	Guidance for repositories
Transparency	To be transparent about specific repository services and data holdings that are verifiable by publicly accessible evidence.
Responsibility	To be responsible for ensuring the authenticity and integrity of data holdings and for the reliability and persistence of its service.
User Focus	To ensure that the data management norms and expectations of target user communities are met.
Sustainability	To sustain services and preserve data holdings for the long-term.
Technology	To provide infrastructure and capabilities to support secure, persistent, and reliable services.

Transparenz, Verantwortung, Zielgruppenorientierung, Nachhaltigkeit und Technologie bilden demnach die Grundpfeiler von vertrauenswürdiger Repositorienarbeit. Mit der Erwähnung der Authentizität und dem Fokus auf die Nutzungsgruppe finden Konzepte aus dem OAIS-Referenzmodell erneut Verwendung. Doch wie können Repositorien dieses Vertrauen (*trustworthiness*) in ihre Ressourcen und ihre Institution unter Beweis stellen?

3.1. Trusted Digital Repositories

Die Research Libraries Group (RLG) stellte mit ihren Attributes and Responsibilities¹² den ersten Kriterienkatalog für vertrauenswürdige digitale Repositorien vor. Darauf folgten weitere Initiativen, die auch die Formalisierung dieser Richtlinien als Zertifizierungen verfolgten.

Im deutschsprachigen Raum wurde ab 2004 vom Kooperationsverbund nestor ein Kriterienkatalog entwickelt, der in der Entwicklung der DIN-Norm 31644 „Kriterien für vertrauenswürdige digitale Langzeitarchive“ resultierte.¹³

Aufbauend auf den Überlegungen von RLG und nestor wurde 2007 vom Online Computer Library Center (OCLC) und vom Center for Research Libraries (CRL) die Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC)¹⁴ vorgestellt. Fortgesetzte Arbeit mündete schließlich in die Publikation des ISO-Standards 16363.

12 RLG: Trusted Digital Repositories (Anm. 8).
13 nestor: nestor-Kriterienkatalog vertrauenswürdige digitale Langzeitarchive, Version 2. 2008. (nestor-materialien 8); nestor-Siegel für vertrauenswürdige digitale Langzeitarchive https://www.langzeitarchivierung.de/Webs/nestor/DE/Zertifizierung/nestor_Siegel/siegel.html
14 OCLC and CRL (2007)

Im europäischen Raum etablierte sich mit der Veröffentlichung des Data Seal of Approval in den Niederlanden eine weitere Möglichkeit zum Nachweis der Vertrauenswürdigkeit. 2017 fusionierte das vom Data Archiving and Networked Services (DANS) vergebene Siegel mit der WDS Regular Member Certification (seit 2011 vom World Data System Scientific Committee vergeben) zum CoreTrustSeal.¹⁵

Im Gegensatz zu den genannten Ansätzen zählt die Methode Digital Repository Audit Method Based on Risk Assessment (DRAMBORA)¹⁶ nicht zu den Kriterienkatalogen, sondern versucht, in einem Risikomanagement-Prozess Gefahrenpotential für Archive und die darin gespeicherte Information aufzufinden und zu beherrschen.

Die meisten Kriterien in den genannten Anforderungskatalogen beziehen sich auf die Organisation, Dokumentation, Arbeitsabläufe und -prozesse und Transparenz im Repository und nicht, wie häufig angenommen, auf konkrete technische Umsetzungsfragen.¹⁷ Die Richtlinien unterscheiden sich teilweise in Umfang, Aufbau und Evaluierung, wenn sie auch die gleichen Ziele verfolgen; so evaluiert beispielsweise das CoreTrustSeal 16 Kriterien, das nestor Siegel 34, ISO 16363 über 100.

2010 einigten sich die führenden Anbieter der Repositorienzertifizierung in einem Memorandum of Understanding auf ein gemeinsames Stufenmodell. Das Ergebnis besteht aus drei Zertifizierungsschritten¹⁸:

- Basic Certification
CoreTrustSeal (self audit)
- Extended Certification
Basic + ISO 16363/DIN 31644 (self audit)
- Formal Certification
Basic + ISO 16363/DIN 31644 (external audit)

Das CoreTrustSeal bietet den Einstieg für die meisten Repositorien, die sich erstmals als vertrauenswürdig zertifizieren lassen. Der Bearbeitungsaufwand für den Zertifizierungsprozess steigt je nach Stufe, mittlerweile werden auch für die Begutachtung in den selbstevaluierenden Verfahren (zwei externe Gutachter:innen pro

15 Core Trust Seal <http://coretrustseal.org>

16 DCC and DPE: Digital Repository Audit Method Based on Risk Assessment (DRAMBORA); Donnelly, M. et al. (2009)

17 Zu solchen Fragen gibt es jedoch ebenfalls Empfehlungen, wie z. B.: Confederation of Open Access Repositories: COAR Community Framework for Best Practices in Repositories (2020), oder die Vision der COAR Next Generation Repositories in Rodrigues, E. et al. (2017).

18 Siehe <http://www.trusteddigitalrepository.eu>

Antrag) Gebühren erhoben.¹⁹ Eine öffentlich zugängliche (am besten englische) Dokumentation bildet die Grundlage für die durchgeführte Peer Review. Der interne Aufwand umfasst daher nicht nur die direkte Beantwortung der Fragen im Kriterienkatalog, sondern besonders die Herstellung der dafür notwendigen Voraussetzungen; dies reicht von der Erstellung entsprechender Dokumentation, Übersetzung von bestehenden Dokumenten bis hin zu Abstimmungsarbeit innerhalb des Repositoriums wie auch oft mit anderen Abteilungen (Rechtsabteilung, IT-Services, Forschungsmanagement etc.). Eine erfolgreiche Zertifizierung berechtigt zum Führen eines entsprechenden Nachweises auf der eigenen Webpräsenz (Logo), wie auch zur Aufnahme in die Liste des jeweiligen Zertifizierungsgremiums. In Verzeichnissen für Forschungsdatenrepositorien (Registries wie z. B. re3data.org²⁰ oder OpenDOAR²¹) wird die Zertifizierung ebenso gesondert als Kriterium erfasst. Beispielsweise führt re3data.org mit Stichtag 10.6.2022 41 Repositorien in Österreich, Open DOAR 48; davon verfügen drei über das CoreTrustSeal. Die Zertifizierungen tragen üblicherweise ein Ablaufdatum, so erwartet das CoreTrustSeal eine erneute Zertifizierung nach drei Jahren. Dies spiegelt die sich ständig verändernden Rahmenbedingungen von digitalen Repositorien wider und versteht Qualitätskontrolle und Vertrauenswürdigkeit als iterative Prozesse, die kontinuierliche Aufmerksamkeit benötigen.

Derzeit verlangen die Zertifizierungsrichtlinien die Festlegung auf eine Zielgruppe, d. h. generalisierte Repositorien²² (z. B. Zenodo, Figshare, OSF etc.) fallen per Definition aus dem Fokus, obwohl einige von ihnen die Kriterien erfüllen könnten. Trotz bisher noch fehlender offizieller Zertifizierung können solche Anbieter eine gute Alternative sein, wenn auch die Unterstützung beim Forschungsdatenmanagement und fachspezifische Harmonisierung und Optimierung definitiv verloren gehen. Dieser Gesichtspunkt wird beim CoreTrustSeal unter dem Stichwort *level of curation* erfasst: Findet eine Kuratierung der Daten vor dem Abspeichern statt und in welchem Umfang? Je höher die Stufe der Kuratierung, desto höher die Datenqualität²³.

19 CoreTrustSeal: EUR 3.000, nestor Siegel: EUR 500.

20 re3data.org, Registry of Research Data Repositories <https://www.re3data.org>

21 OpenDOAR, Directory of Open Access Repositories <https://v2.sherpa.ac.uk/pendoar>

22 Für eine Auflistung mit Vergleich der wichtigsten Eigenschaften siehe Stall, S. et al. (2020).

23 Beispielsweise mit Hinblick auf die FAIRness der Daten, vgl. dazu die Beiträge in diesem Band.

4. Vorteile und Herausforderungen für Forschende und Institutionen

Für Forschende sind die oben genannten Verzeichnisse für Repositorien oft die erste Anlaufstelle, wenn sie nach Archivierungspartnern suchen. In der Forschungsförderung wird mittlerweile die Ablage der Daten in einem Repository verlangt bzw. in einem zertifizierten Repository empfohlen.²⁴ So wird die nachhaltige Verfügbarkeit der öffentlich geförderten Daten und Ergebnisse sichergestellt und diese stehen Forschenden für aufbauende Studien zur Verfügung.

Die Vorteile der Zertifizierung von Repositorien für Forschende und Fördergeber liegen damit auf der Hand. Doch warum sollten sich Repositorien einer solchen Prozedur unterziehen? Immerhin kostet die Zertifizierung Geld, nicht nur in Form von direkten Gebühren, sondern auch in Form von Personal, das die Zertifizierung durchführt und entsprechende Dokumentation verfasst und Arbeitsabläufe anpasst; so können je nach Ausgangslage durchaus aufwändige Änderungen notwendig sein. Jedoch bietet die Zertifizierung die Möglichkeit, den aktuellen Stand im Repository zu evaluieren und Verbesserungspotential zu erkennen. Das wird durch die externe Review erleichtert, da mit Hinblick auf das eigene Repository eine gewisse „Betriebsblindheit“ auftreten kann. Gerade für die Dokumentation und Standardisierung von Arbeitsprozessen kann diese Perspektive sehr wertvoll sein. Zusätzlich zu diesem (nicht monetär bezifferbaren) Vorteil führt eine erfolgreiche Zertifizierung in der Regel zu einer höheren nationalen und internationalen Sichtbarkeit des Repositoriums, was wiederum zu besserer Finanzierung und erhöhter Projektauslastung führen kann.²⁵

5. Fazit

Die Zertifizierung als vertrauenswürdiges digitales Repository bringt allen Beteiligten durchwegs Vorteile. Die dadurch hergestellte Transparenz und Nachvollziehbarkeit verbessert die Qualität der Forschungsdaten, ausreichende Dokumentation fördert die Verständlichkeit und Weiterverwendbarkeit (Stichwort FAIR Data, Open Access und Open Science). Repositorien können so optimal ihre Funktion in der Unterstützung von wissenschaftlicher Forschung und Lehre wahrnehmen. Voraussetzung für die Zertifizierung und den Betrieb eines Repositoriums insgesamt bleibt die ausreichende organisatorische und damit auch finanzielle Selbstverpflichtung

24 Siehe z. B. die Open-Access Policy des FWF: <https://www.fwf.ac.at/ueber-uns/aufgaben-und-aktivitaeten/open-science/open-access-policy>

25 Zu den Vorteilen der Zertifizierung für die Repositorien vgl. weiterführend Donaldson, D. R. et al. (2017), S. 130-151.

der betreibenden Institution. Repositorien sollten sich hier in ein Gesamtkonzept für Forschungsdatenmanagement einfügen, das Forschenden idealerweise über den gesamten Datenlebenszyklus hinweg Unterstützung bietet. Diese Funktion wird mehr und mehr von Data Stewards erfüllt, die das Bindeglied zwischen Forschenden und Forschungsinfrastruktur bilden. Nur nach Ende des Projektes einen Speicherort mit persistenter Identifikation zur Verfügung zu stellen, scheint hier zu kurz gegriffen: eine fachspezifische Datenmanagementbegleitung des gesamten Forschungsprozesses wäre der vielversprechendste Lösungsweg²⁶.

Bibliografie

- Becker, Pascal; Beucke, Daniel; Blumtritt, Ute et al. (2022): DINI-Zertifikat für Open-Access-Publikationsdienste 2022 – Request for Comments. <https://doi.org/10.5281/zenodo.6389914>
- cOAlition S: Plan S Principles and Implementation. Part III: Technical Guidance and Requirements. https://www.coalition-s.org/technical-guidance_and_requirements (abgerufen am 10.06.2022)
- Confederation of Open Access Repositories (2022): COAR Community Framework for Best Practices in Repositories. <https://doi.org/10.5281/zenodo.4110829>
- The Consultative Committee for Space Data Systems (2012): Reference Model for an Open Archival Information System (OAIS). <https://public.ccsds.org/pubs/650x0m2.pdf> (abgerufen am 10.06.2022)
- DCC and DPE: Digital Repository Audit Method Based on Risk Assessment (DRAMBORA). <https://www.repositoryaudit.eu> (abgerufen am 10.06.2022)
- DINI AG Elektronisches Publizieren (E-Pub) (2019): DINI-Zertifikat für Open-Access-Publikationsdienste. Version 6.0. 2019. <http://dx.doi.org/10.18452/20545>
- Donaldson, Devan Ray; Dillo, Ingrid; Downs, Robert; Ramdeen, Sarah (2017): The Perceived Value of Acquiring Data Seals of Approval. In: *International Journal of Digital Curation* 12, pp. 130-151. <https://doi.org/10.2218/ijdc.v12i1.481>
- Donnelly, Martin; Innocenti, Perla; McHugh, Andrew; Ruusalepp, Raivo (2009): DRAMBORA Interactive. User Guide. https://www.dcc.ac.uk/sites/default/files/DRAM-BORA_Interactive_Manual%5B1%5D.pdf (abgerufen am 10.06.2022)
- Gänsdorfer, Nikos (2020): Gespräche mit Data Stewards. Anforderungen, Kompetenzen, Aufgaben. <https://doi.org/10.25365/phaidra.241>
- Lin, Dawei; Crabtree, Jonathan; Dillo, Ingrid et al. (2020): The TRUST Principles for Digital Repositories. In: *Scientific Data* 7, p. 144. <https://doi.org/10.1038/s41597-020-0486-7>
- Keitel, Christian; Schoger, Astrid et al. (Hg.) (2013): Vertrauenswürdige digitale Langzeitarchivierung nach DIN 31644. Berlin/Wien/Zürich: Beuth.

26 Diese Feststellung trifft auch Gänsdorfer in seiner Studie zu Data Stewardship in Österreich, vgl. Gänsdorfer, N. (2020)

- Nestor (2008): nestor-Kriterienkatalog vertrauenswürdige digitale Langzeitarchive. Version 2. (nestor-materialien 8). <http://nbn-resolving.de/urn:nbn:de:0008-2008021802>
- Nestor (2013): Referenzmodell für ein Offenes Archiv-Informationen-System. Deutsche Übersetzung 2.0. (nestor-materialien 16). <http://nbn-resolving.de/urn:nbn:de:0008-2013082706>
- OCLC and CRL (2007): Trustworthy Repositories Audit & Certification. Criteria and Checklist. https://www.crl.edu/sites/default/files/d6/attachments/pages/trac_0.pdf (abgerufen am 10.06.2022)
- Research Libraries Group (RLG) (2002): Trusted Digital Repositories: Attributes and Responsibilities. Mountain View, California: RLG. <http://www.oclc.org/research/activities/past/rlg/trustedrep/repositories.pdf> (abgerufen am 10.06.2022)
- Rodrigues, Eloy; Bollini, Andrea; Cabezas, Alberto et al. (2017). Next Generation Repositories. Behaviours and Technical Recommendations of the COAR Next Generation Repositories Working Group. <https://doi.org/10.5281/zenodo.1215014>
- Stall, Shelley; Martone, Maryann E.; Chandramouliswaran, Ishwar et al. (2020): Generalist Repository Comparison Chart. <https://doi.org/10.5281/zenodo.3946720>
- Wilkinson, Mark. D.; Dumontier, Michel; Aalbersberg, IJsbrand Jan et al. (2016): The FAIR Guiding Principles for Scientific Data Management and Stewardship. In: Scientific Data 3, 160018. <https://doi.org/10.1038/sdata.2016.18>

Elisabeth Steiner studierte Linguistik, Germanistik und Digital Humanities in Graz (AT), Aarhus (DK) und Köln (DE). Seit 2012 verstärkt sie das Team des ZIM-ACDH an der Universität Graz in den Bereichen Metadatenmanagement und Repositorienmanagement. Sie beschäftigt sich dabei praktisch und theoretisch mit der Langzeitarchivierung und -verfügbarkeit von geisteswissenschaftlichen Forschungsdaten und lehrt zu diesen Themengebieten.