Handlungsfelder der Datengovernance

CUT | M1 | Juni 2022

Partnerstädte:

Hamburg

Stadt Leipzig

Landeshauptstadt München

Gefördert durch:

Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen

KFW

Versionierung

Version	Erläuterung	Datum der Änderung
V1.0	Erste Definition der Handlungsfelder	30.06.2022

Inhalt

1 Einleitung

Die Digitalisierung greift tief und umfassend in die bestehenden gesellschaftlichen Prozesse und in die Verwaltungsprozesse ein, von denen die Stadtgesellschaft insgesamt betroffen ist. Die Städte erkennen die zentrale Bedeutung der Digitalisierung und des Potentials der Daten für die Stadtverwaltung selbst wie auch für die Stadtgesellschaft. Die sich hier ergebenden Chancen müssen unter Beachtung der inhärenten Risiken einer datengetriebenen oder datenzentrischen Sicht ausgelotet und nutzbringend ergriffen werden. Trotz der zentralen Rolle der Daten ist ihr Potential in der Stadtverwaltung uneinheitlich und teilweise erst rudimentär erschlossen. Es ist notwendig eine Datengovernance mit Prinzipien und Handlungsfeldern zu etablieren, um den Umgang mit Daten stadtweit kohärent zu organisieren. Beim Aufbau einer Datengovernance identifizieren wir folgende Chancen:

- Zentraler und einfacher Zugang zu städtischen und kommunalen Daten
- Effektive Regeln zur Gewährleistung von Datenschutz und Datensicherheit
- Effizientere Verwaltungsvorgänge mit erhöhtem Mehrwert für die Stadtgesellschaft
- Neue Möglichkeiten zum partizipativen Mitgestalten und datengestützten Entscheiden
- Schaffung neuer Strukturen für die nachhaltige Stadtentwicklung und innovative Geschäftsmodelle
- Positionierung im internationalen Wettbewerb um Unternehmen und Köpfe

Gleichzeitig müssen wir folgenden Herausforderungen begegnen:

- Umgang mit umfangreichen Datenschutz- und Datensicherheitsregularien
- Klärung von unklaren Besitzverhältnissen und Nutzungsbedingungen von Daten
- Datensilos öffnen und Daten zugänglich machen
- Sicherung der Datenqualität inklusive Vermeidung redundanter Daten
- Umgang mit Daten ohne Aussagekraft und missverständlichen Daten
- Fehlende oder inkompatible Standards und Definitionen
- Unterschiedliche Interpretation von Daten

1.1 Ziel des Dokuments

Dieses Dokument dient einer ersten Orientierung im komplexen Thema Datengovernance für Städte und Kommunen. Hierfür wurden die Handlungsfelder der Datengovernance in Kurztexten definiert, um u.a. ein gemeinsames Verständnis der Begriffe zu erlangen. Die Inhalte wurden im Projekt Connected Urban Twins zwischen den Projektstädten Hamburg, Leipzig und München unter Einbezug von lokalen Datengovernance-Expert/-innen abgestimmt. Das Dokument bildet die Grundlage für eine tiefergehende Betrachtung einzelner, anwendungsfallbezogener Handlungsfelder, Formulierung von Empfehlungen und der Dokumentation von Best Practice Beispielen.

1.2 Prinzipien

Unser Handeln im Rahmen der Maßnahmen der Digitalisierung allgemein und im Themenfeld der Daten und der Datengovernance speziell wird von Zielkonflikten begleitet werden, die eine besondere Sorgfalt beim Umgang mit und bei der Formulierung von Datenthemen erfordern. Geleitet werden wir hier von Prinzipien, die wir nach Maßgabe der breiten Erfahrungen aus der Digitalisierung als Grundlage für unsere Entscheidungen im Kontext der Datengovernance heranziehen wollen. Alle unsere Ziele und Maßnahmen orientieren sich daran.

Wir unterscheiden zwei Arten von Prinzipien, zum einen allgemeine **strategische Prinzipien** der Digitalisierungs- und Datenstrategie, die einen Rahmen für die Umsetzung der (digitalen) Verwaltungsleistungen bilden, und zum anderen spezifische **Funktionsprinzipien** für (digitale) Verwaltungsleistungen. Die strategischen Prinzipien bilden einen Rahmen bei der Digitalisierung und beim Umgang mit Daten, gegen den alle Handlungen bei der Umsetzung standhalten müssen. Die spezifischen Funktionsprinzipien bilden ein konkretes Ziel ab, das in funktionalen Teilbereichen wirkt. Die Funktionsprinzipien müssen naturgemäß auch den strategischen Prinzipien genügen.

Zu den strategischen Prinzipien der Digitalisierung zählen wir die Informationssicherheit und den Datenschutz, die Digitale Souveränität, Offenheit und Transparenz, die Nutzung und Einhaltung von Standards, die Nachhaltigkeit aller Aktivitäten bei der Umsetzung der Digitalisierung und der Praxis der Leistungen im Betrieb, ferner die Gleichstellung, Inklusion, Diskriminierungs- und Barrierefreiheit, und schließlich die Orientierung allen Verwaltungshandelns am Nutzen für Kunden, Kundinnen und der Stadtgesellschaft insgesamt.

Funktionsprinzipien sind beispielsweise die Datenvermeidung (als Teil des Datenschutzes), eine datenzentrische Sicht (ein Betrachtungsprinzip für das Vorgehen bei der Annäherung an eine Lösung), Once-Only (ein Merkmal und Prinzip der Qualität für die Leistungen für die Stadtgesellschaft), Open by Default (das Grundsatzprinzip, dass Daten nicht schon im Vorhinein als Geheimnis angesehen werden, sondern grundsätzlich verfügbar gemacht werden sollen) und der Datenschutz by Design (der Entwurf von Leistungen in einer Weise, dass der Datenschutz schon während der Konzeptionierung inhärenter Bestandteil der Umsetzung und der Lösung ist).

2 Ethische Rahmenbedingungen für den Umgang mit Daten

Begriffsannäherung: Was Datenethik (nicht) ist und Datenethik als Teil der Datengovernance

Ethik versucht, „das Gute" an Kriterien festzumachen und Prinzipien des guten Handelns zu formulieren. Dabei hinterfragt Ethik einerseits, welche moralischen Ansichten wann und warum gelten, und sie reflektiert andererseits im rechtsphilosophischen Sinne auch die Legitimität der Rechtsgeltung. Ethik darf jedoch weder mit Moral noch mit Rechtmäßigkeit (Legalität) gleichgesetzt werden. In der Angewandten Ethik wird das beschriebene Vorgehen auf konkrete Handlungsfelder (hier: Datengovernance bzw. den Umgang mit Daten) bezogen. „Datenethik" ist eine Spielart der Angewandten Ethik und hinterfragt sowohl unser moralisches Handeln und moralische Urteile als auch unseren rechtlichen Rahmen beim Umgang mit Daten.

Dafür können wesentliche Prinzipien[1] definiert werden, aus denen sich Anforderungen[2] an den Umgang mit Daten ableiten lassen.

Gesetzgebung ist eines von mehreren Instrumenten (wie bspw. Dialog- und Schulungsformate, Entwicklung von Templates zur Anwendung in konkreten Projekten oder Use Cases), um ethische Prinzipien zu implementieren. Die Komplexität und Dynamik von Datenökosystemen erfordern jedoch das Zusammenwirken verschiedener Governance-Instrumente auf unterschiedlichen Ebenen (politisch, operativ und strategisch), um einen ethisch ausreichend reflektierten und gut begründbaren Umgang mit Daten sicherzustellen.

[1] Die Datenethikkommission des Bundes bspw. formuliert folgende wesentliche Prinzipien : (1) Menschenwürde, (2) Selbstbestimmung, (3) Privatheit, (4) Sicherheit, (5) Demokratie, (6) Gerechtigkeit, (7) Nachhaltigkeit (https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6, letzter Zugriff: 30.06.2022)

[2] Diese Anforderungen lassen sich daraus u.a. ableiten: (1) Achtung der Rechte beteiligter Personen, (2) vorausschauende Verantwortung, (3) Wohlfahrtssteigerung durch Teile und Nutzen von Daten, (4) Zweckadäquate Datenqualität, (5) Risikoadäquate Informationssicherheit, (6) Interessenadäquate Transparenz.

3 Rollen

Im Rahmen der Ausgestaltung der Datengovernance im **gesamtstädtischen Kontext** werden auch Ansprechpersonen in den Behörden und Ämtern benötigt, die bei datenbezogenen Fragen eingebunden werden können. Für die Rollenzuordnungen ist es wichtig, dass die fachliche, strategische und technische Ebene berücksichtigt wird.

Unabhängig von schon etablierten (Daten-)Schnittstellen kann beispielsweise über folgende Rollenzuordnungen eine Konkretisierung erfolgen:

- wer bei datenbezogenen Fragestellungen in einer Organisation die Verantwortung trägt (Data Owner),
- wer ein fachlicher Multiplikator und Vernetzer ist und die Umsetzungsverantwortung trägt (Data Steward),
- wer für operative Fragestellungen ansprechbar ist (Data Manager).

Wichtig ist, dass dieser gesamtstädtische Kontext im Folgenden auf den CUT-Kontext angepasst wird.

4 Datentransparenz

Die Datentransparenz ist eine sowohl fachliche als auch technische Spezialisierung[3] der Verwaltungstransparenz und leitet sich aus dem strategischen Transparenz-Prinzip als eine Konkretisierung ab. Die Datentransparenz ist zunächst verwaltungsintern sicherzustellen; Kenntnisse der eigenen Daten ermöglichen es sowohl Anforderungen z.B. aus gesetzlichen Vorgaben (wie dem Once-Only-Prinzip) zu erfüllen als auch die Grundlagen für ein Data Driven Government herzustellen. Da aus Daten Informationen abgeleitet werden und Informationen zum Wissen über Sachverhalte führt, ist die Datentransparenz eine grundlegende Voraussetzung, um der Stadtverwaltung selbst, aber auch den Stakeholdern der Stadt zur Erreichung ihrer Ziele zu dienen. Verwaltungsintern können hier durch Kenntnis der bestehenden Daten und deren Austausch zwischen den Organisationseinheiten bestehende Dienste[4] verbessert und neue Dienste geschaffen werden[5]. Kundinnen, Kunden und Unternehmen können über Ihre Anträge und Rahmenbedingungen Information erhalten, und die Stadtgesellschaft insgesamt kann über die Transparenz wertvoller Stadtdaten neue Erkenntnisse gewinnen oder ableiten und neue Geschäftsmodelle entwickeln, welche die Stadt mit ihrer Stadtgesellschaft insgesamt weiterbringt. Die Datentransparenz kann weiter konkretisiert werden, z.B. im Kontext von Open Data durch das Funktionsprinzip Open by Default. Die Datentransparenz muss sich dennoch substanziell auch immer am Rahmen der strategischen Grundprinzipien orientieren, insbesondere an den Anforderungen, die sich aus den Datenschutzbestimmungen und den Anforderungen an die Sicherheit ergeben, und sie wird durch diese Prinzipien fallspezifisch auch eingeschränkt. Typische Werkzeuge, die eine Datentransparenz unterstützen oder in der Praxis gar erst ermöglichen, sind beispielsweise Datenkataloge, Plattformen für Open Data oder Digitale Zwillinge, virtuelle Abbilder der Stadt, anhand der sie beschreibenden Daten.

[3] Die fachliche Transparenz bezieht sich auf übergeordnete Informationen zu Datensätzen oder Prozessen, z.B. den Bearbeitungsstand eines Prozesses. Unter den technischen Aspekt der Transparenz fallen Maßnahmen und Strukturen, die den Zugriff auf Daten ermöglichen bzw. vereinfachen, beispielsweise die Anbindung von IoT-Daten.
[4] Dienste können sowohl technische Dienste als auch Verwaltungsdienste sein.
[5] Beispiele hierfür sind die Zusammenführung und Vereinheitlichung von inkohärenten Datensätzen innerhalb der Verwaltung oder eine zentrale Datenabfrage nach DSGVO von dezentral organisierten Daten.

5 Datenqualität

Daten sind die essenzielle Grundlage moderner Technologien, zahlreicher Dienstleistungen und Geschäftsmodelle. Unabhängig wofür sie eingesetzt werden, ist die Qualität der Daten und Metadaten[6] von zentraler Bedeutung. Sie werden als qualitativ hochwertig angesehen, „wenn sie für ihren vorgesehenen Gebrauch im operativen Geschäft, bei Entscheidungen und bei der Planung geeignet sind“[7]. Je nach Domäne [8], Verwendungskontext, Struktur, Inhalt und Vorwissen der Datennutzer können Daten verschiedene Merkmale aufweisen, die ihre Qualität beeinflussen. Dies umfasst u.a. das Datenformat (z.B. offen, maschinenlesbar), sowie vor allem die semantische und strukturelle Gestaltung der Daten.

Grundlage für die Steigerung der Datenqualität ist eine Erfassung des Status quo, darauf aufbauende gezielte Maßnahmen, sowie die erneute bzw. kontinuierliche Bewertung der Datenqualität. Zur Bewertung der Datenqualität auf der Ebene von Datensatz (z.B. Tabelle) und/oder Attribut können z.B. die folgenden 11 Kriterien[9] herangezogen werden:

- Vollständigkeit
- Eindeutigkeit
- Korrektheit
- Aktualität
- Genauigkeit
- Konsistenz
- Redundanzfreiheit
- Relevanz
- Einheitlichkeit
- Zuverlässigkeit
- Verständlichkeit

Die Auswahl der Bewertungskriterien ist dabei abhängig vom Verwendungskontext der Daten. Für Metadaten, also Daten über Daten, können ähnliche Bewertungskriterien herangezogen werden. Folgende Kriterien können beispielweise verwendet werden: Vollständigkeit, Genauigkeit, Herkunft, Erwartungen, Konsistenz/Kohärenz, Aktualität. Die Verwendung von detailliert ausspezifizierten Metadatenstandards wie DCAT-AP.de[10] oder INSPIRE[11] bietet ein Grundgerüst zur Orientierung und erleichtert somit die Erstellung und Pflege von Metadatensätzen.

---

[6] https://cdn0.scrvt.com/fokus/551bf951bf1982f5/0c96fbf464ef/NQDM_Leitfaden_2019.pdf

[7] Europäische Kommission (2013): Die Qualität von offenen Daten und Metadaten. https://www.europeandataportal.eu/sites/default/files/d2.1.2_training_module_2.2_open_data_quality_de_edp.pdf (Letzter Zugriff: 30.06.2022)

[8] Fachgebiet/Wissensgebiet

[9] Datenqualität messen: Mit 11 Kriterien Datenqualität quantifizieren https://www.business-information-excellence.de/datenqualitaet/86-datenqualitaet-messen-11-datenqualitaets-kriterien (Letzter Zugriff: 30.06.2022)

[10] https://www.dcat-ap.de/def/dcatde/2.0/spec/specification.pdf (Letzter Zugriff: 30.06.2022)

[11] https://inspire.ec.europa.eu/documents/inspire-metadata-implementing-rules-technical-guidelines-based-en-iso-19115-and-en-iso-1 (Letzter Zugriff: 30.06.2022)

6 Datenklassifikation

Von einer Datenklassifikation sprechen wir im Kontext der Datengovernance, um auf die gleichartige oder eine besondere Behandlung von Daten einer Art hinzuweisen und auch eine korrekte und angemessene automatisierte Behandlung der Daten zu ermöglichen. Die Klassifikation von Daten kann entsprechend Kategorien vorgenommen werden, die fachlich, technisch, rechtlich oder organisatorisch motiviert sein können.

Eine fachliche Kategorie könnte Daten kritischer Infrastrukturen identifizieren, die nur in besonderen Anwendungs- oder Organisationskontexten genutzt werden dürfen. Technisch können beispielsweise quasi-statische Stammdaten[12] von Echtzeitdaten unterschieden werden. Im Rahmen einer rechtlichen Einordnung könnten entsprechend der DSGVO schutzwürdige personenbezogene Daten identifiziert werden oder entsprechend der PSI-Richtlinie wertvolle Daten festgelegt sein, für die Veröffentlichungspflichten bestehen. Organisatorisch können Daten nach Eigentümerschaft/Datenhoheit oder Lizenz- und Nutzungsrechten differenziert werden.

Idealerweise werden die Informationen über die Datenklassifikation als Merkmale der Metadaten zusammen mit den eigentlichen Datensätzen aus derselben Datenquelle abgefragt. Üblicherweise werden für die Speicherung dieser Metadaten (Meta-)Datenkataloge eingesetzt.

[12] Stammdaten repräsentieren Grundinformationen über relevante Objekte einer Organisation (z.B. Kunden, Personal oder Produkte) und ändern sich nur selten (beispielsweise die Anschrift eines Mitarbeiters).

7 Datenkompetenz

Sowohl das Bereitstellen als auch verschiedene Formen der Nutzung von Daten erfordern Kompetenzen im Umgang mit Daten und Metadaten. Die Datenkompetenz der Bereitsteller/-innen von Daten und (primär der internen) Nutzer/-innen sollte daher mit verschiedenen Maßnahmen aufgebaut und gefördert werden. Diese Anspruchsgruppen sollten im Umgang mit Daten befähigt und für wichtige Aspekte sensibilisiert werden. Einerseits betrifft das konkret die zielgruppengerechte Aufbereitung und Vermittlung der durch die Datengovernance festgelegten Inhalte wie Rollen, Regeln, Strukturen, Kategorien, Techniken und Abläufe im Umgang mit Daten der Urbanen Datenplattformen. Maßnahmen können beispielsweise die Bereitstellung eines gemeinsamen Glossars für Fachvokabular oder die Erstellung von anschaulichen Schulungs- und Informationsmaterialien, (digitalen) Handbüchern[13] und Wizards[14] umfassen. Darüber hinaus kann angestrebt werden, Datenkompetenz in einem globaleren Sinne (Data Literacy[15]) als Bildungsziel für die Stadtgesellschaft zu fördern.

[13] Vgl. https://berlinonline.github.io/open-data-handbuch/ (Letzter Zugriff: 30.06.2022)
[14] gemeint sind Software-Assistenten
[15] „Die Fähigkeit, Daten auf kritische Art und Weise zu sammeln, zu managen, zu bewerten und anzuwenden" (Ridsdale et al., 2015). Siehe Framework für Data Literacy des Hochschulforums Digitalisierung 2019: http://dx.doi.org/10.1007/s11943-019-00261-9 (Letzter Zugriff: 30.06.2022)

8 (Rechtliche) Vorgaben

Regeln, Modelle und Muster können in standardisierter oder rechtlich verbindlicher Form verwendet werden. D.h. (rechtliche) Vorgaben können Standards und gesetzliche Vorschriften implementieren.

Dies wird durch die Einführung und Verwendung von Regeln oder Modellen, bzw. –Mustern erreicht, z.B.:

- Regeln zu Datenaustausch / Datenbereitstellung zwischen Akteuren
- Regeln zur Datenerfassung
- Regeln zur Datennutzung (Nutzungsbedingungen)
- Muster / Verträge / Vorgehensmodelle / Handlungsleitfaden / Entscheidungshilfen
- Verwendung von Referenzmodellen (z.B. DIN SPEC)
- Verwendung von fachlichen und technischen (Meta-)Datenstandards (z.B. ALKIS, XBAU, DCAT-AP)

9 Prozesse

Im Kontext der Daten haben wir in der Verwaltung mit zwei Arten von Prozessen zu tun, allgemeine, fachliche digitale Verwaltungsprozesse und spezielle Datengovernance-Prozesse.

Die Verwaltungsprozesse haben einen unmittelbaren Bezug zu den Daten, mit denen sie umgehen; Daten werden durch die Verwaltungsprozesse aus Datenquellen abgefragt und über Kommunikationskanäle empfangen, sie werden verarbeitet und dargestellt, sowie am Ende gespeichert und an Folgeprozesse weitergegeben. Es ist von Bedeutung, den engen Zusammenhang zwischen Daten und Prozessen zu erkennen, und diesen z.B. auch im Rahmen des Geschäftsprozessmanagements als inhärenten Bestandteil zu berücksichtigen.

Für ein professionelles Datenmanagement sind neben den fachlichen Prozessen die speziellen Datengovernance-Prozesse zu identifizieren. Hierzu zählen anlassbezogene Datengovernance-Prozesse, beispielsweise die Prüfung neuer Anwendungsfälle hinsichtlich ihrer Relevanz für eine Datengovernance oder die Umsetzung von Anforderungsänderungen an Datenobjekten, ebenso wie übergreifende Datengovernance-Prozesse, z.B. die Definition von Datenqualitäts-Metriken oder die Definition der Aufgaben und Rechte der Datengovernance-Rollen.

10 Datenschutz

Unter Datenschutz wird primär der Schutz personenbezogener Daten vor missbräuchlicher Verwendung und Datenverarbeitung verstanden. Der Datenschutz besteht in der Erklärung der Schutzwürdigkeit von Daten und der Umsetzung von Datenschutzmaßnahmen.

Den rechtlichen Rahmen für das Thema Datenschutz in einer Stadt oder Kommune bildet auf europäischer Ebene die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, DSGVO[16]). Darüber hinaus gelten ergänzende allgemeine sowie bereichsspezifische Datenschutzvorschriften des Bundes (z.B. Bundesdatenschutzgesetz[17]), der Länder und der Kommunen (z.B. Dienstanweisungen, Beschlüsse) selbst in den jeweils geltenden Fassungen.

Die Datengovernance einer Kommune bezieht sich auf die vorhandenen Regelwerke und berücksichtigt diese bei der Aufstellung von Rollen (z.B. Datenschutzbeauftragte) und Regeln im Umgang mit Daten und bezieht diese mit ein.

Datenschutzmaßnahmen im Rahmen einer Datengovernance umfassen u.a.:

- Sicherstellung der Erfüllung gesetzlicher Vorgaben
- Anwendung von Methoden zur Anonymisierung (Werkzeuge, Algorithmen)
- Bestimmung des Spielraums für die Datennutzung (z.B. Datenverknüpfung - ab wann ist diese kritisch?)
- Entscheidungssicherheit bei der Klassifikation von Daten (datenschutzrelevant vs. offen; personenbezogene Daten)
- Kommunale Regelungen zum Datenschutz referenzieren und vermitteln (z.B. Rollen, Zuständigkeiten, Haftung)
- Umgang mit Datenspenden regeln (z.B. aus Beteiligungsprozessen mit Bürger/-innen)
- Erwartungen und Forderungen von Bürgerinnen und Bürgern berücksichtigen

[16] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE (Letzter Zugriff: 28.03.2022)

[17] https://www.bmi.bund.de/DE/themen/verfassung/datenschutz/bundesdatenschutzgesetz/bundesdatenschutzgesetz-node.html (Letzter Zugriff: 28.03.2022)

11 Informationssicherheit

Als Informationssicherheit[18] bezeichnet man Eigenschaften von technischen oder nicht-technischen Systemen zur Informationsverarbeitung, -speicherung und -lagerung, die die Schutzziele Vertraulichkeit (z.B. kritische Infrastruktur), Verfügbarkeit (technisch und nach Zugangsberechtigung) und Integrität (Verhindern von Datenmanipulation) sicherstellen. Aus den Schutzzielen[19] können konkrete Maßnahmen für eine Datengovernance abgeleitet werden:

- Vertraulichkeit: Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.
- Verfügbarkeit: Dem Benutzer stehen Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung.
- Integrität: Die Daten sind vollständig und unverändert. Der Verlust der Integrität von Daten kann daher bedeuten, dass diese unerlaubt verändert wurden oder Angaben zum Autor verfälscht wurden oder der Zeitpunkt der Erstellung manipuliert wurde.

Zum Aufbau eines Informationssicherheitsmanagements kann auf die bewährte BSI-Grundschutz-Methodik[20] zurückgegriffen werden. Darüber hinaus sollten auch bereits bestehende kommunale Rollen und Regelungen (z.B. Dienstanweisungen und Beschlüsse zur Informationssicherheit inkl. Schutzbedarfsmaßnahmen, Informationssicherheitsbeauftragte, IT-Dienstleister) berücksichtigt werden.

[18] https://de.wikipedia.org/wiki/Informationssicherheit (Letzter Zugriff: 30.06.2022)
[19] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=1 (Letzter Zugriff: 30.06.2022)
[20] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-2-IT-Grundschutz-Methodik/bsi-standard-200-2-it-grundschutz-methodik.html (Letzter Zugriff: 30.06.2022)

12 Digitale Souveränität

Unter dem Begriff der „digitalen Souveränität", die als eigenes Handlungsfeld in die Datengovernance eingebettet ist, wird die Fähigkeit zu selbstbestimmtem Handeln und Entscheiden im digitalen Raum verstanden.

Dem Staat und der Verwaltung kommt bzgl. der digitalen Souveränität die Aufgabe zu, nicht nur als Rahmengeber, der Regeln für seine Gesellschaft festlegt und deren Einhaltung nachverfolgt, sondern auch als „Befähiger", der digitale – und damit in einem immer größer werdenden Maße auch gesellschaftliche – Partizipation ermöglicht (z.B. indem er die Datenkompetenzen der gesellschaftlichen Akteure steigert und verstetigt), zu agieren.

Dabei ist zwischen den widerstreitenden Interessen der verschiedenen Perspektiven, Akteuren und Rollen sorgsam abzuwägen und für alle Seiten zufriedenstellende Lösungen zu finden. Dies bezieht sich sowohl auf den Aspekt der Datensouveränität als auch auf den Aspekt der Vermeidung bzw. Minimierung technologischer Abhängigkeiten – ohne gleichzeitige weitreichende Einschränkung bzw. Abschottung in einer zunehmend vernetzten und digitalisierten Welt.

Um die digitale Souveränität aller Akteure zu stärken, spielen drei wesentliche Aspekte eine Rolle:

1. **Kompetenzen:** Digitale und Datenkompetenzen der Verwaltung und der handelnden Akteure stärken und steigern
2. **Umgang mit Abhängigkeiten:** Neubewertung bestehender und anstehender Abhängigkeiten und die Aufgabe des Staates eines wachsenden Steuerungsanspruchs
3. **Operationalisieren:** Bewertung der eigenen Digitalen Souveränität anhand des Reifegrads in der Praxis mit damit einhergehenden Handlungsempfehlungen.[21]

[21] Mögliche Kriterien für die Operationalisierung sind: (1) Daten: Grad der Ausgestaltung der Berechtigungen zum Datenzugriff und -verarbeitung, (2) Quellcodes: Grad der Verfügbarkeit und der Nachvollziehbarkeit des Quellcodes, (3) Systemabhängigkeit: Grad der Einflussnahme hinsichtlich Migration, Kontrolle und Flexibilität, (4) Kompetenzen: Grad des Kenntnis- und Erfahrungsstands hinsichtlich der Prozesse, Anwendungen und mögliche Anpassungen, (5) offene Schnittstellen: Unterstützung offener Standards und Schnittstellen, (6) Weitere.

13 Datenkatalog

Der Datenkatalog ist als ein technisches und funktionales Werkzeug realisiert, das einen zentralen Überblick über den Datenbestand der Verwaltung bietet. Ein Datenkatalog ist eines der wichtigsten Instrumente zur Unterstützung der Datentransparenz. Der Datenkatalog an sich garantiert nicht die Qualität und Vollständigkeit der bereitgestellten Inhalte und Daten, er muss jedoch eine Reihe von Funktionalitäten bereitstellen, die für die effiziente Suche und nachhaltige Nutzung der verschiedenen Datenquellen notwendig sind. In diesem Sinne ist ein Datenkatalog eine Zusammenstellung der im Datenbestand der Verwaltung vorhandenen Daten, zusammen mit Metainformationen zur Typisierung/Klassifizierung, ggf. mit Aussagen zur Datenqualität, Informationen zum Dateneigentümer und Ansprechpartner, Zugriffsberechtigungen und Nutzungsbedingungen, Quellenangaben, zeitbezogene Metainformationen (erstellt & zuletzt aktualisiert, Datenerfassungszeitpunkt/Gültigkeitszeitraum) und ggf. räumliche Informationen (Standort, Ausdehnung). Datenschutzanforderungen, wie z.B. Löschfristen, aber auch die konkreten Fälle einer Löschung, können (z.B. mittels Löschstatus und Löschdatum) ebenfalls im Datenkatalog gepflegt und nachvollzogen werden. Zusätzlich zu den Informationen über eine Datenquelle/Ressource können/sollten die entsprechenden Datenformate (z.B. Excel-Daten) und Zugriffskanäle (API/Schnittstelle) hinzugefügt werden. Dies verdeutlicht die verschiedenen Informationsebenen, die ein Katalog bieten kann. Dies umfasst die Bandbreite von Metainformationen ohne Link oder herunterladbare Daten bis hin zu Metainformationen mit allen zugehörigen Daten in verschiedenen Formaten. Bei der Bereitstellung der Daten selbst sind zusätzliche Metainformationen wie Medientyp, Datenformat, Konformität, usw. erforderlich. Um die Interoperabilität zu gewährleisten, sollte der Datenkatalog nicht nur eine Benutzeroberfläche für die Benutzerinteraktion bieten, sondern auch eine standardisierte Schnittstelle für die interoperable Kommunikation mit verschiedenen Anwendungsprogrammen. Ein weiterer Aspekt zur Gewährleistung der Interoperabilität ist die Verwendung von standardisierten und bekannten Metadatenmodellen wie W3C DCAT2, ISO 19115 und schema.org.

14 Datenarchivierung

Eine Langzeitspeicherung und -archivierung von Geodaten ist aufgrund der Ermittlung und Nachvollziehbarkeit von ausgewählten zeitlichen, gesellschaftlichen und umweltbedingten Veränderungen von großer Bedeutung. Um diese Veränderungen überwachen zu können, müssen auch nicht mehr aktuelle Geodaten – welche i.d.R. nicht mehr in der GDI/UDP bereitgestellt werden - sicher vorgehalten und nachhaltig verfügbar gemacht werden. Hierbei ist in eine **Langzeitspeicherung** und eine **Langzeitarchivierung** zu differenzieren:

Die **Langzeitspeicherung** beinhaltet die Auswahl, revisionssichere Aufbewahrung, Erhaltung und Wiedernutzbarmachung von älteren, nicht mehr regelmäßig verwendeten elektronischen Dokumenten/Geodaten. Die Daten der Langzeitspeicherung werden für den Zeitraum der Aufbewahrungsfrist und mit einer definierten Übergabe von Datenpaketen an die Archivverwaltungen langzeitgespeichert. Die Langzeitspeicherung schließt somit die Lücke zwischen der Haltung von aktuellen Daten und der Langzeitarchivierung von Daten.[22]

Die **Langzeitarchivierung** hingegen beschreibt die dauerhafte Aufbewahrung und Erhaltung von Unterlagen durch Archive nach Ablauf der Aufbewahrungsfrist zur Bewahrung historischer Überlieferungen. Dies inkludiert die Festlegung der archivwürdigen Datensätze bzw. Eigenschaften eines Datensatzes und die Wiederherstellung für die Nutzbarmachung. Die Regelungen und Anforderungen werden in verschiedenen Gesetzen (z. B. Bundesarchivgesetz) und Verordnungen (z. B. Signaturverordnung) definiert.[22]

Die Fragestellung, welche Geodaten als (nicht) archivwürdig eingestuft werden, wird vom Betreiber der Langzeitspeicherung, den geodatenhaltenden Stellen und den Vorschriften der Archiv-Gesetze bestimmt. Generell müssen Daten, die in eine Langzeitspeicherung oder -archivierung übergehen, registriert und mit einer Metadatenbeschreibung versehen werden. Zudem sind alle Vorschriften des Datenschutzes bei der Speicherung und Recherche zu berücksichtigen.[22]

[22] https://www.gdi-de.org/download/Architektur_GDI-DE_Leitlinien_Langzeitspeicherung_von_Geoinformationen.pdf (Letzter Zugriff: 30.06.2022)

15 Datenintegration

Unter Datenintegration wird ein Prozess verstanden, der Daten aus - ggfs. unterschiedlichen - Datenquellen in eine andere Dateninfrastruktur (z.B. Urbane Datenplattform einer Kommune) einbindet. Die Dateneinbindung kann beispielsweise durch ETL-Prozesse (Extract Transform Load) erfolgen. Die Daten können konsolidiert in einem Data Warehouse gespeichert und über Kataloge und Dienste verfügbar gemacht werden. Innerhalb des Prozesses sind verschiedene Akteure mit verschiedenen Rollen und Zuständigkeiten beteiligt. Im Rahmen einer Datengovernance wird der Prozess innerhalb einer Kommune standardisiert (z.B. Formulare), beschrieben (z.B. Datenintegrations-Wiki) und kommuniziert (z.B. Landingpage UDP). Zudem werden Rollen (z.B. Dateneigentümer:innen, Datenmanager:innen) und Zuständigkeiten (z.B. Datenbereitstellung, Datenmodellierung, Datenspeicherung) festgelegt.