gaia-x Hub Germany

Datenräume für den Katastrophenschutz

Kleiner Wegweiser für einen datenzentrierten Ansatz

White Paper 1/2025
März 2025

Bernhard Bürger, Dr. Kai Fischer, Martin Huschka, Dr. Karl Wienand

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

Über die Serie

White Papers des Gaia-X Hub Deutschland dienen dem Diskurs und Ideenaustausch. Sie spiegeln die Meinung der Autoren wider und nicht notwendigerweise jene der Gaia-X Association oder einer anderen Institution der Gaia-X Initiative.

Autoren

AIT Austrian Institute of Technology GmbH
Bernhard Bürger, Scientist

Fraunhofer-Institut für Kurzzeitdynamik, Ernst-Mach-Institut (EMI)
Dr. Kai Fischer, Gruppenleiter Robustheits- und Resilienzanalysen
Martin Huschka, Wissenschaftlicher Mitarbeiter, Digital Engineering

acatech – Deutsche Akademie der Technikwissenschaften
Dr. Karl Wienand, Wissenschaftlicher Referent

Herausgeber

Gaia-X Hub Deutschland c/o acatech – Deutsche Akademie der Technikwissenschaften
Karolinenplatz 4
80333 München

Empfohlene Zitierweise

Bürger, B., Fischer, K., Huschka, M., Wienand, K. (2025) Datenräume für den Katastrophenschutz
White Paper 1/2025.

Danksagung

Diese Veröffentlichung resultiert in Teilen aus einer Zusammenarbeit mit dem Gaia-X Hub Austria und Fördermitteln des Bundesministeriums für Bildung und Forschung (BMBF) im Rahmen des Programms „Forschung für die zivile Sicherheit“ (www.sifo.de) der Bundesregierung. HERAKLION (Förderkennzeichen 13N16293) ist ein bewilligtes Projekt im Rahmen der Corona-Sondermaßnahme.

Inhaltsverzeichnis

Zusammenfassung

Dieses White Paper zeigt das Potenzial von Datenräumen im Katastrophenschutz am Beispiel Deutschlands auf. Lokale Rettungskräfte, Kommunen und höhere Verwaltungsebenen müssen bei Notfällen zusammenarbeiten, doch eine fragmentierte IT und Interoperabilitätsprobleme erschweren oftmals die wirksame Koordinierung.

Datenräume versprechen eine Lösung zu sein. Das sind dezentrale, föderierte Systeme, die Daten aus verschiedenen Quellen sicher und effizient verknüpfen und dabei die Bedürfnisse vielfältigen Akteuren erfüllen können. Diese Merkmale sind im Katastrophenschutz entscheidend, weil besonders heterogene Konstellationen von Teilnehmenden gegeben sind: Verwaltungen, Notdienste, Privatunternehmen, Forschungseinrichtungen und nicht zuletzt Bürgerinnen und Bürger spielen wichtige Rollen. Ebenso vielfältig sind auch die Daten, die es auszutauschen gilt. Vereinfacht lassen sich diese in drei Kategorien einteilen: offene Daten, nicht-offene Daten von öffentlichen Stellen und nicht-offene Daten von Privatpersonen und privaten Unternehmen. Diese Kategorisierung ermöglicht es, die Souveränität- und Datenschutzkonzepte zu optimieren.

Datenräume bieten den Teilnehmenden im Ökosystem des Katastrophenschutzes viele Vorteile. Behörden können diese beispielsweise nutzen, um die Effizienz der Kommunikation und Koordination zwischen verschiedenen Entscheidungsebenen für den Krisenfall zu steigern oder um die Krisenprävention zu verbessern – beispielsweise mittels Simulationen. Die Datenverfügbarkeit ermöglicht eine bessere Vorbereitung und Kommunikation auch bei Einsatzkräften, was Reaktionszeiten mindert. Private Unternehmen können mit Hilfe von Datenräumen die Compliance-Kosten senken, die beispielsweise auf Grund des Data Acts (DA) der EU entstehen können. Zudem können Unternehmen neue Märkte erschließen und neue Geschäftsmodelle entwickeln – insbesondere durch die Bereitstellung datengestützter Dienste.

Jüngste Krisen, wie die Überschwemmungen der Jahre 2021 und 2024 sowie die COVID-19-Pandemie, verdeutlichen den dringenden Bedarf an datenbasierten und flexiblen Strategien für die Vorbereitung und Bewältigung von Krisen. Wie sich diese umsetzen lassen, zeigt ein Beispiel aus dem Projekt HERAKLION. Der Anwendungsfall gehört zum Bereich des Hochwassermanagements und demonstriert, wie Geodaten, Geländemodelle und regionale Statistiken die Vorsorge und Reaktion auf eine angespannte Lage sowie den Wiederaufbau verbessern.

1. Daten und Katastrophenschutz

Daten bieten eine wichtige Unterstützung für die Entscheidungsfindung im öffentlichen Sektor. Entscheidungssituationen mit hoher Komplexität, starkem Zeitdruck und großer Tragweite profitieren besonders davon. Dazu zählen Katastrophen, denn bei diesen gilt es durch frühzeitige Warnungen, schnelle Entscheidungen und sofortige Reaktionen, gravierende Konsequenzen zu vermeiden oder zu begrenzen. In der heutigen technologisch fortgeschrittenen und global vernetzten Gesellschaft können Katastrophen außerdem zu unvorhersehbaren, verwickelten Effektkaskaden führen. Die COVID-19-Pandemie und die Flutkatastrophen der letzten Jahre – darunter jene im Ahrtal im Jahr 2021 und in Katalonien im Herbst 2024 – sind Beispiele für solche gravierenden Ereignisse, mit langfristigen, weitgehenden Konsequenzen für Gesellschaft und Politik. Durch den Klimawandel ist außerdem die Wahrscheinlichkeit deutlich gestiegen, dass solche Ereignisse eintreten (World Economic Forum, 2024). Damit hat sich auch die Notwendigkeit für Resilienz erhöht, um auf Krisen vorzubereiten, diese zu bewältigen, Auswirkungen einzuschränken und den Wiederaufbau schnell und effizient einzuleiten (acatech, 2014). So gelten Daten als weltweit kritische Ressource für Resilienz (OpenDRI, 2022).

Um Daten als Entscheidungshilfe zu nutzen, ist jedoch ein weiter Weg von Rohdaten zu handlungsrelevanten Informationen zurückzulegen. Dazu müssen in der Regel verschiedene Datenquellen kombiniert, gezielt ausgewertet und kontextualisiert werden. Visualisierungen und Dashboards, zum Beispiel, sind ein geeignetes Mittel, um wichtige Informationen zu bündeln und Entscheidungsfindung zu erleichtern (Schulze et al., 2023). Häufig scheitern der Austausch und die Nutzung von Daten in der Praxis jedoch an technischen und organisatorischen Hürden.

Diese ergeben sich aus der Vielfalt relevanter Akteure bei der Erhebung, Verarbeitung und Nutzung von Daten. Eine solche Vielfalt zeigt sich besonders im Bereich des deutschen Bevölkerungsschutzes. Dieser ist ein komplexes und vielschichtiges System. Die Gemeinde, Städte und Landkreise bilden die operative Basis (Karutz et al., 2017), während die Behörden auf Landesebene die strategische Führung übernehmen, insbesondere bei schwerwiegenderen Ereignissen. Viele weitere Akteure, von Forschungseinrichtungen bis hin zu Privatunternehmen, sind an der Planung oder den Bewältigungsmaßnahmen beteiligt oder davon betroffen. Dies erschwert die Verfügbarkeit von Daten. Eine enge Vernetzung aller Beteiligten und strukturierte, verlässliche Austauschprozesse wären nötig – beides fehlt jedoch oft in der Praxis (Bundesministerium des Innern und für Heimat & Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2021).

Datenökosysteme und Datenräume

Ein Datenökosystem ist ein Netzwerk, in dem Akteure Daten interagieren, um Daten zu finden, zu archivieren, zu veröffentlichen, zu nutzen oder wiederzuverwenden sowie um Innovationen zu fördern, Mehrwert zu schaffen und neue Geschäftsmodelle zu unterstützen (S. Oliveira et al., 2019).

Ein Datenraum ist eine föderierte, offene Infrastruktur für souveränen Datenaustausch, die auf gemeinsamen Vereinbarungen, Regeln und Standards beruht (Reiberg et al., 2022). Technisch betrachtet, stützt er sich auf verteilte Datenspeicher und eine bedarfsorientierte Integration (data europa academy, 2023). So kann ein Datenraum die Grundinfrastruktur für ein Datenökosystem anbieten (s. Abs. 3.3).

Dieses White Paper gibt einen Überblick über die Datennutzung im Bereich des Katastrophenschutzes und zeigt auf, dass sich Datenräume als Lösungsansatz für eine vertrauenswürdige Datennutzung anbieten. Dazu geht Abschnitt 2 auf relevante rechtliche Aspekte auf deutscher und europäischer Ebene ein. Anschließend erfolgt in Abschnitt 3 eine Übersicht zur möglichen Zusammensetzung des Datenökosystems, wobei auf die Rolle der Teilnehmenden, die Kategorien benutzter Daten und die Fragen der Governance eingegangen wird. Dabei werden insbesondere die durch Datenräume erschlossenen Lösungen erleuchtet. Zum Abschluss illustriert Abschnitt 4 anhand eines Anwendungsfalls im Bereich des Hochwassermanagements die Möglichkeiten zur praktischen Umsetzung einer Datenraumlösung.

2. Rechtlicher Rahmen

2.1. Katastrophenschutz in Deutschland

Um den Datenaustausch zu verbessern, muss man die Konstellation der Akteure im Katastrophenschutz in den Blick nehmen. Dieser Abschnitt zeigt, wie ihre Zusammenarbeit rechtlich geregelt ist.

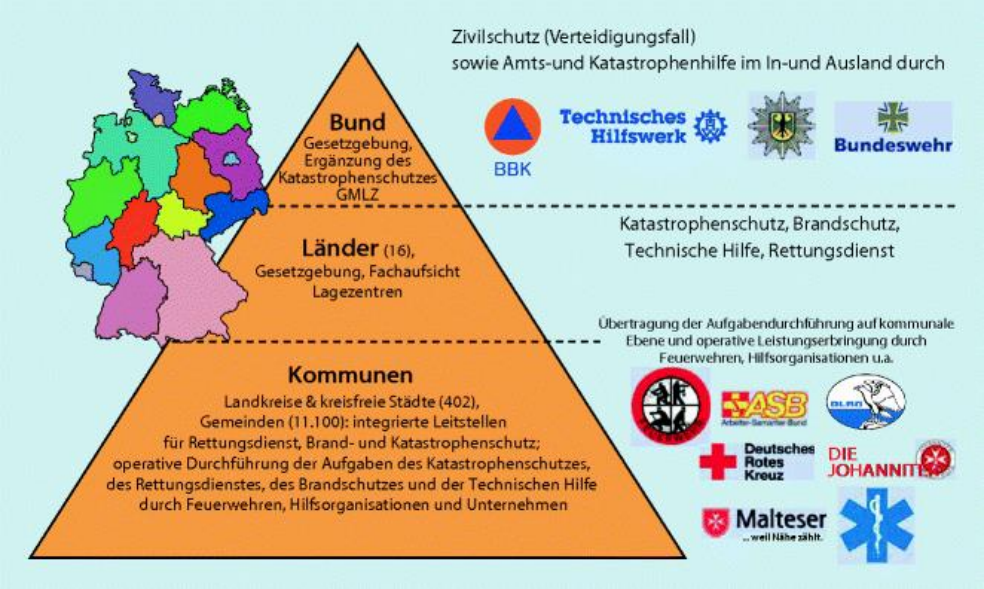

Abbildung 1: Die Bevölkerungsschutz-Pyramide in Deutschland nach Karutz et al. (2017) und BBK

Wie Abbildung 1 zeigt, umfasst der deutsche Bevölkerungsschutz viele Organisationen auf allen drei Verwaltungsebenen: Bund, Länder und Kommunen. Der Bund koordiniert den Schutz vor militärischen Bedrohungen (sog. „Zivilschutz“), ist aber in anderen Fällen lediglich indirekt bzw. beschränkt beteiligt. Die Länder regeln den Schutz vor Extremwetter, Hochwasser, Infektionsausbrüchen, Bränden und andere Katastrophen. Dabei sind die Rechtsgrundlagen jeweils einheitlich: Die lokale Feuerwehr, die Polizei, das Rote Kreuz, sowie weitere private Hilfsorganisationen und Spontanhelfer bekämpfen den Notfall operativ. Kommunen und Gemeinden koordinieren, organisieren und leiten dabei die Einsätze, sowohl in der Vorbereitung als auch in der Bekämpfungsphase. Werden die Kapazitäten der örtlichen Einsatzkräfte überschritten, ruft die Kommune den Katastrophenfall aus und bildet einen Krisenstab. Bei Bedarf kann Hilfe von Nachbarkommunen, vom Bezirk, vom Land und gegebenenfalls vom Bund oder von der EU angefordert werden. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) berät auf allen Ebenen, koordiniert die Zusammenarbeit von Bund und Ländern, bereitet die Vorsorge für Krisenfälle vor, erstellt Risikoanalysen und gibt Warnungen heraus.

Was ist eine Katastrophe?

Eine Katastrophe ein Ereignis, welches das Leben und die Gesundheit von vielen Menschen und Tieren, die Umwelt, erhebliche Sachwerte oder die lebensnotwendige Versorgung der Bevölkerung in einem solchen Ausmaß bedroht, dass die koordinierte Zusammenarbeit verschiedener Dienste zu ihrer Bekämpfung und Abwehr erforderlich ist (Bundesregierung, 2022).

2.2. Pflichten zu Datenbereitstellung

Der datenzentrierte Katastrophenschutz erfordert einen Austausch von Daten, der auf rechtlichen Grundlagen von Ländern, Bund und EU basiert. Dieser Abschnitt beleuchtet insbesondere die Pflichten, Daten bereitzustellen.

Besonders betroffen von diesen Pflichten sind kritische Infrastrukturen. Dies sind Einrichtungen und Anlagen „von hoher Bedeutung für das Funktionieren des Gemeinwesens, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“ (§2 Abs 10 BSIG). Daher ist die Zusammenarbeit zwischen ihren Betreibern und den Katastrophenplanungsstellen unerlässlich. Die Betreiber müssen spezifische Vorgaben einhalten, die u.a. ihre Einbindung in ein Datenökosystem erleichtern. Sie müssen z.B. mit Katastrophenschutzbehörden kooperieren, um ihre Aufgaben bei Ausfall oder Beeinträchtigung auch anderer kritischer Infrastrukturen fortführen zu können (vgl. bspw. §28 Abs 2 KatSG, Berlin). In Sachen bspw. werden Betreiber von kritischen Infrastrukturen explizit aufgefordert, relevante Daten bereitzustellen (§45a SächsBRKG) und in Niedersachsen müssen sie organisatorische und technische Vorkehrungen treffen (§5a NKatSG).

Auf der EU-Ebene spielt der Data Act (Verordnung 2023/2854) eine maßgebliche Rolle im Datenaustausch zwischen Unternehmen und öffentlichen Stellen[1] (s. Tabelle 1), besonders in Katastrophenfällen. Letztere können gem. Kapitel V der DA nicht-personenbezogene Daten von Unternehmen verlangen, die für die Katastrophenbekämpfung relevant sind (Europäische Kommission, 2024a). Personenbezogene Daten dürfen dabei nur angefordert werden, wenn ein nachweisbarer Bedarf besteht und nur unter Anhaltung von besonderen Schutzmaßnahmen. Behörden dürfen weiterhin die erhaltenen Daten gemeinnützige Forschungseinrichtungen und statistische Ämter zur Verfügung stellen oder durch Drittanbieter bearbeiten lassen. Die Unternehmen sind aufgefordert, die Konformität und Angemessenheit der Datenbereitstellungsverlangen zu prüfen, die sie von den Behörden erhalten (Gaia-X Hub Germany, 2024). In der Praxis wird die Überprüfung jedes Antrags voraussichtlich einen wesentlichen Aufwand für die Unternehmen darstellen. In Datenräumen lassen sich übergreifende Rahmenbedingungen für die Datennutzung durch gemeinsame Nutzungsregeln festlegen, daher dürfte der Einsatz von Datenräumen diese Überprüfungsaufgaben wesentlich erleichtern.

Tabelle 1: Datenbereitstellung vor und nach dem Data Act

Vor dem Data Act	*Nach dem Data Act*
Öffentliche Stellen müssen Unternehmen zur Datenübermittlung überzeugen	Unternehmen müssen Weigerung von Datenübermittlung begründen
Datennutzung basiert auf bilateralen Vereinbarungen	Festgestellte, einheitliche Grundregelung für Datennutzung
Unklare Verfahren für Verhandlungen, Beschwerde und Einsprüche	Definierte Verhandlungsverfahren und Zuständigkeiten bei Beschwerden und Einsprüche

Anderseits zwingen EU-Regelungen auch öffentliche Stellen dazu, wichtige Daten bereitzustellen. Die Open-Data-Richtlinie (Richtlinie 2019/1024) verpflichtet sie, viele Daten als Open Data (s. Abs. 3.2) zu veröffentlichen. Dazu gehören besonders „High-Value Datasets“ wie meteorologische Daten, Satellitenbilder sowie lokale und nationale Karten (Europäische Kommission, 2023). Ein datenzentrierter Katastrophenschutz erzeugt zudem viele Daten, die in öffentlicher Hand liegen, aber nicht als Open Data erscheinen können, etwa bei Behörden, Einsatzkräften oder im Gesundheitswesen. Diese Daten könnten dem gesamten Datenökosystem nützen. Der Data Governance Act (DGA) (Verordnung 2022/868) fordert öffentliche Stellen auf, diese Daten für Forschungszwecke bereitzustellen (Europäische Kommission, 2024b).

[1] Im Folgenden werden die Begriffe „Behörden“ und „öffentliche Stellen“ synonym verwendet. Es ist darauf hinzuweisen, dass der Data Act den Begriff „öffentliche Stellen“ weiter fasst als „Behörden“. Öffentliche werden Stellen als „die nationalen, regionalen und lokalen Behörden, Körperschaften und Einrichtungen des öffentlichen Rechts […] oder Verbände, die aus einer oder mehreren dieser Behörden […] bestehen“ definiert (Art. 2(28), DA).

2.3. Chancen zur Umsetzung von Dateninfrastrukturen

Um den Datenaustausch zu fördern und ein dynamisches Datenökosystem zu schaffen, eignen sich Datenräume (s. Abs. 3.3). Rechtsgrundlagen für deren Einrichtung finden sich sowohl in nationalen als auch in europäischen Gesetzen.

Die Einrichtung von Dateninfrastrukturen, wie bspw. Datenräumen, ist in Ländergesetzen nicht ausdrücklich vorgesehen. Infrastrukturen für den Datenaustausch können jedoch als „vorbereitende Maßnahmen“ betrachtet werden, etwa für Schadensmeldungen oder für die Erstellung von Einsatzplänen. Einige Bundesländer haben außerdem Experimentierklauseln, die es erlauben, Projekte abweichend vom geltenden Recht zu genehmigen, um neue Katastrophenschutzkonzepte zu testen (z.B. §7 LKatSG in Baden-Württemberg, §30b BremHilfeG in Bremen). Diese können die Erprobung und Einrichtung von Dateninfrastrukturen wesentlich beschleunigen. Auch die Vorschriften zur Datenbereitstellung für Betreiber kritischer Infrastrukturen können die Einrichtung von Katastrophenschutz-Datenökosystemen erleichtern.

In einem Katastrophenschutz-Datenökosystem würden also viele sensible Daten ausgetauscht werden. Um diese sicher nutzen zu können, sind entsprechende Schutzmaßnahme nötig. Der Data Governance Act (Verordnung 2022/868) legt Maßnahmen fest, die die sichere Wiederverwendung von solchen Daten erleichtern. Ein wichtiges Beispiel dafür ist der Einsatz von Datentreuhändern, die unter anderem für die sichere Nutzung besonders sensibler Daten sorgen (Reiberg et al., 2023).

Datentreuhänder

Datentreuhänder verwalten und schützen Daten oder Rechte an Daten im Auftrag von anderen. Im Zuge ihrer Tätigkeit erhalten die Datentreuhänder Kontrolle über Daten und nutzen diese dann, um dem Datengebenden oder Dritten einen Zugriff zu ermöglichen. Datentreuhänder bieten mehrere für den Katastrophenschutz nützliche Funktionen:

1. Aggregation von Daten (z.B. aus unterschiedlichen Unternehmen)
2. Anonymisierung und Pseudonymisierung von personenbezogenen Daten
3. Geschützte Rechnung: sensiblen Daten werden zu einer geschützten Umgebung übertragen, in der die Verarbeitung erfolgt, dann werden nur die Analyseergebnisse weitergegeben.

3. Ein datenzentrierter Katastrophenschutz

In den vorherigen Abschnitten wurde die Bedeutung von Daten im Katastrophenschutz und der wesentliche Rechtsrahmen für deren Austausch und Nutzung behandelt. Um die Vorteile von Daten im Katastrophenmanagement voll auszuschöpfen, bedarf es eines umfassenden Datenökosystems – eines Netzwerks, das den Austausch und den Datenaustausch, aber auch Innovation und Wertschöpfung fördert (S. Oliveira, et al., 2019). Dieser Abschnitt gibt einen Überblick darüber, welche Daten und Akteure in Frage kommen, um ein solches Datenökosystem für Katastrophenschutz aufzubauen. Wie sich zeigen wird, wären mit dem Aufbau eines solchen Datenökosystems Herausforderungen verbunden, für die Datenräume effiziente Lösungen bieten.

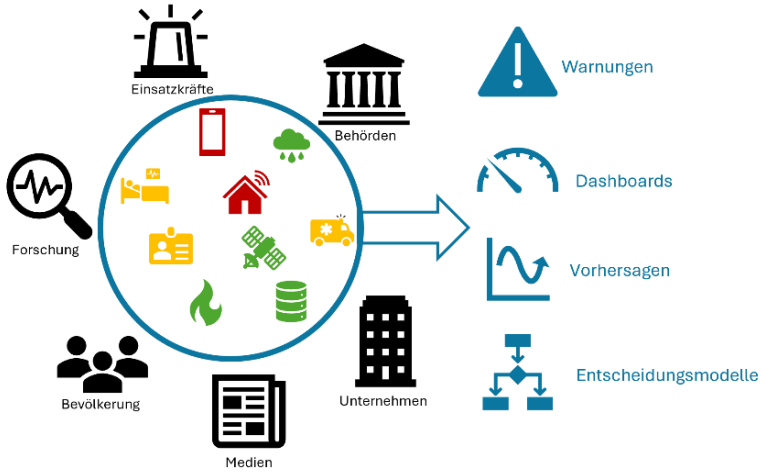

Abbildung 2: Teilnehmenden, Daten und Ergebnisse eines Datenökosystems für Katastrophenschutz

Abbildung 2 veranschaulicht, welche Akteure und Daten in ein Datenökosystem für Katastrophenschutz integriert werden könnten und welche Nutzungsmöglichkeiten somit zu erschließen wären. Die Abbildung zeigt den Gesamtüberblick über das Datenökosystem. Je nach Anwendungsfall sollten die einzelnen Elemente genauer betrachtet werden (siehe z. B. Sautter et al., 2021).

Zu den möglichen Teilnehmenden gehören nicht nur diejenigen, die rechtlich für das Krisenmanagement Sorge tragen und es koordinieren – also die öffentliche Verwaltung und die Einsatzkräfte – sondern auch Forschungseinrichtungen, Privatunternehmen, Medien und die Bevölkerung. Jeder dieser Akteure könnte sich auf unterschiedliche Weise am Datenökosystem beteiligen, um verschiedene Arten von Daten bereitzustellen oder zu nutzen. Dazu gehören Daten, die frei verfügbar sind (Grün) – z.B. Wetterdaten oder Satellitenbilder. Viele Daten sind nicht frei zugänglich, obwohl sie in öffentlicher Hand liegen (Gelb). Daten zur Verfügbarkeit von Krankenhausbetten oder zu Einsätzen von Hilfskräften, zum Beispiel, erfordern auf Sicherheits- oder Datenschutzgründen Zugangsbeschränkungen. Daten von Privatpersonen oder Unternehmen (in Rot), wie die von „smarten“ Geräten oder Smartphones gewonnen, müssen auch besonders geschützt werden, etwa weil sie personenbezogen sind oder geistliches Eigentum darstellen. Zusammen betrachtet bilden diese Daten die Grundlage für Analysen, Simulationen und Prognosen zur Unterstützung von Entscheidungsprozessen. Die Daten können weiterhin in Dashboards zusammengefasst werden oder für Frühwarnungen und Entscheidungsunterstützungssysteme verwendet werden.

3.1. Teilnehmenden

Dieser Abschnitt skizziert die potenziellen Teilnehmenden eines Katastrophenschutz-Datenökosystems. Nicht alle der hier genannten Akteure wären für jeden Anwendungsfall relevant, weil Jeder unterschiedliche Zielen und Bedürfnissen mit der eigenen Beteiligung am Ökosystem verbindet, wie Tabelle 2 zusammenfassend aufzeigt. Diese reichen von der Krisenbekämpfung (operativ oder strategisch) über die Zusammenführung von Informationen bis hin zu wirtschaftlichen Interessen wie Effizienzgewinnen und Kostenreduktionen.

Die Bedürfnisse der Teilnehmenden als Datenanbieter sind manchmal gegensätzlich. Beispielsweise ist einerseits Datenschutz sicherzustellen – beispielsweise zum Schutz von geistigem Eigentum oder der Privatsphäre betroffener Personen. Andererseits müssen öffentliche Stellen und Forschungseinrichtungen gesetzliche Verpflichtungen zur Datenverfügbarkeit erfüllen. Der Data Governance Act und die OpenData-Richtlinie verlangen zum Beispiel, dass sie zahlreiche Daten veröffentlichen bzw. den Zugang zu nicht öffentlich bereitstellbaren Daten erleichtern (s. Abschnitt 3.2).

Als Datenkonsumenten ist für alle Teilnehmenden ein schneller und niederschwelliger Zugang zu Daten von Interesse. Ob öffentliche Stellen, oder privater Unternehmen, keiner soll mit komplizierten Schnittstellen zurechtkommen müssen. Zum Teil, weil es in manchen Fällen an nötigen Kompetenzen fehlt, aber vor allem, weil solche technischen Schwierigkeiten die Reaktionseffizienz mindern. Ein Schlüssel zur niederschwelligen Datennutzung ist die Interoperabilität von Daten, Formaten und Softwarelösungen. Schließlich ist für einige Beteiligte (insbesondere öffentliche Stellen und Einsatzkräfte) die Vertrauenswürdigkeit der Datenquellen entscheidend, da sie in Krisen zügig handeln müssen, ohne Zeit für die Prüfung von Daten und deren Quellen zu haben. An dieser Stelle bieten Datenräume (s. Abschnitt 3.3) einige Vorteile. Hier können Daten einfach und verlässlich verfügbar gemacht und gefunden werden. Dabei sammeln Kataloge die Datenangebote und gleichen ihre Nutzungsbedingungen automatisch mit der vorgeschlagenen Nutzung ab. Zudem nutzen Datenräume zertifizierte Identitäten, wodurch im Krisenfall weniger bis keine weiteren Verifizierungen nötig sind.

Tabelle 2: Teilnehmende des Katastrophenschutz-Datenökosystems und ihre Bedürfnisse

Teilnehmende	*Ziele*	*Bedürfnisse als Datengeber*
Untere Katastrophenschutz-behörden (bspw. Städte, Gemeinde)	• Erstellung von Präventions- und Vorbereitungs-Maßnahmen, auf Basis vorliegender Daten über den geographischen Verantwortungsbereich und dessen Gefahrenquellen • Koordination und Aufsicht von Katastropheneinsätzen, mithilfe von Daten zur Lageentwicklung und den vorhandenen Mitteln zur Gefahrenabwehr • Enge Vernetzung mit Einsatzorganisationen auf lokaler Ebene und mit der oberen Katastrophenschutzbehörde • Schnelle Schätzung und Bereitstellung von Schadensersatzfonds	• Wiederverwendbarkeit von Daten (gem. DGA, Open Data Directive) • Schutz von sensiblen und personenbezogenen Daten • Direkte, niederschwellige Möglichkeit zur Datenübermittlung an andere relevante Teilnehmenden
Obere Katastrophenschutz-behörden (Bundesländer)	• Strategische Ausrichtung des Katastrophenschutzes • Identifizierung von Verbesserungsbedarfen • Enge Vernetzung mit Einsatzorganisationen auf (über-)regionaler Ebene und mit der unteren	• Wiederverwendbarkeit von Daten (gem. DGA, Open Data Directive) • Schutz von sensiblen und personenbezogenen Daten • Direkte, niederschwellige Möglichkeit zur Datenübermittlung an andere relevante Teilnehmenden

	Katastrophenschutzbehörde, sowie Stellen des Bundes • Frühzeitige Warnung der Bevölkerung mittels unterschiedlicher Kanäle (Cell Broadcast, Sirene, Social Media, etc.)	
Einsatzkräfte (bspw. Feuerwehr, Hilfsorganisationen)	• Planung, Auswertung von Einsatztaktik und Personalansatz • Koordinierte Einsatzbewältigung, im Sinne der einsatzführenden Behörde	• Schutz von sensiblen und personenbezogenen Daten • Möglichkeit zur Datenübermittlung an andere relevante Teilnehmenden
Bevölkerung	• Selbstschutz in Katastrophenfällen • Informiert sein • Niederschwellig Schadenersatz beantragen • Einbindung in die Bewältigung, als Spontanhelfende	• Schutz von personenbezogenen Daten • Transparente Nutzung der bereitgestellten Daten • Niederschwellige und sichere Wege, Daten selbstständig zu teilen (z.B. Datenaltruismus nach DGA)
Forschungs-einrichtungen und Anbieter von Analysen	• Seltene Ereignisse auswerten, um eine valide Datengrundlage für die Forschungsarbeit zu erhalten	• Wiederverwendbarkeit von Daten (gem. DGA, Open Data Directive) • Schutz von sensiblen und personenbezogenen Daten
Medien	• Genau und frühzeitig informieren und warnen • Schneller und valider Zugang zu Informationen für die Berichterstattung	• Verfügbarkeit, Auffindbarkeit Interoperabilität von Daten
Betreiber kritischer Infrastrukturen (bspw. Stromversorger)	• Risiken abschätzen • Aufgaben bei Ausfall oder Beeinträchtigung (auch anderer Infrastrukturen) fortfahren	• Einfache Zusammenarbeit mit Behörden • Schutz von sensiblen Daten • Transparente Nutzung der bereitgestellten Daten
Versicherungen	• Schnell und genau Schadenersatz zahlen • Risiken abschätzen	• Einfache Zusammenarbeit mit Behörden • Schutz von sensiblen Daten • Transparente Nutzung der bereitgestellten Daten

Ein effektiver und vertrauenswürdiger Datenaustausch steigert die Effizienz der Katastrophenhilfe. Lokale Behörden können dadurch z.B. die Prävention verbessern und Schadenersatzleistungen schneller und einfacher abwickeln. Für Einsatzkräfte äußert sich diese Effizienz in einer besseren Vorbereitung, einer schnelleren Triage der Fälle, einer verbesserten Kommunikation und Koordination (auch mit Spontanhelfenden) und letztlich in kürzeren Reaktionszeiten. Je umfangreicher die verfügbaren Daten sind, desto größer sind die Vorteile, zum Beispiel von personalisierten Dashboards und KI-basierten Entscheidungsmodellen.

Diese Performancesteigerungen betreffen auch private Unternehmen. Für Betreiber kritischer Infrastrukturen, zum Beispiel, erleichtert die Teilnahme an einem gemeinsamen Datenökosystem den Datenaustausch mit den Behörden enorm. So werden die Kosten der gesetzlich geforderten Datenbereitstellung wesentlich gesenkt. Ein etablierter Kommunikationskanal mit den Behörden mit klaren, vordefinierten Regeln verringert außerdem die Kosten für die Compliance mit dem Data Act (siehe Abschnitt 2.2). Auch für

Versicherungen reduzieren auffindbare und zugängliche Daten den Zeitaufwand und die Fehlerquote bei der Abwicklung von Schadensersatzansprüchen (s. Abschnitt 4.1). Schließlich ermöglicht die Datenverfügbarkeit einigen Teilnehmenden auch, innovative Mehrwertdienste wie Simulationen, Dashboards und KI-basierte Tools anzubieten.

3.2. Datenkategorien und Datennutzung

Dieser Abschnitt bietet einen Überblick über die im Katastrophenschutz-Ökosystem verfügbaren Datenarten. Abbildung 2 zeigt, wie vielfältig diese Daten sein können. Welche davon eingeschlossen werden, hängt von einer durchdachten, auf den jeweiligen Anwendungsfall angepassten Planung ab. Entscheidend sind dabei auch die Akteure im Ökosystem, ihre verfügbaren Daten und ihre Ziele.

In Tabelle 3 werden die möglichen Daten in drei Kategorien geteilt, je nach dem erforderlichen Maß an Schutz und Verfügbarkeit. Diese Kategorien sind: Offene Daten (Open Data), nicht-offene Behördendaten und nicht-offene private Daten. Open Data sind öffentlich zugängliche und nutzbare Daten. Die Lizenz dieser Daten erlaubt ihre Verarbeitung, Kombinierung und Verbreitung für jeden Zweck. Öffentliche Stellen müssen viele für den Katastrophenschutz wichtigen Daten als Open Data bereitstellen (s. Abs. 2.2). Die Plattformen, auf denen diese Daten in der Regel veröffentlicht werden, können durch entsprechende Schnittstellen (wie z.B. APIs[2]) im Ökosystem angebunden werden. Allerdings muss oftmals eine Umformatierung erfolgen. Das liegt daran, dass Daten derselben Kategorie, die aber aus verschiedenen Quellen stammen, nicht selten in unterschiedlichen Formaten vorliegen.

Zahlreiche wertvolle Daten, wie Einsatzdaten von Polizei und Feuerwehr oder Patientendaten aus Kliniken, liegen bei öffentlichen Stellen. Aus Sicherheits- und Datenschutzgründen bleibt ihre Veröffentlichung als Open Data ausgeschlossen. Doch wäre der Austausch dieser Daten im Krisenmanagement wertvoll. Die uneinheitliche und oft mangelhafte Digitalisierung der Verwaltungen verhindert die sinnvolle Nutzung dieser Daten erheblich (Brucke et al., 2024), wie bspw. die COVID-19-Pandemie gezeigt hat. Verschiedene Regelungen (u.a. der Data Governance Act, s. Abs. 2.3) schaffen Anreize für die Verwaltung, solche Daten bereitzustellen. Diese Bereitstellung erfordert auch strenge Schutzmaßnahmen und Zugriffskontrolle, besonders bei personenbezogenen Daten. Diese sollten zum Beispiel nur aggregiert, pseudonymisiert oder anonymisiert verfügbar sein.

Für manchen Krisenfälle sind Daten von Privatunternehmen nötig (Europäische Kommission, 2022). Die Daten über den Zustand von Industrieanlagen, die mit Gefahrstoffen arbeiten, sind beispielweise nur vom Betreiberunternehmen zu erhalten. Oft besitzen private Unternehmen auch viele wichtige personenbezogene Daten über Bürgerinnen und Bürger, wie Standortdaten, die vom GPS von Smartphones und Wearables oder durch Anrufe und

[2] Eine Programmierschnittstelle, häufig nur kurz API genannt (von englisch application programming interface, wörtlich ‚Anwendungs-programmier-schnittstelle'), ist der Teil eines Softwaresystems, der es anderen Programmen ermöglicht, mit ihm zu interagieren, z.B. um Daten zu erhalten.

Internetnutzung über Mobilfunknetze erfasst werden (Verhulst et al., 2021). Die Nutzung dieser Daten in Katastrophenfällen stellt offensichtliche Herausforderungen für den Datenschutz dar. Außerdem müssen die Bedingungen für den Zugang, die Nutzung und die Weitergabe verhandelt werden. Bestimmte Fälle sind dabei gesetzlich geregelt. Die europäische „Seveso-III"-Richtlinie (Richtlinie 2012/18) verpflichtet z.B. Anlagen, die mit Schad- und Gefahrstoffen arbeiten, Daten mit Behörden zu teilen. Der Data Act (s. Abschnitt 2.2) legt darüber hinaus allgemeine Grundregeln für die Datennutzung von Unternehmensdaten bei Behörden fest.

Tabelle 3: Kategorisierung der im Katastrophenschutz benutzten Daten

Datenklasse	*Beispiele*	*Zugriff*	*Herausforderungen*	*Relevante Gesetze und Richtlinien*
Open data	Wetter, Pegelstände, Satellitenbilder	Öffentlich	Vernetzung existierender Plattformen, Interoperabilität der Formate Heterogene Datenqualität	OpenData Directive
Geschützte Daten bei öffentlichen Stellen	Einsatzdaten von Hilfskräften, personenbezogenen Daten über Bürger:innen	Beschränkt	Datenschutz und -sicherheit, Digitalisierung der Behörden	Verwaltungs-cloud Strategie, DSGVO, DGA
Private Daten	Standortdaten aus Mobilnetz, Nutzungsdaten von Smart Devices	Beschränkt	Datensicherheit (Urheberrecht und Geschäftsgeheimnisse), Zugangsbedingungen verhandeln	DA, DSGVO

Ein Datenökosystem für den Katastrophenschutz muss die Anforderungen der Teilnehmenden erfüllen und die angemessene Nutzung verschiedener Datentypen sicherstellen. Hier wird ein weiterer Vorteil von Datenräumen deutlich (s. Abschnitt 3.3): Sie können dezentral und als Multi-Cloud-Infrastrukturen umgesetzt werden. Das bedeutet, dass Daten über verschiedene Speicherorte verteilt sind, jeweils von den entsprechenden Dateninhabern selbst bestimmt. So lässt sich die Speicherung und Sicherheit dem Schutzbedarf der Datensätze anpassen. Wenig sensible Daten wie Open Data lassen sich kostengünstig speichern, selbst bei Hyperscalern wie Google, AWS oder Microsoft. Gesundheitsorganisationen, private Unternehmen und Inhaber anderer geschützter Daten können mittlerweile unabhängig Lösungen wählen, die ihren Bedürfnissen entsprechen.

3.3. Datenräume als Lösungsansatz

Der Katastrophenschutz profitiert erheblich von der Verfügbarkeit und Verknüpfung relevanter Daten von verschiedenen Teilnehmenden. Diese lassen sich auf vielfältige Weise in ein Datenökosystem einbinden. Eine zentralisierte Plattform, die alle relevanten Daten sammelt, würde aus erstem Blick sich als Lösung anbieten. Eine solche Plattform wäre für den Katastrophenschutz jedoch undenkbar. Sie würde enorme Herausforderungen für Datensicherheit und Datenschutz darstellen. Zudem müssten sich alle Beteiligten auf eine gemeinsame Datenverwaltung einigen. Private Unternehmen müssten schließlich überzeugt werden, ihre Daten einzubringen und die Kontrolle über sie abzugeben.

Im Gegenteil sind Datenräume föderierte – also dezentral organisierte – Infrastrukturen, deren Teilnehmenden die Kontrolle über ihre Daten (Datensouveränität) behalten: Sie entscheiden beispielsweise, wer Zugang zu den Daten erhält, und für welche Zwecke, Zeiträume etc. Datenräume sind insofern offen gestaltet, als kein Akteur von der Teilnahme ausgeschlossen wird, solange dies die notwendigen Voraussetzungen erfüllt (z.B. die Voraussetzung, Teil einer bestimmten Branche zu sein, für Datenräume derselben Branche). Die grundlegenden Vereinbarungen zur Teilnahme und Datennutzung werden transparent für den gesamten Datenraum bestimmt und kommuniziert (s. Abs. 3.4).

So unterscheiden sich Datenräume grundlegend von zentralisierten Plattformen, beispielsweise von Open-Data-Plattformen. Daten auf diesen Plattformen sind unbeschränkt nutzbar (s. Abs. 3.2), während die Datennutzung in einem Datenraum den gemeinsamen Regeln und den von den Teilnehmern festgelegten Bedingungen unterliegt. Diese können eine unbeschränkte Nutzung vorsehen, müssen dies jedoch nicht. Ein Datenraum ist außerdem auch kein zentralisierter Ablageort, sondern vermittelt den Austausch zwischen Dateninhabern und -nutzern. Datenräume können also eine offene, sichere und transparente Datennutzung ermöglichen und somit die Grundlage für Datenökosysteme bilden. Frühere Arbeiten haben außerdem ihre praktische Umsetzung für den Katastrophenschutz untersucht (Sautter et al., 2021).

Gaia-X und andere Datenraum-Initiativen bieten Umgebungen, in der die vereinbarten Regeln automatisch durchgesetzt werden (Giussani et al., 2024). Die Nutzungsregeln sind außerdem klar und werden im Voraus (also vor dem Auftritt der Krise) vereinbart. So lassen sich standardisierte Datennutzungsvereinbarungen per Mausklick abschließen. So werden Zugriffsanträgen schneller erstellt und überprüft (eine Pflicht der Unternehmen gemäß dem Data Act, s. Abs. 2.2) und Daten werden schneller zur Verfügung gestellt.

Ein Datenraum stellt einen „One-Stop-Shop“ dar, in dem Daten aus verteilten Speichern auffindbar sind: er ist also zentral zugänglich, aber dezentral organisiert (Sautter et al., 2021). In einem Datenraum sind bspw. alle Daten und Dienste in leicht durchsuchbaren Katalogen gesammelt. Verschiedene Quellen oder Analysewerkzeuge können integriert werden, was die Erfüllung der FAIR-Kriterien (Wilkinson et al., 2016) erleichtert: In Datenräumen sind Daten also auffindbar (engl.: *findable*), zugänglich (engl. *accessible*), interoperabel und wiederverwendbar (engl.: *reusable*).

Datenräume setzen auf Open-Source-Lösungen, standardisierte Datenformate und Übertragungsprotokolle, was die Effizienz steigert (FITKO, 2020). Beteiligte Akteure können voneinander entwickelte Lösungen leicht übernehmen, oder bestehende Lösungen kooperativ einsetzen und betreiben. Der dezentrale Ansatz der Datenräume basiert auf der Föderation interoperabler Instanzen. Diese ermöglicht es z.B. lokalen Behörden, eigene Datenräume zu schaffen und zu betreiben. Sie sind interoperabel und erlauben den Datenaustausch sowie die Programmausführung über verschiedene Systeme innerhalb der Föderation, unabhängig von der spezifischen Softwarelösung jeder Behörde. Jede lokale Lösung kann so nicht nur die eigenen spezifischen Bedürfnisse erfüllen, sondern auch von Netzwerk-Effekten des gesamten Ökosystems profitieren. Die Nutzung mehrerer interoperabler Lösungen verhindert zudem die Abhängigkeit von bestimmten einzelnen Anbietern (sog. „*Vendor Lock-in*“). Die Abhängigkeit von externen Anbietern mit undurchsichtigen und unvorhersehbaren internen Entscheidungsprozessen führt auch zu weniger Transparenz und Souveränität in der Datennutzung.

Transparenz und Vertrauen sind in jedem Datenökosystem wesentlich. Im Katastrophenfall ist insbesondere die Vertrauenswürdigkeit der Identität der Partner entscheidend. Jeder Verifizierungs- oder Authentifizierungsschritt kostet in einer Krise Zeit und Mühe, die in dessen Bewältigung fließen sollte. Verifizierte Identitäten, wie die von Gaia-X Datenräumen, schaffen die Basis für Vertrauen (Gaia-X AISBL, 2022). Wenn ein Datenanbieter zum Beispiel angibt, es handele sich bei ihm um eine bestimmte Organisation, kann ein Datennutzer sich darauf verlassen, dass es sich tatsächlich um die betreffende Organisation handelt. So bietet ein Datenraum eine vertrauenswürdige Umgebung, in der selbst sensible Daten sicher ausgetauscht werden können.

Die Teilnehmenden müssen nicht nur der Identität der anderen vertrauen, sondern auch der Einhaltung der Regeln bei der Nutzung ihrer Daten, was durch automatische Regelanwendung gewährleistet wird. Die Neutralität der Instanzen, die diese Regeln bestimmen, stärkt das Vertrauen innerhalb des Datenraums (s. Abs. 3.4): Die Teilnehmenden können sicher sein, dass die Regeln klar sind und, dass sie die Interessen aller harmonisieren.

3.4. Governance von einem Katastrophenschutz-Datenraum

Die bisherigen Abschnitte betonen, wie wichtig es ist, im Voraus zu planen, welche Akteure und Daten in den Datenraum kommen, welche Grundregeln gelten und, wie sie technisch umgesetzt sind. Wer diese Regeln aufstellt und diese Entscheidungen trifft, spielt daher eine zentrale Rolle beim Aufbau des Datenraums. Diese Fragen stehen im Mittelpunkt der Datenraum-Governance, die in diesem Abschnitt erläutert wird.

Der Begriff „Governance“ hat mehrere Definitionen. Hier beschreibt „Governance eines Datenraums“ die Koordinierung jener Akteure, die am Geschehen im Datenraum beteiligt oder von dieser (potenziell) betroffen sind (Reiberg et al., 2024). In den meisten Datenraum-Initiativen nimmt eine Instanz eine zentrale Rolle in der Governance ein – diese nennt man Orchestrator.

Zu deren Aufgaben gehören:

- Entscheiden, wer teilnehmen darf und wie die Teilnahme gefördert oder subventioniert werden kann (unter Beachtung von Nichtdiskriminierungsvorschriften)
- Festlegen, durch welche Dienste die Interaktion der Teilnehmer ermöglicht und erleichtert wird und von wem diese Dienste erbracht werden
- Schätzen, welche Kosten anfallen und regeln, wie diese gedeckt werden

Besonders wichtige Teilnehmende oder ad-hoc Gremien können die Rolle des Orchestrators übernehmen (Brousseau et al., 2024). In der Anfangsphase eines Katastrophenschutz-Datenraums treten oft zentrale Figuren aus der öffentlichen Verwaltung (etwa Kommunen, Länder oder Wasserwirtschaftsgesellschaften) auf, die als Orchestrator agieren können. Langfristig verlieren diese jedoch ihre dominante Rolle. Zum einen gilt: Je mehr neue und unterschiedliche Teilnehmende aufgenommen werden, desto größer wird der Bedarf an kollegialen Entscheidungsprozessen und neutralen Entscheidungsinstanzen (Brousseau et al., 2024). Zum anderen kann sich ein Katastrophenschutz-Datenraum aus einer Föderation lokal entstandener Datenräumen entwickeln oder vom Anfang an grenzübergreifend konzipiert sein.

Langfristig ist es daher meist unzureichend, eine bestehende Organisation als Orchestrator zu beauftragen. Stattdessen ist meist eine dezidierte Organisation zu schaffen, in der die relevanten Teilnehmenden und Betreiber des Datenraumes angemessen partizipieren können. Dabei ist auf die angemessene Beteiligung wesentlicher Interessengruppen zu achten (wie kommunale Verwaltungen, bestimmte Unternehmen oder Branchen).

Viele der existierenden Datenraum-Projekte werden durch öffentliche Fördermittel sowie Regulierungsmaßnahmen unterstützt. Die Europäische Kommission hat zum Beispiel den European Health Data Space (EHDS) in ihrer Strategie zur Stärkung des Gesundheitssektors verankert (Europäische Kommission, 2024c). Wie es auch bei einem Katastrophenschutz-Datenraum der Fall wäre, arbeitet der EHDS mit sensiblen Daten, bezieht Teilnehmende aus dem öffentlichen und privaten Sektor ein und operiert in einem streng regulierten Bereich mit starkem Fokus auf dem Gemeinwohl (Europäische Kommission, 2024d). Der EHDS stützt seine Governance auf verschiedene Gremien auf EU- sowie auf nationaler Ebene (European Commission & Trasys International, 2022). Erstere definieren die Gesamtstrategie und die Richtlinien, während letztere (z.B. die EHDA e.V. in Deutschland) die Umsetzung dieser Richtlinien in ihrem jeweiligen Land koordinieren (Europäische Kommission, 2024e; European Health Data Alliance e.V., 2025).

4. Anwendungsfall: Der HERAKLION Resilienz-Datenraum

Ein praktisches Beispiel für den Einsatz von Datenräumen veranschaulicht die genannten Konzepte und macht greifbar, wie Daten den Katastrophenschutz verstärken. Dieser Abschnitt stellt ein Anwendungsfall aus dem BMBF-Projekt HERAKLION vor. Das Projekt entwickelt einen skalierbaren Datenraum, der lokale Behörden und Einsatzkräfte bei Entscheidungen unterstützt. Gleichzeitig erleichtert er die Analyse zentraler Faktoren in Krisen, die durch Extremwetter oder Pandemien entstehen. So lassen sich solche Ereignisse früher erkennen und effizienter bewältigen. Am Beispiel eines Flutereignisses wird deutlich, wie die Integration und Verknüpfung heterogener Datenquellen im Datenraum die Entscheidungsprozesse im Katastrophenschutz optimiert (HERAKLION Projekt, 2022).

Hierbei werden folgende Leitfragen adressiert:

- Wie kann sich auf zukünftige Ereignisse bestmöglich vorbereitet werden?
- Wie erzeugen Daten ein Verständnis zwischen Ursache und Wirkung?
- Wie lassen sich potenzielle Schwachstellen identifizieren?

4.1. Datenraum-gestützte Vorbereitung auf Dammbruch

Jüngste Hochwasserkatastrophen verdeutlichen die Anfälligkeit von Bevölkerung und Infrastruktur gegenüber Naturgefahren. Die verheerende Flutkatastrophe im Ahrtal 2021 verursachte nicht nur personelle Schäden, sondern hatte auch weitreichende Folgen für die Verkehrsinfrastruktur (Burghardt et al., 2024), mit überregionalen Auswirkungen. Das folgende Beispiel verwendet u. a. Daten der Emschergenossenschaft/Lippeverband, um einen Deichbruch zu simulieren und zu zeigen, wie Daten zur Vorbereitung auf Katastrophenereignisse beitragen.

Die Emschergenossenschaft/Lippeverband ist ein Wasserwirtschaftsverband, der sich unter anderem mit dem Hochwassermanagement der Flüsse Emscher und Lippe befasst (EMGLV, 2024). Beispielhaft werden hier verschiedene Hochwasserszenarien und mögliche Dammbrüche betrachtet. Hierzu führt der Wasserwirtschaftsverband hydrodynamische Simulationen durch, um gefährdete Gebiete einer Kommune aufzuzeigen. Die ortsbezogenen Informationen bezüglich der Ausbreitungsfläche der Flut wurden als externe Datenquelle aufgegriffen und mit weiteren Informationen zusammengeführt. Zur umfassenden Analyse wurden Datenquellen aus verschiedensten Bereichen herangezogen:

- Regionalstatistiken geben Auskunft zur Bevölkerungsstruktur.
- Digitale Gelände-, Gebäude- und Landschaftsmodelle liefern Informationen bezüglich der Topografie und Bebauung.
- Weitere Geodaten können Auskunft zu Verkehrsnetzen oder wichtigen Einrichtungen (sog. Points of Interest) aufzeigen.

Anhand dieser Daten lässt sich simulieren, welche Straßen durch die Flut blockiert werden und wie gut verschiedene Gebiete erreichbar sind. In Krisensituationen ist das eine wichtige Grundlage für den Einsatz der Hilfskräfte. Abbildung 3 zeigt beispielhaft Simulationen über die

Erreichbarkeit eines Krankenhauses: grüne Bereiche identifizieren eine hohe Erreichbarkeit, das heißt es liegt eine kurze Fahrtzeit zum Erreichen des Krankenhauses vor. Rote Bereiche zeigen dagegen Gebiete mit langen Fahrtzeiten zum Krankenhaus (niedrige Erreichbarkeit). Diese Fahrtzeiten werden für das gesamte Gebiet von einem Algorithmus berechnet. Das linke Bild zeigt die Lage im Normalzustand, in dem das Krankenhaus vom ganzen Gebiet gut erreichbar ist. Das mittlere Bild in Abbildung 3 zeigt die überflutete Fläche als Resultat der hydrodynamischen Simulation. Im rechten Bild sind beide Datensätze kombiniert. Es wird sichtbar deutlich, welche Straßen durch die Überflutung unpassierbar werden und wie sich die Erreichbarkeit des Krankenhauses somit ändert. Das Bild visualisiert schnell potenzielle Versorgungsengpässe, was in die Planung von Vorsorgemaßnahmen einfließen kann. Diese neu entwickelte Methodik beruht auf der Zusammenführung verschiedener Datensätze und kann effizient für beliebige Orte eingesetzt werden.

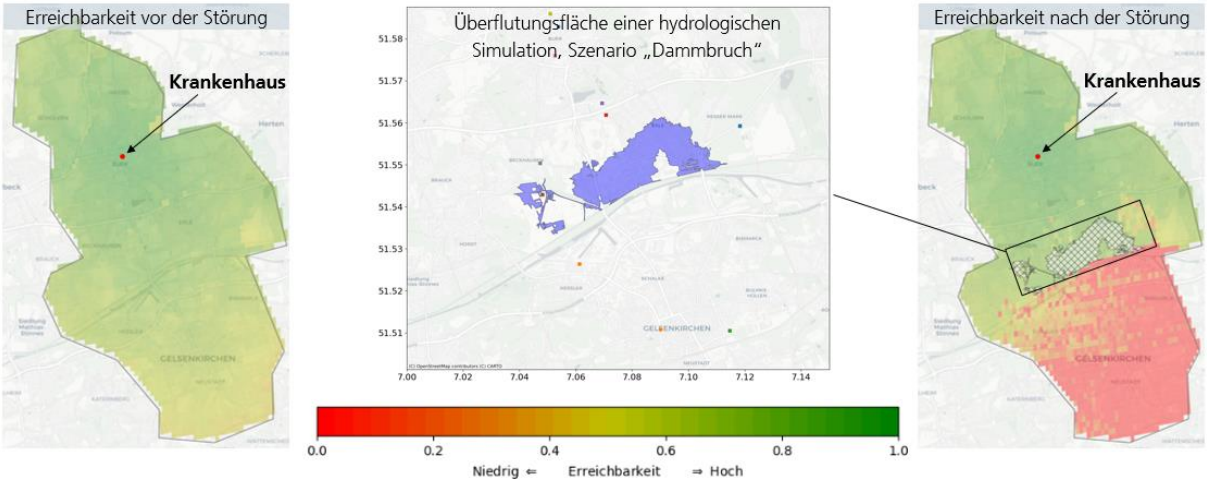

Abbildung 3: Verknüpfung dreier Datenquellen (Flutsimulation, Straßennetz, Points of Interest) zur Analyse der Erreichbarkeit vor und nach einem Hochwasserereignis.

Die Überflutungsfläche in Abbildung 3 zeigt das betroffene Gebiet nur zweidimensional. Die Daten eines digitalen Geländemodells, beispielsweise mit Informationen des Bundesamtes für Kartographie und Geodäsie (BKG) (Bundesamt für Kartographie und Geodäsie, 2024) ermöglichen weitere Analysen. So lassen sich etwa Wasserstände abschätzen, wie im linken Bild von Abbildung 4 dargestellt. Diese Informationen sind wichtig, um potenzielle Schäden einzuschätzen. Das rechte Bild in Abbildung 4 zeigt beispielhaft die detaillierte Auflösung der erwarteten monetären Schäden. Dies ist nicht nur für die kommunalen Entscheidungsträger relevant, sondern auch für Versicherer.

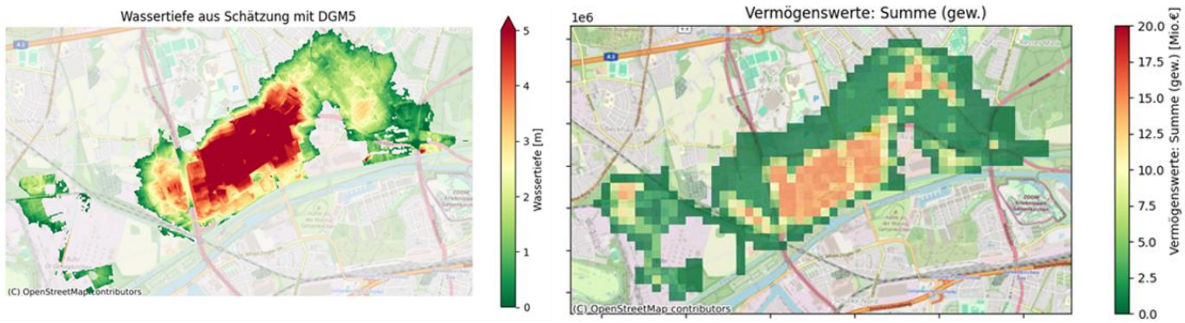

Abbildung 4: Abschätzung des Wasserstands (links) und des zu erwartenden monetären Schadens (rechts).

Durch die Zusammenführung und Auswertung heterogener Datensätze Typs können also effizient Informationen zusammengeführt werden, was einen Beitrag für Entscheidungen im Katastrophenfall liefert. In diesem Beispiel betreffen die Analysen hauptsächlich die Vorbereitung vor Katastrophen. Somit wird der Frage nachgegangen, was eintreten kann und wo potenzielle Schwachstellen vorliegen. In einer Krisensituation können somit gezielter und effizienter Maßnahmen eingeleitet werden, um potenzielle Schäden einzudämmen und die Reaktionszeit zu mindern.

4.2. Technische Umsetzung des Anwendungsfalles im Datenraum

Im vorherigen Abschnitt wurde an einem Anwendungsfall dargestellt, was der Datenraum leisten kann. Hier wird untersucht, wie dies technisch umgesetzt wird. Abbildung 5 zeigt eine vereinfachte Darstellung der Geschäftsschicht des HERAKLION Resilienz-Datenraums, basierend auf dem IDSA-Standard (IDSA, 2022). Der Standard teilt die Teilnehmenden in Rollen ein: Datennutzende und -konsumenten (links in der Skizze), Dateninhaber und -anbieter (rechts) sowie einen Broker-Dienst, der eine Exploration der im Datenraum bereitgestellten Daten auf Basis der Metadaten ermöglicht.

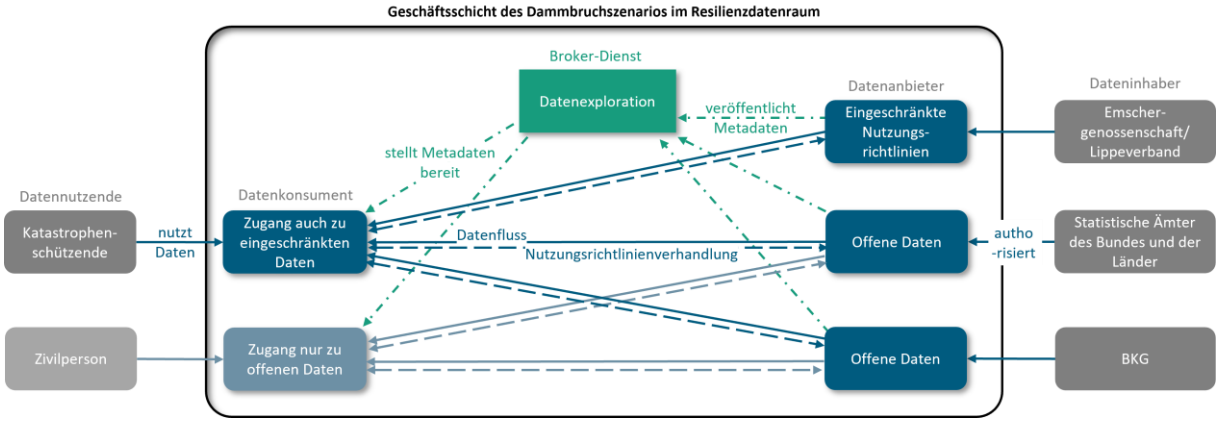

Abbildung 5: Rollenverteilung nach IDSA-Standard für den Anwendungsfall Hochwasserschutz.

Im Dammbruch-Szenario aus Abschnitt 4.1 nutzen zum Beispiel Mitarbeitende des kommunalen Katastrophenschutzes den Datenraum. Ihr zentraler Zugang erfolgt über eine technische Schnittstelle, die auf den Eclipse Dataspace Components basiert (Eclipse Foundation, 2021a, 2021b). Um aktiv teilzunehmen, verwenden diese Katastrophenschützende zertifizierte Identitäten. Mit diesem Zugang werden sie im Datenraum als Datenkonsumenten aktiv.

Alle Teilnehmenden im Datenraum erhalten eigene Identitäten. Diese regeln den Zugriff auf die Daten. Katastrophenschützende bekommen zum Beispiel Zugang zu den Daten, die sie für ihre Analysen im Krisenfall benötigen – auch wenn der Zugang zu diesen Daten aufgrund der eingeschränkten Nutzungsrichtlinien der breiten Öffentlichkeit nicht gewährt wird. Zivile Nutzende können über eine eigene Schnittstelle und eine eigene Identität ebenso als Datenkonsumenten auftreten. Sie erhalten jedoch nur Zugriff auf frei verfügbare Daten, die uneingeschränkt genutzt werden dürfen. Die Zertifizierung und Identitätsprüfung schaffen also Vertrauen unter allen Beteiligten. So lässt sich die kommunale Resilienz mit verlässlichen Daten und belastbaren Analysen stärken.

Offene Daten sind zwar auch ohne den Datenraum verfügbar, doch dieser bietet durch Gewährleistung der FAIR-Prinzipien klare Vorteile. Im Datenraum lassen sich alle für den Katastrophenschutz wichtigen Daten schnell finden, automatisch abrufen und dank einheitlicher Daten- und Metadatenstandards interoperabel kombinieren. So kann auch ein ziviler Datenkonsument verteilte Daten zügig analysieren, um etwa das eigene Grundstück besser vor Extremwetter zu schützen.

Ein Broker-Dienst, der auf dem Federated Catalog (Eclipse Foundation, 2022/2025) basiert, erlaubt Datenkonsumenten, die für sie zugänglichen Daten einzusehen. Automatisierte Agenten aktualisieren die katalogisierten Metadaten kontinuierlich, sodass das Lagebild stets auf den neuesten Daten beruht. Informationen zur Datenqualität ergänzen die von den Datenanbietern bereitgestellten Metadaten. So erhalten die Datenkonsumenten zusätzliche Metriken zur Zuverlässigkeit, Vollständigkeit sowie zur geografischen und zeitlichen Auflösung der Daten. Dies ermöglicht ihnen, die Belastbarkeit der Daten einzuschätzen.

Abbildung 5 zeigt auf der rechten Seite verschiedene Dateninhaber. Im Beispiel von Abschnitt 4.1 gehört dazu die Emschergenossenschaft/Lippeverband, die ihre Ergebnisse mit eingeschränkten Nutzungsrichtlinien bereitstellt. Die Statistischen Ämter des Bundes und der Länder sowie das BKG bieten weitere offene Daten an. Auch diese Dateninhaber können dank einer zertifizierten Identität im Datenraum als Datenanbieter auftreten. Sie nutzen ihre eigenen Schnittstellen, basierend auf Eclipse Dataspace Components, um Daten verschiedener Kategorien (siehe Tabelle 3) im Datenraum anzubieten.

Offene Daten lassen sich direkt über die APIs der Anbieter an die Nutzenden weitergeben. Eingeschränkt nutzbare Daten erfordern hingegen spezielle technische Lösungen, um die Einhaltung der Nutzungsrichtlinien sicherzustellen. Wie dieses Beispiel zeigt, schafft ein Datenraum eine einheitliche Plattform, auf der sich alle Datenkategorien bereitstellen lassen.

Die grundlegende Infrastruktur des Datenraums ist dezentral: Die Daten bleiben bei ihren Inhabern. Diese behalten außerdem die Kontrolle darüber, wer Zugriff erhält und unter welchen Bedingungen. Dieses Beispiel zeigt dennoch, dass der Datenraum einen zentralen Zugangspunkt bietet, der alle Daten schnell auffindbar macht. Im Krisenfall lässt sich so rasch ein belastbares, aktuelles und lokales Lagebild erstellen.

Bibliografie

acatech (Ed.). (2014). *Resilien-Tech. 'Resilience-by-Design': Strategie für die technologischen Zukunftsthemen.* https://www.acatech.de/publikation/resilien-tech-resilience-by-design-strategie-fuer-die-technologischen-zukunftsthemen/

Brousseau, E., Eustache, L., & Toledano, J. (2024). *Position Paper: Economics of Data Sharing.* https://gaia-x.eu/wp-content/uploads/2024/03/Study-on-the-emergence-and-creation-of-value-within-data.pdf

Brucke, M., Schöngut, W., Siegfried, T., & Wienand, K. (Eds.). (2024). *Kursbestimmung: Gaia-X und die Zukunft der datenzentrierten Verwaltung.* Gaia-X Hub Deutschland. https://gaia-x-hub.de/positionspapier/pp-gx-datenzentrierte-verwaltung/

Bundesamt für Kartographie und Geodäsie. (2024). *Digitale Geländemodelle.* https://gdz.bkg.bund.de/index.php/default/digitale-geodaten/digitale-gelandemodelle.html

Bundesministerium des Innern und für Heimat & Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. (2021). *Stärkung des Bevölkerungsschutzes durch Neuausrichtung des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe.* https://www.bbk.bund.de/SharedDocs/Downloads/DE/neuausrichtung.pdf?__blob=publicationFile&v=2

Bundesregierung. (2022). *Deutsche Strategie zur Stärkung der Resilienz gegenüber Katastrophen.* https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/BMI22017-resilienz-katastrophen.pdf?__blob=publicationFile&v=2

Burghardt, L., Klopries, E.-M., & Schüttrumpf, H. (2024). *Structural damage, clogging, collapsing: Analysis of the bridge damage at the rivers Ahr, Inde and Vicht caused by the flood of 2021. Journal of Flood Risk Management, n/a(n/a), e13001.* https://doi.org/10.1111/jfr3.13001

Eclipse Foundation. (2021a). *Eclipse Dataspace Components. GitHub.* https://github.com/eclipse-edc

Eclipse Foundation. (2021b). *Eclipse Dataspace Components | projects.eclipse.org.* https://projects.eclipse.org/projects/technology.edc

Eclipse Foundation. (2025). *Eclipse-edc/FederatedCatalog. Eclipse Dataspace Components.* https://github.com/eclipse-edc/FederatedCatalog *(Original work published 2022)*

EMGLV. (2024). eglv. https://www.eglv.de/

Europäische Kommission. *(2022). Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act).* https://ec.europa.eu/newsroom/dae/redirection/document/83524

Europäische Kommission. *(2023). High-value datasets: Questions and Answers | Shaping Europe's digital future.* https://digital-strategy.ec.europa.eu/en/faqs/high-value-datasets-questions-and-answers

Europäische Kommission. *(2024a). Data Act explained | Shaping Europe's digital future.* https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

Europäische Kommission. *(2024b). Data Governance Act explained | Shaping Europe's digital future.* https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained

Europäische Kommission. (2024c). *Europäischer Raum für Gesundheitsdaten (EHDS).* https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_de

Europäische Kommission. (2024d). *Factsheet: Europäischer Raum für Gesundheitsdaten.* https://ec.europa.eu/commission/presscorner/api/files/attachment/878471/Factsheet%20European%20Health%20Data%20Space_DE.pdf

Europäische Kommission. (2024e). *Q&A on the European Health Data Space [Text]. European Commission - European Commission.* https://ec.europa.eu/commission/presscorner/detail/en/qanda_24_2251

European Commission & Trasys International. (2022). *Study on an infrastructure and data ecosystem supporting the impact assessment of the European health data space. Publications Office.* https://data.europa.eu/doi/10.2875/406794

European Health Data Alliance e.V. (2025). https://ehda-ev.eu/

FITKO. (2020). *Deutsche Verwaltungscloud-Strategie—Föderaler Ansatz.* https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/Deutsche_Verwaltungscloud_Strategie.pdf;jsessionid=C1FBD15277856AFA0373125071D3B3E3.live862?__blob=publicationFile&v=2

Gaia-X AISBL (Ed.). (2022). *Gaia-X Trust Framework 22.04.* https://gaia-x.eu/wp-content/uploads/2022/05/Gaia-X-Trust-Framework-22.04.pdf

Gaia-X Hub Germany. (2024). *Wie der EU Data Act und Datenräume den Katastrophenschutz stärken.* https://gaia-x-hub.de/gx-essentials/wie-der-eu-data-act-und-datenraeume-den-katastrophenschutz-staerken/

Giussani, G., Steinbuss, S., Gras, N., & Prasse, T. (2024). *Data Connector Report (Version 16.0). International Data Spaces Association.* https://doi.org/10.5281/ZENODO.13838396

HERAKLION Projekt. (2022). https://www.heraklion-projekt.de/

IDSA. (2022). *3.1 Business Layer | IDS Knowledge Base.* https://docs.internationaldataspaces.org/ids-knowledgebase/ids-ram-4/layers-of-the-reference-architecture-model/3-layers-of-the-reference-architecture-model/3-1-business-layer

Karutz, H., Geier, W., & Mitschke, T. (Eds.). (2017). *Bevölkerungsschutz. Springer.* https://doi.org/10.1007/978-3-662-44635-5

OpenDRI. (2022). *Open Data for Resilience Initiative (OpenDRI) | GFDRR.* https://www.gfdrr.org/fr/open-data-resilience-initiative-opendri

Reiberg, A., Niebel, C., & Kraemer, P. *(2022). Was ist ein Datenraum, Gaia-X Hub Germany, White Paper 1/2022 (White Paper 1/2022). Gaia-X Hub Germany.* https://gaia-x-hub.de/publikation/was-ist-ein-datenraum/

Reiberg, A., Appelt, D., Kraemer, P., & Smoleń, A. *(2023). Datentreuhänder, Datenvermittlungsdienste und Gaia-X (White Paper 2/2023). Gaia-X Hub Germany.* https://gaia-x-hub.de/wp-content/uploads/2024/02/WP-GX-Datentreuhaender.pdf

Reiberg, A., Niebel, C., & Schmitz, A.-R. *(2024). Governance von Datenräumen (White Paper 01/2024). Gaia-X Hub Deutschland.* https://gaia-x-hub.de/wp-content/uploads/2024/03/WP-GX-Governance-Datenraeume.pdf

Richtlinie 2012/18/EU *des Europäischen Parlaments und des Rates vom 4. Juli 2012 zur Beherrschung der Gefahren schwerer Unfälle mit gefährlichen Stoffen, zur Änderung und anschließenden Aufhebung der Richtlinie 96/82/EG des RatesText von Bedeutung für den EWR.*

Richtlinie (EU) 2019/1024 *des europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors.*

S. Oliveira, M. I., Barros Lima, G. de F., & Farias Lóscio, B. (2019). *Investigations into Data Ecosystems: A systematic mapping study. Knowledge and Information Systems, 61(2), 589–630.* https://doi.org/10.1007/s10115-018-1323-6

Sautter, J., Kraft, V., Schmitz, H.-C., Cetin, F., Krauß, J., Offterdinger, M., Müller, P.-S., Kupjetz, S. M., Nell, R., Schofer, A., Dietzel, A., Theobald, J. A., Gözcüler, E., & Vrhovac, Z. (2021). *Ein Vorgehensmodell zur Etablierung eines Resilience Data Space als dezentrale Datenbasis für die sichere Gesellschaft am Beispiel von MANV-Übungsdaten. Konferenz 'Mensch und Computer' (MuC) 2021.* https://doi.org/10.18420/muc2021-mci-ws08-372

Schulze, A., Brand, F., Geppert, J., & Böl, G.-F. (2023). *Digital dashboards visualizing public health data: A systematic review. Frontiers in Public Health, 11.* https://doi.org/10.3389/fpubh.2023.999958

Verhulst, S., Zahuranec, A. J., Young, A., & Ramesh, A. (2021). *The Use of Mobility Data for Responding to the COVID-19 Pandemic.* http://mobility.data4covid19.org/files/Data4COVID19_0318.pdf

Verordnung (EU) 2022/868 *des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt).*

Verordnung (EU) 2023/2854 *des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung).*

Wilkinson, M. D., Dumontier, M., Aalbersberg, Ij. J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J.-W., da Silva Santos, L. B., Bourne, P. E., Bouwman, J., Brookes, A. J., Clark, T., Crosas, M., Dillo, I., Dumon, O., Edmunds, S., Evelo, C. T., Finkers, R., … Mons, B. (2016). *The FAIR Guiding Principles for scientific data management and stewardship. Scientific Data, 3(1), Article 1.* https://doi.org/10.1038/sdata.2016.18

World Economic Forum. (2024). *Global Risks Report 2024. https://www.weforum.org/publications/global-risks-report-2024/*