



gaia-x

 Hub Germany



Data spaces for disaster management

A small guide to a data-centred approach

White Paper 1/2025

March 2025

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

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

 **acatech**
DEUTSCHE AKADEMIE DER
TECHNIKWISSENSCHAFTEN

About the series

White papers of the Gaia-X Hub Germany are intended for discourse and exchange of ideas. They reflect the opinions of the authors and not necessarily those of the Gaia-X Association or any other institution of the Gaia-X ecosystem.

Authors

AIT Austrian Institute of Technology GmbH

Bernhard Bürger, Scientist

Fraunhofer Institute for High-Speed Dynamics, Ernst Mach Institute (EMI)

Dr Kai Fischer, Group Leader Robustness and Resilience Analyses

Martin Huschka, Research Associate, Digital Engineering

acatech - German Academy of Science and Engineering

Dr Karl Wienand, Scientific Officer

Publisher

Gaia-X Hub Germany c/o acatech - National Academy of Science and Engineering

Karolinenplatz 4

80333 Munich

Recommended citation

Bürger, B., Fischer, K., Huschka, M., Wienand, K. (2025) Data spaces for disaster management. White Paper 1/2025.

Acknowledgement

The presented work results from a cooperation with the Gaia-X Hub Austria and is funded in part by the German Ministry of Education and Research (BMBF) within the program “Research for Civil Security” (www.sifo.de) on the project HERAKLION (www.heraklion-projekt.de, Vertrags-Nr. 13N16293).

Table of contents

Summary	3
1. Data and disaster management	4
2. Legal framework	5
2.1. Disaster management in Germany	5
2.2. Obligations to share data.....	6
2.3. Opportunities for the implementation of data infrastructures	7
3. A Data-centred disaster management.....	8
3.1. Participants	9
3.2. Data categories and data use	11
3.3. Data space solutions	12
3.4. Governance for a disaster management data space	14
4. Use case: The HERAKLION resilience data space	15
4.1. Data space-supported preparation for levee breach	15
4.2. Technical implementation of the use case using a data space	17
Bibliography	19

Summary

This White Paper examines the potential of data spaces in disaster management, using Germany as an example. Local emergency services, municipalities and higher levels of government need to work together in emergencies. However, a fragmented IT landscape and interoperability issues often hinder this coordination.

Data spaces offer a promising solution. They are decentralised, federated systems that securely and efficiently connect different data sources, meeting the needs of many possible actors. These features are crucial in the context of disaster management, in which emergency services, private companies, research institutions, and private citizens combine in ever-changing constellations. The exchanged data are also diverse. These fall into three broad categories: open data, protected data from public bodies, and protected data held by companies or relating to private individuals. This categorisation helps to optimally design the systems for data protection and sovereignty.

Actors in the disaster management ecosystem gain many advantages from data spaces. For example, authorities can deploy them to increase the efficiency in communication and coordination between the decision-making levels, or to improve crisis prevention, e.g. through simulations. Data availability also improves preparedness and communication among emergency responders, reducing response times. In private companies, using data spaces reduces compliance costs, for example those incurred under the EU Data Act (DA). Furthermore, companies gain access to new markets and develop new business models – particularly by providing data-based services.

Recent crises – such as the floods of 2021 and 2024 and the COVID-19 pandemic – highlight the urgent need for data-based and flexible strategies to prepare for and manage crises. An example from the HERAKLION project shows the potential of data use for crisis management. The use case focuses on a flood scenario and demonstrates how geodata, terrain models, and regional statistics combine to improve preparedness, response, and recovery.

1. Data and disaster management

Decision-making in the public sector benefits enormously from data, particularly in situations with high complexity, tight deadlines, and far-reaching consequences. Public emergencies fall into this category. In crisis situations, early warnings, quick decisions, and immediate reactions avoid grave consequences. Moreover, because modern society is technologically advanced and globally networked, public emergencies may trigger intricate and unpredictable chains of consequences. The Covid-19 pandemic and the floods of recent years – such as that in Ahrtal in 2021 or in Catalonia in autumn 2024 – exemplify such severe events, with significant, lasting impacts on society and politics. Climate change makes these extreme events even more frequent (World Economic Forum, 2024). Communities must then become more resilient, to respond to the crises, minimise their impact, and quickly recover (acatech, 2014). Data constitute therefore a critical resource for resilience worldwide (OpenDRI, 2022).

A winding path leads from raw data to actionable information: data from various sources must be combined, evaluated, and contextualised. Visualisations and dashboards, for example, help bundle the most important information and facilitate decisions (Schulze et al., 2023). In practice, however, using and sharing data often faces steep technical and organisational challenges.

Many of them stem from the diversity of actors involved in collecting, processing, and using the data. This diversity is on display in German disaster management, a complex and multi-layered system. Municipalities, cities, and districts form the operational basis (Karutz et al., 2017), while authorities at the level of Federal States have the strategic lead, especially during more serious incidents. Many other stakeholders, from research institutions to private companies, are involved in or affected by the planning or response measures. Such diversity of players hinders data availability. To contrast this, participants would need to network closely and adopt reliable exchange processes – two conditions seldom satisfied in practice (BMI & BBK, 2021).

This White Paper provides an overview of the use of data in disaster management and shows how data spaces provide a solution for a trustworthy use of data. Section 2 presents the relevant legal framework at the German and European level. Section 3 contains an analysis of the data ecosystem of disaster management: the role of participants, the categories of data they use, and the governance issues. The Section focuses on the solutions offered by data spaces. Finally, in Section 4, a use case on flood management illustrates the practical implementation of a data space solution.

Data ecosystems and data spaces

A data ecosystem is a socio-technical network in which actors interact to find, archive, publish, consume, or reuse data as well as to foster innovation, create value, and support new businesses (S. Oliveira et al., 2019).

A data space is a federated, open infrastructure for sovereign data exchange based on common agreements, rules and standards (Reiberg et al., 2022). From a technical perspective, it is based on distributed data storage and demand-orientated integration (data europa academy, 2023). Therefore, a data space can represent the base infrastructure for a data ecosystem (s. Section 3.3)

2. Legal framework

2.1. Disaster management in Germany

Before improving the data exchange, it is necessary to consider the constellation of actors in disaster management. This section shows the essential legal foundations of the cooperation between these actors.

The German civil protection encompasses many organisations at all administrative levels: Federal Government, federal States, and municipalities. The federal government coordinates protection against military threats (so-called “civil defence”). In other cases, its involvement is only indirect or very limited. The federal States regulate prevention and response to extreme weather, floods, infectious disease outbreaks, fires, and other disasters. All States organise response following the same general scheme: the local fire brigade and police, the Red Cross, private aid organisations, and spontaneous helpers operationally respond to the emergency. Local authorities and municipalities coordinate, organise and manage the operations, during both the preparation and the response phase. If the crisis exceeds the capacities of the local emergency, the municipal authorities declare a state of emergency and form a crisis committee. If necessary, resources can be brought in from neighbouring municipalities, the district, the federal State and, in particularly serious events, the Federal Government or the EU. The Federal Office of Civil Protection and Disaster Assistance (German: *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe*, short BBK) advises at all levels, coordinates the cooperation between the federal and state governments, takes precautionary measures for crisis situations, draws up risk analyses, and issues warnings.

What is a catastrophe?

A catastrophe is an event that threatens the lives and health of many people and animals, the environment, significant material assets, or the vital supply of the population to such an extent that the coordinated cooperation of various services is required to combat and avert it (German Federal Government, 2022).

2.2. Obligations to share data

The data exchange necessary for a data-centred disaster management relies on legal foundations at the level of federal States, the Federal Government, and the EU. These regulate several aspects of the exchange. This section examines in particular the obligations to share data.

Critical infrastructures are particularly affected by these obligations. These are, in Germany, facilities “of great importance for the functioning of the community, as their partial or complete disruption would result in significant supply bottlenecks or threats to public safety” (§2 (10) BSIG). The cooperation between the operators of such infrastructures and the disaster planning is therefore essential, to which end the operators are subject to specific requirements. These measures would also facilitate the integration of critical infrastructures operators into a data ecosystem. For example, they are usually required to cooperate with disaster control authorities, to be able to continue operations in the event of partial or complete disruption in other critical infrastructures (cf. e.g. §28 (2) KatSG, Berlin). To this end, State law in Saxony, for example, obligates operators of critical infrastructures to provide relevant data (§ 45a SächsBRKG). In Lower Saxony, they must take organisational and technical precautions (§ 5a NKatSG). Both mandates can directly or indirectly create a basis to integrate critical infrastructure operators in a data ecosystem with public authorities.

At the EU level, the Data Act (Regulation 2023/2854) introduced a new framework for the exchange of data between companies and public sector bodies¹ (see Table 1), particularly in the event of a disaster. According to Chapter V of the DA, authorities can request non-personal data from companies, if relevant for disaster response (Europäische Kommission, 2024a). Personal data may also be requested, but only if there is a demonstrable need and only under additional protective measures. Authorities may also make the data received available to non-profit research organisations and statistical offices or have it processed by third-party providers. Upon receiving a data access request, companies are required to check its conformity and appropriateness (Gaia-X Hub Germany, 2024). In practice, individually reviewing each request will likely present a significant burden for companies. An underlying data space infrastructure for the exchange would significantly alleviate this burden. This is due to the overarching framework conditions for the use of data, on which data spaces rely.

¹ In the following, the terms “authorities” and “public sector bodies” are used interchangeably. However, note that the Data Act defines “public sector bodies” more broadly than “authorities”. Public sectors bodies are in fact defined as “national, regional or local authorities [...] and bodies governed by public law [...], or associations formed by one or more such authorities or [...] bodies” (Art. 2(28), DA).

Table 1: Data sharing before and after the Data Act

<i>Before the Data Act</i>	<i>After the Data Act</i>
Authorities must persuade companies to provide data	Companies must justify their refusal to provide data
Data use is based on bilateral agreements	Established, standardised basic regulation for data use
Unclear procedures for negotiations, complaints, and appeals	Defined negotiation procedures and clear responsibilities for complaints and appeals

EU regulations also force public authorities to make important data available. According to the Open Data Directive (Directive 2019/1024), for example, authorities must publish much data as open data (see Section 3.2). This includes especially “high-value datasets” such as meteorological data, satellite images and local and national maps (European Commission, 2023). A data-centred disaster management also generates large amounts of data that cannot be made public as open data, although in public hands – for example of public authorities, emergency services, or healthcare organisations. These data could benefit the entire data ecosystem. The Data Governance Act (DGA for short, Regulation 2022/868) requires public sector to make this data available for research purposes (European Commission, 2024b).

2.3. Opportunities for the implementation of data infrastructures

Data spaces lend themselves particularly well to promote data exchange and to create dynamic data ecosystems (see Section 3.3). Both national and European laws provide grounds for their establishment in the disaster management context.

Establishing data infrastructures, such as data spaces, is not expressly provided for in German federal State laws on disaster management. However, infrastructures for data exchange can be considered “preparatory measures”, for example to reports damages or to draft of response plans. The disaster management laws of some federal States have experimental clauses, which allow to authorise projects in deviation from the applicable law to test new disaster management concepts (e.g. §7 LKatSG in Baden-Württemberg or §30b BremHilfeG in Bremen). Such provisions can significantly accelerate the testing and establishment of data infrastructures. The regulations on data sharing for operators of critical infrastructures can also facilitate the establishment of a data ecosystem for disaster management.

Within such an ecosystem would flow much sensitive data. Securely using data demands appropriate protective measures. The Data Governance Act (Regulation 2022/868) sets provisions to facilitate the secure reuse of such data. For example, the DGA formalises data trustees which, among other things, ensure the secure use of particularly sensitive data (Reiberg et al., 2023).

Data trustees

Data trustees manage and protect data or rights to data on behalf of others. In the course of their work, data trustees gain control over data to make them accessible to data consumers or third parties. Data trustees offer several useful functions for disaster management:

1. Aggregation of data (e.g. from different companies)
2. Anonymisation and pseudonymisation of personal data
3. Protected computing: sensitive data is transferred to a protected environment where processing takes place, after which only the results of the analysis are provided as output.

3. A Data-centred disaster management

The previous sections showed the importance of data in disaster management and the essential legal background for their exchange and use. Reaping the full benefits of data requires a comprehensive data ecosystem. This section presents an overview of what kinds of data and actors could come into play to build such an ecosystem. As it will become clear, constructing this ecosystem presents singular challenges, for which data spaces offer efficient solutions.

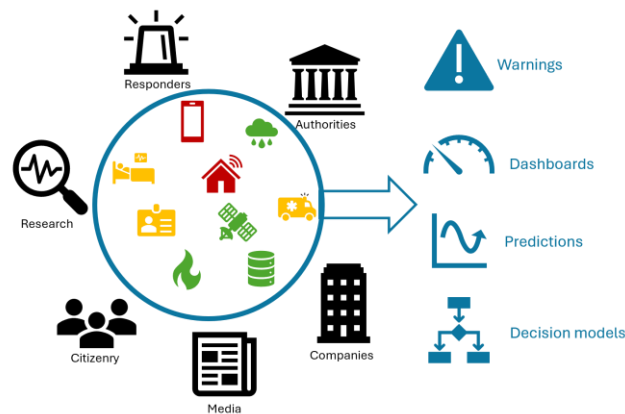


Figure 1: Participants, data and results of a data space for disaster management.

Figure 1 outlines what the actors and data could assemble in a data ecosystem for disaster management. It also shows what opportunities this confluence of actors and data opens. The figure provides a general overview: depending on the use case, each element can assume different forms and should be considered in more detail (see e.g. Sautter et al., 2021).

Possible participants go beyond the entities with legal mandates in crisis management – i.e. the public administration and the emergency services. Research organisations, private companies, the media, and the general public could also fruitfully join the ecosystem. Each of these could participate in different ways, providing or using different types of data. These include publicly available data (green symbols), such as weather data or satellite pictures. In contrast, public sector bodies hold much relevant data, which cannot be published (yellow symbols). Operations data from emergency services and hospital beds availability, for example, require restrictions because of data security or privacy protection. Finally, personal

data or private enterprise data (red symbols), such as data from so-called “smart devices” or smartphones, need further protection. On the one side, these could be private personal data, on the other, they could include intellectual property. Taken together, these data form the basis for analyses, simulations, and forecasts, which can be used to issue early warnings or to support the decision-making processes.

3.1. Participants

This section presents an overview of possible participants in a data ecosystem for disaster management. Not all actors mentioned here are relevant as participants for all use cases. Each of them, in fact, brings different goals and needs as they join the ecosystem, as summarised in Table 2. These range from crisis response (operational or strategic) and information pooling to economic interests – such as efficiency gains or monetary savings.

Some data providers have contrasting needs. On the one hand, most participants need some form of data protection – of trade secrets or intellectual property, as well as personal data or the deployment of emergency responders. On the other hand, public sector bodies and research institutions must fulfil legal obligations regarding data availability. The Data Governance Act (DGA) and the Open Data Directive, for example, require these categories to make much of their data public and facilitate access to the rest of the data (see Sections 2.2 and 3.2).

As data consumers, all ecosystem participants need fast and simple data access. Whether public sector bodies, media or companies, no one should have to deal with cumbersome interfaces. In part because of lacking technical skills and data literacy, but much more because technical obstacles reduce response efficiency. The interoperability of data, formats and software solutions play a crucial role in lowering the thresholds for data use. Finally, the trustworthiness of data sources is paramount for certain stakeholders (especially public sector bodies and emergency services), who need to act quickly in crises and lack the time to check data and sources. In this respect, data spaces (see Section 3.3) offer several advantages. Here, data is readily and reliably available and accessible. A catalogue collects the data offerings and automatically compares their terms of use with the intended use. Furthermore, data spaces use certified identities, requiring little to none further verification during the crisis.

Table 2: Who might participate in a disaster management ecosystem and what are their needs

<i>Participants</i>	<i>Goals</i>	<i>Needs as data providers</i>
<i>Local disaster management authorities (e.g. municipalities)</i>	<ul style="list-style-type: none"> • Create prevention and preparedness measures, based on available data, tailored to specific needs and hazards in the region of responsibility • Coordinate and supervise disaster operations, using data on crisis development and available emergency response resources 	<ul style="list-style-type: none"> • Reusability of data (according to DGA, Open Data Directive) • Protection of sensitive and personal data • Direct, low-threshold data exchange with other participants

	<ul style="list-style-type: none"> • Liaise with local response organisations and with higher disaster management authority • Rapidly estimate and pay damage relief compensations 	
<i>Higher disaster management authorities (e.g. federal States)</i>	<ul style="list-style-type: none"> • Steer disaster management strategy • Identify areas for improvement • Liaise with emergency response organisations at (supra)regional level, lower disaster control authority, and federal agencies • Issue early warnings to the population via various channels (cell broadcast, siren, social media, etc.) 	<ul style="list-style-type: none"> • Reusability of data (according to DGA, Open Data Directive) • Protection of sensitive and personal data • Direct, low-threshold option to transfer data to other relevant participants
<i>Emergency services (e.g. fire brigade, emergency response organisations)</i>	<ul style="list-style-type: none"> • Plan and evaluate tactical plans and personnel deployment • Coordinate operations, as directed by relevant authorities 	<ul style="list-style-type: none"> • Protection of sensitive and personal data • Transfer data to other participants
<i>Citizenry</i>	<ul style="list-style-type: none"> • Protect self and property in disaster situation • Get up-to-date information • Easily apply for damage relief compensation • Volunteer to assist response 	<ul style="list-style-type: none"> • Protection of personal data • Transparent use of provided data • Low-threshold, secure channels for autonomous data sharing (e.g. data altruism, according to DGA)
<i>Research institutions, analysis providers</i>	<ul style="list-style-type: none"> • Analyse rare events to obtain a valid data basis for research work 	<ul style="list-style-type: none"> • Reusability of data (according to DGA, Open Data Directive) • Protection of sensitive and personal data
<i>Media</i>	<ul style="list-style-type: none"> • Inform and warn accurately and timely • Quickly access relevant information 	<ul style="list-style-type: none"> • Availability, findability, interoperability of data
<i>Operators of critical infrastructures (e.g. utility companies)</i>	<ul style="list-style-type: none"> • Assess risks • Continue operations despite disruptions (also of other infrastructures) 	<ul style="list-style-type: none"> • Easy cooperation with authorities • Protection of sensitive data • Transparent use of provided data
<i>Insurance companies</i>	<ul style="list-style-type: none"> • Pay compensation quickly and accurately • Assess risks 	<ul style="list-style-type: none"> • Easy cooperation with authorities • Protection of sensitive data • Transparent use of provided data

Effective and trustworthy data exchange increases the efficiency of disaster relief. For example, local authorities improve their preparedness, but can also process damage compensation payments more quickly and easily. For emergency services, efficiency gains manifest themselves as better preparation, faster triage of cases, improved communication and coordination (including with spontaneous helpers). Taken together, these gains ultimately lead to faster response times. The more extensive the available data, the greater the benefits, for example of personalised dashboards and AI-aided decision models.

Private companies also gain efficiency. Operators of critical infrastructures, for example, exchange data more easily with the authorities. This may significantly reduce compliance costs for legally required data sharing. Having established channels to communicate with authorities, with clear and predefined rules also reduces the costs to comply with the Data Act

(see Section 2.2). Insurance companies can leverage findable and accessible data to process damage claims faster and more accurately (see Section 4.1). Finally, data availability makes innovative and value-added services possible, such as simulations, dashboards, and AI-based tools.

3.2. Data categories and data use

This section provides an overview of what kinds of data are exchanged in a disaster management ecosystem. Figure 1 shows how diverse this data can be. Well-planned strategy, tailored to the specific use cases will determine which data types to include. The participants, the data they can provide, and their goals also play crucial roles.

Table 3 classifies data in three categories, depending on the level of protection or availability they require. These categories are: Open data, restricted public sector data and private data. Open data are publicly accessible and freely usable data. The Open Data licence allows to process, combine, and distribute them for any purpose. The Open Data Directive mandates public sector bodies to provide under this licence much relevant data for disaster management (see Section 2.2). These data are published on platforms, which can typically be connected to an ecosystem via appropriate interfaces (e.g. APIs²). However, different data sources often make their data available in different formats. Therefore, Open Data often need reformatting to be integrated in the ecosystem.

Public authorities hold much valuable data, such as operation data from police and fire brigades, or patient data from hospitals. However, data protection and data security concerns prevent them from being published as open data. Still, exchanging this type of data is highly beneficial to disaster management. The inconsistent and often lagging digitalisation of administrations significantly hinders meaningful use of these data (Brucke et al., 2024), as became apparent during the COVID-19 pandemic. The Data Governance Act (DGA) create incentives for the administration to make such data available (see Section 2.2). The DGA also mandates strict protective measures and data access control, especially if personal data are involved. For example, personal data should only be available in aggregated, pseudonymised or anonymised form.

Certain crisis situations make data from private companies necessary (European Commission, 2022). For example, only the operating companies can provide data about industrial facilities involving hazardous substances. Private companies often also hold much personal data about citizens, such as location data collected from GPS sensors in smartphones or wearables, or from calls and internet use through mobile networks (Verhulst et al., 2021). Using this data in crisis scenarios poses obvious data protection challenges. Furthermore, the conditions to access, use, and share these data must be negotiated. Specific legislation regulates certain scenarios. The European “Seveso III” Directive (Directive 2012/18), for example, mandates facilities that work with harmful and hazardous substances to share data with authorities. The

² An application programming interface (API) is a part of a software system that enables other programmes to interact with it, e.g. to obtain data.

Data Act (see Section 2.2) also outlines ground rules for authorities to request and use data from private companies.

Table 3: Categorisation of disaster management data

<i>Data category</i>	<i>Examples</i>	<i>Accessibility</i>	<i>Challenges</i>	<i>Relevant laws and guidelines</i>
<i>Open data</i>	Weather, water levels, satellite images	Public	Connecting existing platforms, formats interoperability Heterogeneous data quality	Open Data Directive
<i>Restricted public sector data</i>	Operation data from emergency services, personal data about citizens	Restricted	Data protection and security, digitisation of public authorities	German public sector cloud strategy, GDPR, DGA
<i>Private data</i>	Location data from mobile network, usage data from smart devices	Restricted	Data protections and security (privacy, copyright, and trade secrets), negotiating access conditions	DA, GDPR

A data ecosystem for disaster management must fulfil the requirements of its participants and ensure the appropriate use of different types of data. Data spaces offer practical solutions to this challenge through decentralised, multi-cloud implementation (see Section 3.3). This way, each data holder can determine how to store and distribute their own data, adapting storage and security to the protection requirements of the data. For example, less sensitive data – such as open data – can be cheaply stored, even at hyperscalers (such as Google, AWS or Microsoft). Healthcare organisations, private companies and holders of other protected data, instead, can choose solutions that meet their individual needs.

3.3. Data space solutions

Disaster management substantially benefits when relevant data from diverse participants are connected and made available. Such integration into a data ecosystem may happen in a variety of ways. A centralised platform that collects all relevant data would appear at first glance as a solution. However, such a platform would be unthinkable in the context of disaster management. Firstly, it would pose enormous challenges for data security and data protection. Secondly, all involved parties would need to agree on a joint data management. Finally, private companies would have to be persuaded to contribute their data and relinquish control over them.

In contrast, data spaces are federated (i.e. decentral) infrastructures, in which participants retain control over their data (so-called “data sovereignty”). They decide for example who gains access to their data, for what purposes, time periods, etc. Data spaces open, to the extent that no actor is excluded, if they fulfil the necessary requirements, for example being

part of a certain industry branch. The basic agreements on participation and data use are determined and communicated transparently for the entire data space (see Section 3.4).

Therefore, data spaces differ fundamentally from centralised platforms, such as open data platforms. Data available on such platforms can in fact be used without restriction (see Section 3.2), whereas the use of data in a data space is subject to common rules and specific conditions set by the participants. These conditions may provide for unrestricted use, but do not have to. Furthermore, a data space is not a centralised storage location. Rather, it mediates the exchange between data holders and users. Data spaces can therefore enable open, secure and transparent data use and thus underpin data ecosystems. Their practical implementation for disaster management use cases has also been explored in some previous work (Sautter et al., 2021).

Gaia-X and other data space initiatives offer sovereign environments in which the clearly stated and previously (i.e. before the crisis) agreed-upon rules are automatically enforced (Giussani et al., 2024). This allows to conclude standardised data usage agreements at the click of a mouse, making it easier to create access requests, review them (an obligation for companies under the Data Act, see Section 2.2) and access data.

A data space offers a “one-stop shop” to find data from distributed repositories. It has a central access point but a decentral organisation (Sautter et al., 2021). For example, easily searchable catalogues collect all data and services. Various sources or analysis tools can be integrated, which makes it easier to fulfil the so-called FAIR criteria (Wilkinson et al., 2016), meaning that data are *findable, accessible, interoperable* and *reusable*.

Thanks to open source solutions, standardised data formats and transfer protocols, data spaces increase the efficiency of data exchange (FITKO, 2020). Participating stakeholders can thus easily adopt solutions developed by others, or use and operate existing solutions in a cooperative manner. Data spaces also allow the federation of interoperable instances. This decentralised approach enables local authorities, for example, to each create and operate their own data spaces. Being interoperable, these allow data exchange and programme execution via different systems within the federation, regardless of the specific software solution of each public body involved. Thus, each local solution can not only fulfil specific needs, but also benefit from the network effects of the entire ecosystem. Using several interoperable solutions also reduces the vendor lock-in, i.e. the reliance on individual providers. Depending on external providers with opaque and unpredictable internal decision-making processes would also lead to less transparent and sovereign data use.

Transparency and trust are essential in any data ecosystem. But in disaster scenarios, the trustworthiness of identity of one’s partner is particularly important. Every verification or authentication step costs time and effort, which in a crisis should be better used for the response. Verified identities, such as those of Gaia-X data spaces, create the basis for trust (Gaia-X AISBL, 2022). Thanks to these certifications, if a data provider claims to be a specific organisation, a data user can confidently trust this claim. A data space thus offers a trustworthy environment in which even sensitive data can be exchanged securely. Beside

trusting the identities of each other, participants must be able to trust that rules will be upheld when their data is used. Automated rules enforcement guarantees this. Furthermore, the neutrality of the instances dictating the rules strengthens trust within the data space (see Section 3.4). Participants thus rest assured that the common rules are clear and that they harmonise all interests equally.

3.4. Governance for a disaster management data space

The previous sections emphasised the importance of planning which actors and data to include in a data space, which basic rules apply, and how to implement them technically. Therefore, the instance setting these rules and making these decisions plays a central role in building the data space. These questions are the heart of data space governance, on which this section will focus.

The term “governance” has several definitions. Here, “governance of a data space” describes the coordination of actors involved in or (potentially) affected by what happens in the data space (Reiberg et al., 2024). In most data space initiatives, a single entity plays a central role in governance – this is called the orchestrator. Its tasks include:

- Decide who may participate and how to promote or subsidise participation (in compliance with non-discrimination rules)
- Determine which services enable and facilitate the interaction of participants and who provides them
- Estimate operational costs and regulate how to cover them

Particularly important participants or ad-hoc bodies can take on the role of orchestrator (Brousseau et al., 2024). During the initial phases of building a disaster management data space, central figures from the public administration (such as municipalities, federal states or water management companies) would likely act as orchestrators. However, in the long term these lose their dominant role. On the one hand, growing numbers and diversity of participants increase the need for collegial decision-making processes and neutral decision-making bodies (Brousseau et al., 2024). On the other hand, a disaster management data space may develop by federating several smaller local data spaces, or be designed to be cross-border from the outset.

Therefore, commissioning an existing organisation as an orchestrator is likely inadvisable in the long term. Usually, a dedicated organisation will become necessary to assemble the data space participants and operators and allow them to participate in the decision-making. In this context, key interest groups – such as local authorities, certain companies, or industry sectors – will need special attention.

Public funding and regulations support many existing data space projects. For example, the European Commission anchored the European Health Data Space (EHDS) in its strategy to strengthen the health sector (European Commission, 2024c). As would be the case with a disaster management data space, the EHDS involves sensitive data, with a combination of participants from the public and private sectors within a strictly regulated sector, and it has a

strong focus on the common good (European Commission, 2024d). The EHDS governance relies on several bodies at EU and national level (European Commission & Trasys International, 2022). The former define the overall strategy and guidelines, while the latter (e.g. the EHDA e.V. in Germany) coordinate the implementation of these guidelines in their respective countries (European Commission, 2024e; European Health Data Alliance e.V., 2025).

4. Use case: The HERAKLION resilience data space

The previous sections of this paper presented an abstract framework for data ecosystems in disaster management, with a focus on the use of data spaces. A practical example will put these concepts in concrete terms and make the contribution of data to disaster management tangible. This section presents a use case from the project HERAKLION, funded by the German Federal Ministry for Education and Research (Bundesministerium für Bildung und Forschung, or BMBF for short). The project develops a scalable data space to support decision making for local authorities and emergency services during crises. At the same time, the data space simplifies the analysis key factors in extreme weather or pandemic crises. This analysis allows to recognise such events earlier and manage them more efficiently. The example of a flood event shows how integrating and linking heterogeneous data sources in the data space optimises decision-making processes in disaster management (HERAKLION Project, 2022). The example addresses the following key questions:

- How to best prepare for future events?
- How to use data to understand causal relations?
- How to identify weaknesses and vulnerabilities?

4.1. Data space-supported preparation for levee breach

Recent flood disasters illustrate the threat natural disasters pose to population and infrastructures are to natural hazards. The devastating flood in Ahrtal of 2021 not only caused personal damage, but also caused major disruptions in the transport infrastructure (Burghardt et al., 2024), with far-reaching effects that extended well beyond the region. The following example uses data from, among others, the Emschergenossenschaft/Lippenverband to simulate a levee breach and show how data helps prepare for disasters.

The Emschergenossenschaft/Lippeverband is a waterway manager. Among its task is the flood management along the rivers Emscher and Lippe (EMGLV, 2024). This example considers various flood scenarios and possible levee breaches. To this end, the waterway manager carries out hydrodynamic simulations to identify vulnerable areas within a municipality. For a comprehensive analysis, local information on the flood area is combined with other data from a wide range of sources:

- Regional statistics for information on the population structure.
- Digital terrain, building and landscape models for information on topography and development.

- Other geodata for information on transport networks or points of interest (for example important facilities or infrastructures).

Based on these data, simulations show which roads would become flooded and consequently the reachability of different areas. This provides a crucial information basis for emergency relief during the crisis. Figure 2 shows the results of simulations on the accessibility of a hospital. From areas coloured green areas, the hospital can be reached with a short journey (high accessibility). From red areas, on the other hand, the journey to the hospital takes longer (low accessibility). An algorithm calculates the journey duration for the entire considered region. The left panel in Figure 2 shows the situation in normal situations: the hospital is easily accessible from the whole area. The middle panel shows what area the hydrodynamic simulation predicts will be flooded. The right panel combines these two sets of data. It shows what roads become flooded and untraversable, and how this affects the accessibility of the hospital. The image quickly visualises potential bottlenecks, allowing to take them into account when planning the response. This newly developed methodology combines different data sets and can be used efficiently for any point in the map.

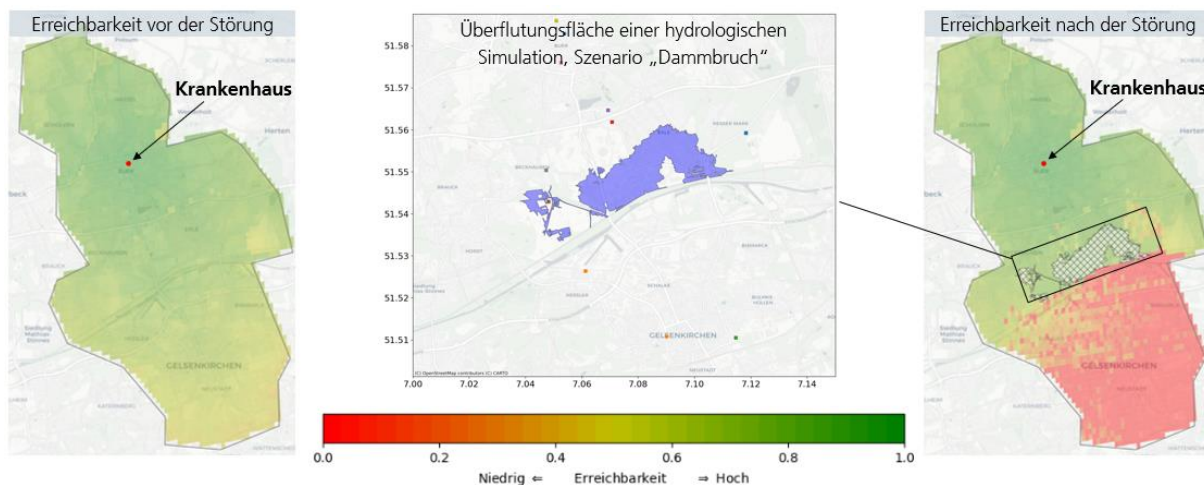


Figure 2: Combination of three data sources (flood simulation, road network, points of interest) to analyse accessibility before and after a flood event. Left: accessibility of a hospital before the flood event. Middle: flooded area as predicted by simulations. Right: accessibility of the hospital after the predicted flooding.

The flooded area in Figure 2 only shows the affected area in two dimensions. This analysis can be further enriched with the data from a digital terrain model, for example with information from the Federal Agency for Cartography and Geodesy (Bundesamt für Kartographie und Geodäsie, BKG) (BKG, 2024). This combination, for example, allow to estimate water levels in the flooded area, as shown in the left panel of Figure 3. With this information it becomes possible to assess potential damages. The right panel in Figure 3 shows for example the expected monetary damage. This information is relevant and valuable both for municipal decision-makers, and for insurance companies.

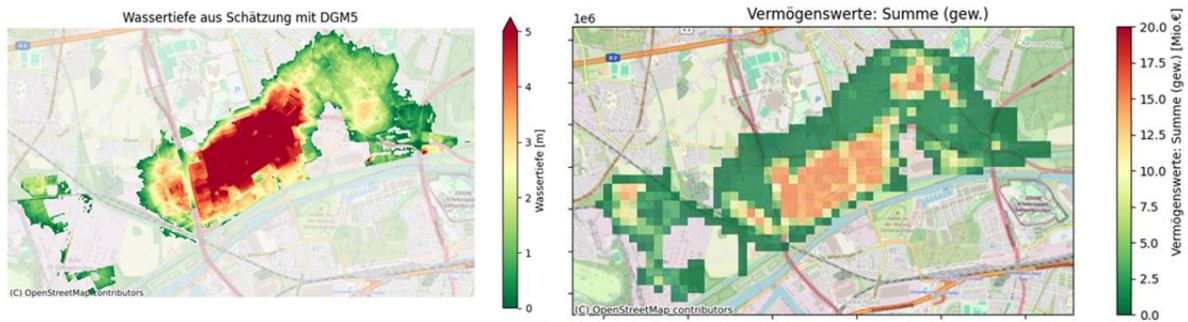


Figure 3: Estimation of the flood height (in metres, left) and the expected monetary damage (in Millions €, right) in the flooded area.

In conclusion, the data space allows to integrate and analyse data of heterogeneous types and provenance. This information is efficiently collected to improve decision-making in the event of a disaster. In this example, the analyses mainly contributed to preparations before the crisis: forecasting possible events and identifying weaknesses. During a crisis, these preparations will facilitate more targeted and efficient interventions to minimise potential damage and reduce response times.

4.2. Technical implementation of the use case using a data space

The previous section presented a use case to illustrate the potential of data space applications. This section examines how the use case can be implemented technically. Figure 4 shows a simplified representation of the business layer of the HERAKLION resilience data space, based on the IDSA standard (IDSA, 2022). The standard classifies participants based on their roles: data users and consumers (on the left side of the sketch), data holders and providers (on the right side of the sketch), and a broker service that enables metadata-based browsing of the data available in the data space.

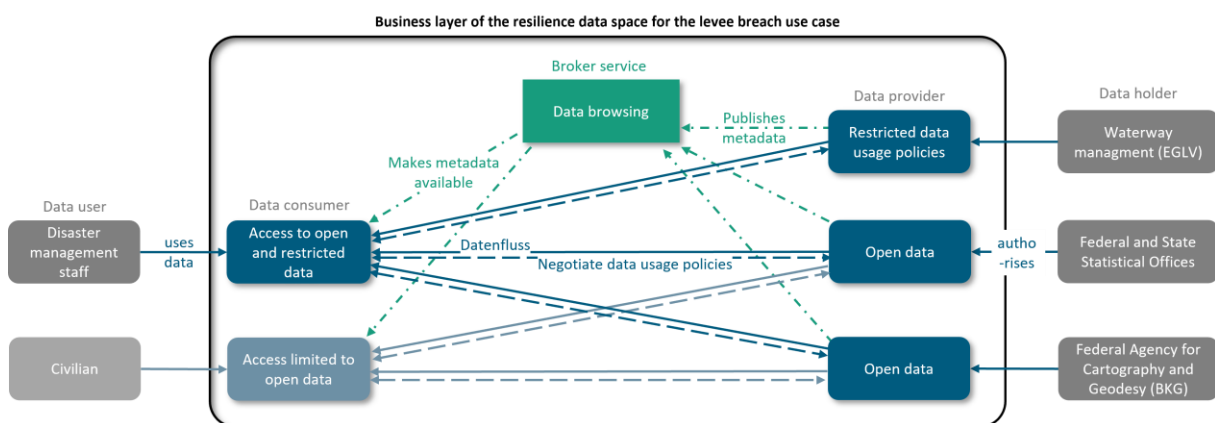


Figure 4: Role allocation according to the IDSA standard for the flood protection use case.

To practically understand these roles, let us consider the levee breach scenario from section 4.1 and a member of the municipal disaster management staff using the data space. Their central access point is an interface based on the Eclipse Dataspace Components (Eclipse Foundation, 2021a, 2021b). To actively participate, the staffer uses their certified identities. Once they are granted access, they become active in the data space as data consumers.

Each data space participant has a verified identity, which regulates their data access. For example, disaster management personnel have access to the data they need for their analyses

in the event of a crisis – even such data has restricted access or usage guidelines and is not publicly available. Civilian users, too, can enter the data space as consumers using their own interface and identity. However, they only have access to publicly available data without usage restrictions. Identity certification and verification therefore create trust among all participants. Thus, the data space strengthens municipal resilience by providing reliable data and promoting robust analyses.

Civilian users' access will be restricted to open data, which is available also outside the data space. However, the data space safeguards the FAIR data principles: all relevant data can be found quickly, retrieved automatically, and combined in an interoperable way, thanks to uniform data and metadata standards. This provides clear benefits to all participants. In fact, civilian data consumers gain not only data access, but can also quickly analyse distributed data, for example to better protect their own property against extreme weather.

A broker service based on the Federated Catalog (Eclipse Foundation, 2022/2025) allows data consumers to browse the data available to them. Automated agents continuously update the catalogued metadata to ensure accurate information. Data quality metrics supplement the metadata, providing data consumers with additional information on reliability, completeness and resolution (both spatial and temporal) of the data. This enables consumers to assess the reliability of the data.

The right side of Figure 4 shows various data holders. These can use their certified identities to enter the data space as data providers. To this end, they use their own interfaces, based on Eclipse Dataspace Components, to offer data of various categories (see Table 3). In the example of section 4.1, these include, for example, the Emschergerossenschaft/Lippeverband, which provides its simulation results, with restricted usage guidelines. Federal and State Statistical Offices, as well as the BKG offer open data.

Open data can be integrated in the data space directly through the providers' APIs. Restricted data, on the other hand, requires specific technical solutions to ensure compliance with usage guidelines. As this example shows, a data space creates a standardised environment, in which all categories of data can be made available.

A decentralised basic infrastructure underpins the data space: data remains with its original holders. These also retain control over who has access and over the access conditions. Nevertheless, this example shows that the data space offers a centralised access point, through which all data is quickly retrievable. In the event of a crisis, this allows to quickly gain a reliable, up-to-date and localised overview of the situation.

Bibliography

- 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). *Setting the Course: Gaia-X and the Future of data-centric Government.* Gaia-X Hub Germany. <https://gaia-x-hub.de/en/position-paper/pp-gx-data-centric-government/>
- BKG.** (2024). *Digitale Geländemodelle.* <https://gdz.bkg.bund.de/index.php/default/digitale-geodaten/digitale-gelandemodelle.html>
- BMI & BBK.** (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
- 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>
- Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC Text with EEA relevance (2018).
- Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information.
- 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* [Java]. Eclipse Dataspace Components. <https://github.com/eclipse-edc/FederatedCatalog> (Original work published 2022)
- EMGLV.** (2024). *eglv.* <https://www.eglv.de/>
- European Commission.** (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) (SWD(2022) 34 final).* <https://ec.europa.eu/newsroom/dae/redirection/document/83524>
- European Commission.** (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>

- European Commission.** (2024a). *Data Act explained | Shaping Europe's digital future.* <https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained>
- European Commission.** (2024b). *Data Governance Act explained | Shaping Europe's digital future.* <https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained>
- European Commission.** (2024c). *European Health Data Space Regulation (EHDS).* https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en
- European Commission.** (2024d). *Factsheet: European Health Data Space.* https://ec.europa.eu/commission/presscorner/api/files/attachment/878490/Factsheet%20European%20Health%20Data%20Space_DE.pdf
- European Commission.** (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 & Trasy 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, (Föderale IT Kooperation).** (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/>
- German Federal Government.** (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
- 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 Project.** (2022). https://www.heraklion-projekt.de/?page_id=528&lang=en
- IDS.** (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.gfdr.org/fr/open-data-resilience-initiative-opensdri>
- Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) <http://data.europa.eu/eli/reg/2022/868/oj/eng>
- Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance), Pub. L. No. 2023/2854 (2023).
- Reiberg, A., Niebel, C., & Kraemer, P.** (2022). *What is a Data Space?, Gaia-X Hub Germany, White Paper 1/2022 (White Paper 1/2022).* Gaia-X Hub Germany. <https://gaia-x-hub.de/en/publication-en/wp-data-space-gaia-x/>
- Reiberg, A., Appelt, D., Kraemer, P., & Smoleń, A.** (2023). *Data trusts, data intermediation services and Gaia-X* (White Paper 2/2023). Gaia-X Hub Germany. <https://gaia-x-hub.de/en/publication-en/wp-data-trusts-gaia-x/>
- 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>
- 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., & Böhl, 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
- 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/>