

Responsible Information Sharing in the era of Big Data Analytics facilitating Digital Economy through the use of Blockchain technology and observing GDPR

Vijon Baraku¹^a, Iraklis Paraskakis^{2,3}^b, Simeon Veloudis^{2,3}^c and Poonam Yadav¹^d

¹*Department of Computer Science, University of York, York, United Kingdom*

²*SEERC - South East European Research Centre, Thessaloniki, Greece*

³*CITY College, University of York Europe Campus, Thessaloniki, Greece*
{qnr509, poonam.yadav}@york.ac.uk, {iparaskakis, sveloudis}@seerc.org

Keywords: Data Sovereignty, Data Ownership, Data Privacy, Ontologies, Blockchain Technology, GDPR

Abstract: In the contemporary digital landscape, the intersection of big data analytics, data ownership, and GDPR compliance emerges as a critical arena. This paper proposes a transformative framework to redefine data control, shifting ownership from entities such as Data Controllers to individuals. Central to this innovation is the proposed novel and disruptive concept of the Data Capsule, empowering individuals to effectively own and thus dictate terms and conditions for their data usage. The Data Capsule framework draws on ontologies, semantic technologies, and blockchain to homogenise heterogeneous data, automate annotation, enforce governance rules, and ensure transparency. By making individuals primary custodians of their data, this paper aims to provide privacy, security, and ethical data handling, counteracting the potential pitfalls of profit-driven practices. This paper outlines a comprehensive research plan, provides a state-of-the-art review, and shows aligning objectives with the system workflow.

1 INTRODUCTION


In the pervasive digital landscape, data stands as the cornerstone of our economy and technological advancements. Yet, the rapid proliferation of data-driven systems has accentuated concerns over privacy, fairness, and regulatory compliance. As our reliance on technology grows, so does the need for stronger data protection as well as benefiting from the monetisation of the data. Data breaches, cyber-attacks, as well as data mismanagement, can result in the theft of personal information, which can be used for identity theft, fraud, and other criminal activities (Fathullah et al., 2022). In some cases, the consequences of a data breach can be devastating and long-lasting, leading to financial losses, reputational damage, and loss of trust (Schlackl et al., 2022) (Tawalbeh et al., 2020).


This paper responds to this imperative by introducing a pioneering framework that not only ensures strict adherence to prevailing regulations like GDPR,


Data Governance Act, Data Act, and the Artificial Intelligence Act but fundamentally redefines the treatment of personal data, placing explicit emphasis on individual rights.


This research draws inspiration from the unsettling concept of “Surveillance Capitalism,” as elucidated in (Zuboff and Schwandt, 2019). The rise of digital technology has birthed a novel form of capitalism, where corporations collect and monetise personal data on an unprecedented scale. These data, often referred to as “exhaust” or residual data, hold immense value in predictive analytics, forming the bedrock of the prediction industry in the digital society era (Zuboff and Schwandt, 2019). This new paradigm, however, tips the balance of power in favor of corporations, raising formidable challenges to individual privacy, autonomy, and broader democratic ideals.

Motivated by the burgeoning importance of data in our daily lives and the escalating challenges of data breaches and privacy infringements, this paper seeks to explore a comprehensive solution. Beyond mere alignment with GDPR objectives, it acknowledges and addresses the limitations of current practices. The

^a <https://orcid.org/0009-0005-8411-2548>

^b <https://orcid.org/0000-0002-8031-0775>

^c <https://orcid.org/0000-0002-8197-6667>

^d <https://orcid.org/0000-0003-0169-0704>

proposed framework pivots around the novel and disruptive concept of the **Data Capsule** intending to empower individuals as the primary custodians of their data, effectively shifting control away from conventional entities such as typical Data Controllers.

In the ensuing sections, this paper meticulously unveils the intricacies of the proposed framework. It delineates research objectives, explores the potential impact of the framework on responsible and individual-centric data management, and outlines a structured plan for implementation. By delving into data homogenisation, efficient annotation, governance rule definition, and the integration of blockchain technology, this research aspires to foster a paradigm shift towards a secure, transparent, and ethical data ecosystem.

2 BACKGROUND AND THE CURRENT DEVELOPMENTS

Through a comprehensive review of existing literature, this background sets the stage for the proposed framework, which endeavours to redefine data control and empower individuals in the digital age. Additionally, the current developments in the field are presented and discussed.

2.1 Data ownership and the GDPR

In the rapidly evolving digital landscape, the issue of data ownership has become paramount. Data, often considered the lifeblood of contemporary society, fuels economic growth and technological advancements (Marr, 2023). However, this surge in data-driven systems has raised pressing concerns regarding privacy, fairness, and regulatory compliance. The General Data Protection Regulation (GDPR), implemented in May 2018, emerges as a pivotal legislative response, aiming to safeguard individuals' fundamental freedoms and rights, especially their right to personal data protection (Parliament and of the Council, 2016).

The GDPR, enacted to address the challenges posed by the digital age, outlines principles for the lawful and transparent processing of personal data. It grants individuals significant rights, including the right to access their data, the right to rectify inaccuracies, and the right to erasure. While GDPR represents a significant step forward in data protection, it is not without its limitations (Sirur et al., 2018). The concept of data ownership primarily lies with Data Controllers, raising concerns about transparency and the true empowerment of individuals over their personal information.

Ownership by the Data Controller implies that organisations and businesses are the owners of other people's data and thus making them responsible for ensuring that the personal data they collect are processed in accordance with the GDPR's principles and provisions. Given that the primary goal of businesses is to maximise profits, this approach can be problematic since it could result in a situation in which individuals are not fully aware of how their personal data are being used, or they may be unable to exercise their GDPR rights, such as the right to access their personal data or the right to have them deleted.

Moreover, the whole existing infrastructure setup can be characterised as reactive and taking corrective actions retrospectively, i.e., after the damage has occurred.

2.2 International Data Spaces Association

The International Data Spaces Association (IDSA) is an initiative with over 140 organisations for the development of a European standard for independent and controlled data sharing. It is a not-for-profit association which creates standards for sharing data in data spaces. These standards aim to facilitate participants into having full control over their data.

The IDS Association's specifications establish the foundation for a vendor-independent data marketplace based on European principles such as data privacy, security, equal opportunities, and data sovereignty. This architecture serves as a strategic link between data generated in the Internet of Things (IoT) and its use in machine learning (ML) and AI algorithms (Bohlen et al., 2018).

Digital responsibility is becoming an important differentiator, and the IDS Reference Architecture Model places the user at the center, ensuring trustworthiness and control over data. This model proposes a standard architecture for sovereign data exchange among partners, regardless of size or financial strength. The IDS Association's goal is to lower entry barriers and associated costs for data sharing while simplifying partner identification, legal governance, and commercial transactions (Bohlen et al., 2018).

The semantic standard for data sovereignty developed by the IDS Association makes it easier to create software-readable contracts that define data usage rules and policies. These contracts, which are governed by use control rules and identify the purpose and cost of data use, allow partners to model, create, monitor, and enforce data-sharing policies.

In summary, the International Data Spaces Association's standards have the potential for developing a

global standard for data interchange, promoting open, safe, and trustworthy data ecosystems.

2.2.1 Dataspaces

A foundational concept used in the architecture of the IDSA is the concept of *Dataspaces*. Dataspaces represent a conceptual paradigm within data management that addresses issues found in data integration systems. The major purpose is to simplify the development of a data integration system by utilizing existing matching and mapping creation techniques (Belhajjame et al., 2010). The strategy stresses gradual enhancements to the system as needed, using a "pay-as-you-go" paradigm. Labor-intensive components of data integration are postponed until they are necessary (Dong and Halevy, 2007).

Traditionally, both data integration and data exchange systems sought to provide functions comparable to those provided by dataspace systems. However, dataspaces represent a step forward in the evolution of data integration architectures and differ from current systems in an important way. Unlike traditional data integration systems, dataspaces do not demand semantic integration before providing services (Franklin et al., 2005). While data in dataspaces may lack a consistent schema and live across numerous host systems, these systems do not require accurate prior knowledge of the relationships between terms in each schema. Dataspaces thereby reduce the initial work necessary for system setup.

The essence of dataspaces is to use a data coexistence approach, which provides fundamental functionality across all data sources, regardless of their level of integration. This strategy marks a change from the traditional model, stressing flexibility and agility in managing multiple data sources (Jimenez et al., 2023).

2.3 Potential use for Blockchains in an International Data Spaces context

The fundamental goal of International Data Spaces (IDS) is to enable controlled data sharing between organizations, regardless of data type. Structured data, such as measurements, product information, or logistics/procurement data, are commonly transferred, but the IDS also enables a wide range of additional (streaming) data. Data owners can use the IDS Connector to control how their data is shared with other IDS ecosystem participants (Steinbuss et al., 2021).

Data sharing in IDS serves several functions, which often fall into two categories in use cases:

1. Feeding new data-driven services: Using data in

innovative apps, complex algorithms, or digital services that mix data from numerous sources.

2. Business process synchronization is the use of data to perform transactions (e.g., exchanging orders), facilitate production (e.g., exchanging product data), check quality (e.g., the temperature of perishable items), or synchronize activities.

Many of these scenarios involve data that leads to transactions, converting the data into a 'shared data asset' with liabilities and duties for participating businesses. This shared data asset could include temperature records, product capabilities, or other pertinent information that is held in a shared environment (Steinbuss et al., 2021).

From a functional aspect, blockchain technology is expected to play an important role in preserving these 'shared data assets' in the IDS context. This builds on the existing IDS design's capacity to share potentially massive datasets via its connector architecture. For example, blockchain can enable data consistency and transparency across a network of businesses, aligning with the IDS methodology for data sovereignty and safe data exchange. This linkage enables enterprises to leverage existing data integration arrangements, such as internal Data Lakes, hence boosting information extraction capabilities (Steinbuss et al., 2021).

When a business community chooses to store shared data assets in a blockchain and make this data available to the IDS ecosystem, there are two scenarios:

1. **Blockchain as a Data Consumer:** In this scenario, specific data from the IDS ecosystem must be registered in a blockchain. For instance, recording a measurement or specific sensor data.
2. **Blockchain as a Data Provider:** In this case, the blockchain stores data that must be made available to other parties in the IDS ecosystem. For example, certain transaction data is recorded on a blockchain.

The IDS architecture adds a critical mechanism for enabling such integration: 'data apps' within a Custom Container. These apps are linked to an IDS Connector, which allows for seamless connection between IDS and other systems. Data apps, for example, can be used to link a Connector to an existing ERP system's REST-API or an OPC-UA interface on a smart device.

Typical blockchain solutions include nodes that synchronize data and link to client apps. These client programs frequently offer an API that allows other systems to access data on the blockchain. IDS 'data applications' communicate with this API, exposing

their functions within the IDS ecosystem. Several data apps have been developed for Hyperledger Fabric in IDS projects, and work on BigChainDB is still ongoing (Steinbuss et al., 2021).

2.4 Positioning in the EU Landscape

Embarking on the Horizon Europe Framework Programme, our research aligns itself with the overarching goals and aspirations set forth by the European Union. The call, which covers digital technologies, structures, and processes, aims to make data operations more user-friendly, secure, and compliant. The technology it calls for would allow for secure data processing, sharing, and reuse within the framework of common European data spaces. Furthermore, the call highlights the convergence of technological and social innovation to promote environmentally responsible data practices.

We are strategically positioning our research within this call to match with the EU's objective of creating a globally attractive, secure, and dynamic data-agile economy and investigate what other research is carried in this area. Our commitment to the development and adoption of next-generation computing and data technologies seeks to promote the European single data market while also contributing to a trustworthy artificial intelligence ecosystem. We are particularly interested in the funded research because the proposed framework has both an academic and an industrial component, given that our work is aimed to be adopted in the commercial world.

Below are some notable initiatives that serve as models within the Horizon Europe framework:

- **Digital Technologies Acting as a Gatekeeper to information and data flows (TANGO)** - seeks to transform cross-sector data exchange by providing a user-friendly, secure, and ecologically sustainable platform. It focuses on establishing trustworthy data-sharing technologies and governance models, enabling users in transport, e-commerce, finance, public administration, tourism, and industry. TANGO improves privacy, lowers expenses, and boosts productivity, helping to create a dependable environment for information and data flows within the GAIA-X and EOSC ecosystems. The initiative is focused on improving data availability, quality, and interoperability across multiple domains and sectors (Nils, 2023). Our framework is similar to TANGO in that both projects aim to establish trustworthy, secure, and compliant data management platforms; however, TANGO focuses on addressing environmental degradation and climate change challenges,

particularly in the context of data centers, whereas our project focuses on data management and privacy concerns in a broader sense through the proposed Data Capsule framework.

- **Trust and privacy preserving computing platform for cross-border federation of data (TRUSTEE)** - seeks to develop a secure and environmentally friendly framework for aggregating transdisciplinary data sources while maintaining privacy and compliance with European regulations. It uses homomorphic encryption to allow researchers to search and use data in the encrypted realm. TRUSTEE enables unified FAIR representation, complicated queries, and trustworthy machine learning workflows. It contributes to a Pan-European federated FAIR and private data ecosystem, having been validated through many use cases (Sayeed et al., 2023).
- **Trustworthy, Energy-Aware federated Data Lakes along the computing continuum (TEADAL)** - strives to transform data analytics by providing foundational technologies for extended data lakes spanning the cloud-edge continuum and multi-cloud settings. TEADAL, which prioritizes performance, energy efficiency, and privacy, allows for reliable and verifiable data flows while maintaining privacy and confidentiality. The technology enables an extended data lake and a mediatorless federation, stressing a collaborative approach to privacy enforcement and energy minimization (Plebani et al., 2023).
- **Green responsible privacy preserving data operations (GLACIATION)** - project targets the rising energy consumption and carbon emissions linked with big data analytics, which span from edge to cloud. It integrates a unique Distributed Knowledge Graph (DKG) into the edge-core-cloud architecture, employing AI to reduce data transit and optimize analytics location. GLACIATION saves a great deal of power by focusing on energy-efficient data processes. The project's Meta Data framework combines privacy and trust considerations, as evidenced by its effectiveness in public service, manufacturing, and enterprise data analytics environments (Carvalho, 2023).
- **New data spaces for green mobility (MobiSpaces)** - aims to create a comprehensive, privacy-preserving data governance platform for urban and maritime mobility. The project's goal is to improve data processing efficiency, security, and fairness by leveraging mobility analytics to extract important insights from sensor data and IoT

devices. MobiSpaces uses Explainable AI (XAI) to construct interpretable prediction models. Validated through five diverse use cases, the project intends to build a data processing standard that will contribute to the expansion of the EU digital economy while also focusing on environmental sustainability (Commission et al., 2022).

While both MobiSpaces and our proposed framework emphasize the importance of effective data governance solutions and individual empowerment in data management, our proposal adopts a broader approach to data management and privacy concerns, whereas MobiSpaces focuses on mobility in both urban and maritime contexts.

After reviewing the progress made by the five EU-funded projects (GLACIATION, MobiSpaces, TANGO, TRUSTEE, and TEADAL), we recognize the importance of their contributions in addressing critical challenges such as data management, privacy preservation, and energy efficiency. In the next section, we will offer our own framework, which is carefully designed to align with and complement the intended objectives of these projects. This framework, while sharing the same goal of improving data technology, will provide new insights and techniques that complement the collective efforts of the aforementioned programs. Our proposed framework is suited to complement the innovative spirit of these projects and contribute to the EU's broader ambition of data and computing technology leadership.

3 PROPOSED FRAMEWORK

In response to the complex challenges presented by data management, privacy concerns, and the inadequacies of existing frameworks, this paper proposes a transformative approach — the **Data Capsule**. Serving as the bedrock of this pioneering framework, the Data Capsule aims to redefine the dynamics of data control, placing individuals as the primary custodians of their personal information. By doing so, it not only ensures seamless compliance with prevailing regulations such as GDPR, Data Governance Act, Data Act, and the Artificial Intelligence Act but also champions a paradigm shift towards responsible, transparent, and individual-centric data handling practices.

3.1 The Data Capsule Concept

3.1.1 Conceptual Foundations

The Data Capsule concept represents a departure from the conventional Data Controller-centric model. In-

spired by the principles of responsible data handling, the framework introduces a novel paradigm where individuals exert unprecedented control over the access and processing of their personal data. This shift in control is pivotal in mitigating the potential pitfalls associated with profit-driven practices and fostering a more ethical and transparent data ecosystem.

3.1.2 Individual Empowerment

At its core, the Data Capsule empowers individuals to become the primary custodians of their personal data. This empowerment involves granting data generators the authority to dictate the terms and conditions under which their data is released and processed. This radical shift aims to democratize data ownership, moving it away from centralized entities and placing it firmly in the hands of those to whom the data truly belongs.

3.2 Empowering Individuals through Classification and Annotation

3.2.1 Granular Data Control

The operationalization of the Data Capsule hinges on endowing individuals with the ability to classify, annotate, and apply policies to their data. Leveraging advanced ontologies and semantic technologies, this framework facilitates a nuanced categorization of data, allowing individuals to specify the nature of their information. From strictly confidential data to information available for sale or free, this granular control ensures that individuals can precisely manage the dissemination and usage of their data.

3.2.2 Ontologies and Semantic Technologies

In realizing the vision of data classification and annotation, the Data Capsule leverages ontologies and semantic technologies. These tools enable individuals to articulate the intricate nuances of their data. Through the use of ontologies, individuals can express the context, relationships, and significance of their data, fostering a more profound understanding of the information they share.

3.3 Blockchain Integration for Transparency and Security

3.3.1 Tamper-Proof Transparency

To fortify the principles of transparency and security, the Data Capsule integrates blockchain technology as an underlying layer. This extends beyond

conventional transparency by ensuring tamper-proof records of data transactions. The decentralized nature of blockchain provides an immutable ledger, creating an unalterable history of data interactions. This feature not only enhances privacy but also establishes a trustworthy digital data ecosystem.

3.3.2 Auditable Trail and Data Provenance

Blockchain’s role extends to providing an auditable trail of data transactions, addressing concerns related to data provenance. Individuals can track the lifecycle of their data, from its generation to every interaction it undergoes. This auditable trail enhances accountability, ensuring that data processors adhere to the agreed-upon terms and conditions. It also instills confidence in individuals, as they can verify the ethical handling of their personal information.

4 RESEARCH OBJECTIVES

The proposed framework aligns seamlessly with specific research objectives, each targeted at critical aspects of responsible and transparent data management. Through these objectives, the *data capsule* idea is to be implemented. These objectives ensure the homogenisation of heterogeneous data, efficient data annotation and classification, the definition of governance rules and policies, and the provision of primitives for complete transparency, provenance, and security.

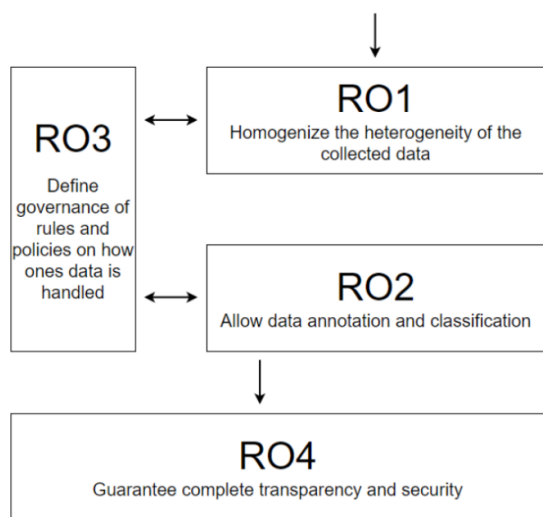


Figure 1: Research objectives alignment with system workflow

4.0.1 RO1 - Define mechanisms to enable the homogenisation of the heterogeneity of the collected data

RO1 is the initial objective given that data comes from numerous heterogeneous sources and in different formats (addressing the variety problem of big data). The current state of the art in homogenising the heterogeneity of acquired data utilize a combination of data integration to a unified schema or ontology, data wrangling, and automated machine learning algorithms (Singh and Singh, 2012). This proposal will extend the current state of the art by investigating methods for developing domain-specific ontologies targeted at empowering the individual, with the objective of enhancing data integration accuracy and efficiency, as well as investigate new automatic data wrangling strategies capable of handling a broader range of data types and representations.

4.0.2 RO2 - Define mechanisms for efficient data annotation and classification

RO2 is important to address aspects and requirements of personal data. Deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), are the current SoA, having revolutionised data annotation and categorization by allowing the development of very accurate models using massive volumes of data.

4.0.3 RO3 - Define governance rules and policies on how one’s data is handled

RO3 is important in allowing for policies and rules to automate the classification done in RO2. XACML, or the eXtensible Access Control Markup Language, is a standard that defines a syntax and semantics for expressing and enforcing access control policies in a distributed environment. The standard defines a policy language for expressing access control policies, as well as a request/response language for making access control decisions based on those policies (Veloudis et al., 2019).

4.0.4 RO4 - Provide primitives to guarantee complete transparency, provenance, and security

RO4 will ensure the transparency, data provenance and security of the designed system. This objective will be facilitated by the use of blockchain technology which will serve as the infrastructure of the proposed system. Although RO4 is called a research objective, it should be noted that the proposed framework merely will utilise blockchain technology as an

underlying infrastructure, and there won't be any further research being done in that area.

By utilising blockchain and particularly Smart Contracts, there will be a well-defined agreement between the individual and the data processor, removing any potential for ambiguity and reducing the chances of misunderstandings (Mohanta et al., 2018). This will enhance security as the terms of the agreement can be easily referenced in case of any disputes, offering an objective basis for resolution.

5 CONCLUSION

In navigating the intricacies of the digital era, where data reigns supreme, this paper has endeavoured to address the pressing concerns surrounding privacy, fairness, and regulatory compliance. The rampant growth of data-driven systems has brought forth challenges such as data breaches, cyber-attacks, and a loss of individual control over personal information. Recognizing the limitations of existing frameworks, we have introduced a transformative solution—the Data Capsule framework.

Inspired by the urgency to empower individuals in the face of Surveillance Capitalism, our framework places data control firmly in the hands of data generators. It goes beyond the confines of traditional models by introducing a paradigm where individuals become the primary custodians of their personal data. The Data Capsule concept is not merely a response to GDPR objectives; it is a disruptive shift that acknowledges and addresses the shortcomings of current practices.

As we navigate the proposed framework, delving into the conceptual foundations of the Data Capsule and its operationalization through granular data control and blockchain integration, it becomes evident that our approach is not just theoretical but it is a tangible and comprehensive solution to the challenges of responsible and transparent data management.

The alignment of research objectives with the system workflow, as illustrated in Figure 1, underscores our commitment to the practical implementation of the Data Capsule framework. Each objective, from homogenising heterogeneous data to providing primitives for transparency and security, contributes to the overarching goal of democratizing data ownership.

In conclusion, the Data Capsule framework offers a new solution in an era where data-driven advancements and privacy concerns seem to be clashing with one another. By redefining the dynamics of data control, we pave the way for a more ethical, transparent, and individual-centric data ecosystem. As we usher

in this transformative framework, we believe it heralds a new era—one where individuals reclaim their rights in the digital landscape, ensuring that the benefits of technological progress are harmoniously balanced with the protection of individual interests.

REFERENCES

- Belhajjame, K., Paton, N. W., Embury, S. M., Fernandes, A. A. A., and Hedeler, C. (2010). Feedback-based annotation, selection and refinement of schema mappings for dataspace. In *Proceedings of the 13th International Conference on Extending Database Technology*, EDBT '10, page 573–584, New York, NY, USA. Association for Computing Machinery.
- Bohlen, V., Bruns, L., Menz, N., Kirstein, F., and Schimpler, S. (2018). Open data spaces: Towards the ids open data ecosystem. *International Data Spaces Association (ed.)*.
- Carvalho (2023). The earth data revolution: Harnessing data for climate insights and the glaciation project.
- Commission, E., for Maritime Affairs, D.-G., and Fisheries (2022). *Public consultation on the EU Maritime Security Strategy – Summary of results – October 2022*. Publications Office of the European Union.
- Dong, X. and Halevy, A. (2007). Indexing dataspace. In *Proceedings of the 2007 ACM SIGMOD International Conference on Management of Data*, SIGMOD '07, page 43–54, New York, NY, USA. Association for Computing Machinery.
- Fathullah, M. A., Subbarao, A., and Muthaiyah, S. (2022). A review of data breach cost in cloud computing. In *Proceedings of the International Conference on Technology and Innovation Management (ICTIM 2022)*, pages 199–209. Atlantis Press.
- Franklin, M., Halevy, A., and Maier, D. (2005). From databases to dataspace: a new abstraction for information management. *SIGMOD Rec.*, 34(4):27–33.
- Jimenez, S., Steinbuss, S., de Roode, M., Papakosta, S., Klinker, P., and Matthijs, P. (2023). Overview and relations of data spaces initiatives, standards, and tools (1.0).
- Marr, B. (2023). Why data is the lifeblood of modern organizations.
- Mohanta, B., Panda, S., and Jena, D. (2018). An overview of smart contract and use cases in blockchain technology.
- Nils, K. (2023). Data economy with tango.
- Parliament, E. and of the Council (2016). Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). Official Journal of the European Union.
- Plebani, P., Kat, R., Pallas, F., Werner, S., Inches, G., Laud, P., and Santiago, R. (2023). Teadal: Trustworthy,

energy-aware federated data lakes along the computing continuum.

- Sayeed, S., Pitropakis, N., Buchanan, W. J., Markakis, E., Papatsaroucha, D., and Politis, I. (2023). Trustee: Towards the creation of secure, trustworthy and privacy-preserving framework. In *Proceedings of the 18th International Conference on Availability, Reliability and Security*, ARES '23, New York, NY, USA. Association for Computing Machinery.
- Schlackl, F., Link, N., and Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. *Information & Management*, 59(4):103638.
- Singh, S. and Singh, N. (2012). Big data analytics. In *2012 International Conference on Communication, Information Computing Technology (ICCICT)*, pages 1–4.
- Sirur, S., Nurse, J. R., and Webb, H. (2018). Are we there yet? understanding the challenges faced in complying with the general data protection regulation (gdpr). In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security*, MPS '18, page 88–95, New York, NY, USA. Association for Computing Machinery.
- Steinbuss, S., Punter, M., Skarbovski, I., Jürjens, P. D. J., and Holtkamp, D. B. (2021). Blockchain technology in ids.
- Tawalbeh, L., Muheidat, F., Tawalbeh, M., and Quwaider, M. (2020). Iot privacy and security: Challenges and solutions. *Applied Sciences*, 10(12):4102.
- Veloudis, S., Paraskakis, I., Petsos, C., Verginadis, Y., Patiniotakis, I., Gouvas, P., and Mentzas, G. (2019). Achieving security-by-design through ontology-driven attribute-based access control in cloud environments. *Future Generation Computer Systems*, 93:373–391.
- Zuboff, S. and Schwandt, K. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books.