Data Collaboration through Privacy-Preserving Computation

SINE Foundation
polytune@sine.foundation

September 25, 2025

Abstract

Access to high-quality data for analysis is the foundation for organizations to make more effective and efficient decisions. Although the necessary data often already exists, this data is managed across different organizations, departments, or IT systems, making it inaccessible.

At the SINE Foundation, we address the support of inter-organizational data collaboration through a specific privacy-enhancing technology (PET), namely secure multi-party computation (MPC). This paper discusses the challenges that organizations face when implementing inter-organizational data collaboration, and explains how MPC can address these challenges. It also presents selected use cases from the public and private sectors in areas such as public services and sustainability.

1 Introduction

Enhancing data access and data collaboration holds significant potential for all societal sectors, particularly for increased economic growth and a more sustainable economy. The EU Data Act, which will grant everyone the universal right to access data from connected devices within the EU-27, will generate economic growth of 2% of GDP (or 270 billion euros annually) according to an EU study [7]. For the provision of data previously accessible only to the public sector (Open Data), the OECD quantifies the direct and indirect value contribution for the EU economic region at 140 billion euros annually [20]. Despite a multitude of studies demonstrating their benefits, a significant share of public and private organizations do not engage in data collaboration practices [20, 15].

This report focuses on **voluntary and inter-organizational data collaboration**, particularly with regard to sensitive and/or high-value data sets. In Section 2, we start with a list of challenges that prevent data collaboration in public and private sectors. In Section 3, we then briefly explain our chosen privacy-enhancing technology, namely secure multi-party computation (MPC), and discuss how MPC can address these challenges. In Section 4, we present SINE's data collaboration framework comprising two main open-source building blocks. Thereafter in Section 5, we discuss potential use cases of this technology we consider, both in the public sector and in sustainability-related data collaboration. In Section 6, we conclude with future directions.

2 Challenges in Data Collaboration

Various challenges complicate the successful implementation of inter-organizational data collaboration in public and private sector organizations. These challenges become more relevant when the data is of higher quality, value, or sensitivity:

Fear of loss of control: Organizations fear losing control over their data, which could cause unforeseen damages [15, 13].

Trade secrets: Private sector organizations in particular are concerned that sharing data could indirectly reveal trade secrets [13].

Data valuation: Companies cite uncertainties in determining the economic value of their data as an impediment to data collaboration and exchange [20, 13].

Risk of losing reputation and trust: Data security breaches can cause lasting damage to the trust in institutions and companies [5].

Free riding: Private and public sector organizations are willing to contribute data if they receive benefits in return and if the beneficiaries of their data also share data reciprocally [20, 13].

Compliance, particularly in data protection: In a recent survey in Germany, 56% of companies cite data protection concerns as a reason to oppose data sharing [15].

Trust in infrastructure: Conveying and instilling trustworthiness in users is an open challenge to this date [17]. Regular approaches such as certifications, do not appear to be sufficient either [27].

Lack of alignment, unclear incentives: Especially in voluntary settings, the collaborating parties need to find alignment and incentives for them to provide the necessary and appropriate data [13]. Incentives for truth-telling, i.e., providing accurate data, needs to be considered and addressed use case by use case.

Even when all organizations have aligned interests, there are technical barriers to collaborating on sensitive and high-value datasets.

Technical complexity and lack of standards: Industry reports claim that the complexity of existing IT landscapes, in combination with the lack of standards that support data collaboration, significantly increases IT expenditures for private companies [1, 6, 13, 24].

Lack of trusted third parties: When multiple organizations send their data to a trusted third party for analysis, they expose themselves to potential unauthorized access, breaches, or insider threats. Advanced certification schemes are not sufficient to overcome this trust issue [27, 13].

Lack of trusted third parties and lock-in risks: When multiple organizations send their data to a trusted third party for analysis, they expose themselves to potential unauthorized access, breaches, or insider threats. Advanced certification schemes are not sufficient to overcome this trust issue [27, 13]. Additionally, centralizing sensitive data such as supply chain information on a single platform creates significant lock-in effects, where organizations become overly dependent on one provider's infrastructure, pricing models, and technical standards.

As a result, organizations are forced to choose between protecting their data and obtaining valuable insights. A solution is needed that allows meaningful computation on sensitive data without ever exposing it, ensuring both privacy and usability in collaborative environments.

3 Secure Multi-Party Computation (MPC)

Secure multi-party computation (MPC) enables organizations and individuals to perform computations on sensitive data collaboratively, without ever exposing them to each other. This capability unlocks completely new approaches to reconcile utility and confidentiality tradeoffs, allowing data-driven collaboration while maintaining full control over private information.

3.1 MPC Protocols

At its core, MPC is built on cryptographic protocols that allow multiple parties to jointly compute a function over their private inputs while keeping those inputs hidden from one another. Depending on the nature of the computation and the security guarantees required, various MPC protocols can be applied.

Security models: MPC protocols operate under different security models, such as semi-honest (where parties might try to learn the inputs of another party, but are assumed to follow the protocol) [29, 30, 11, 2] or malicious (where parties are not assumed to follow the protocol and can behave arbitrarily to learn other parties' inputs). Protocols with malicious security can be further categorized into protocols with honest majority (more than half of the parties are honest) [11, 4], dishonest majority (less than half of the parties are honest) or full threshold (up to all but one of the parties can be corrupt) [26, 9, 10]. The protocols in these categories guarantee that the honest parties' inputs are protected even in the presence of malicious behavior. The choice of the model directly affects the complexity and computational cost of the solution.

Computation types: MPC protocols can express any computable function but use different representations depending on how the function is structured:

- **Boolean circuits** [29, 30, 11, 2]: Represent functions using logical gates. While capable of expressing any computation, they are generally more efficient for functions that involve making decisions, comparing values, and following different paths based on conditions.
- **Arithmetic circuits** [4, 10, 14]: Use addition and multiplication operations over a defined mathematical field. Like Boolean circuits, they can represent any function, but they are often more efficient for computations involving numerical operations, such as summation, averaging, or statistical analysis.

The choice between Boolean and arithmetic circuits does not limit what can be computed – both are universal models of computation. Instead, the selection hinges on what the function does: arithmetic circuits naturally align better with tasks with arithmetic computations, while Boolean circuits can streamline logic-based operations.

3.2 MPC for Inter-Organizational Data Collaboration

MPC addresses several challenges of inter-organizational data collaboration.

First, MPC **eliminates the need for a trusted third party** by allowing multiple parties to perform computations on their private inputs without ever exposing them. Unlike traditional cryptographic systems, MPC does not rely on centralized key management or trusted third parties. Instead, data is split into encrypted data ("shares") such that the parties compute directly on those. No single party possesses the full data or decryption keys, which removes single points of failure and reduces the risks associated with centralizing sensitive information.

Second, MPC **ensures transparency, agency, and control** by allowing each party to see which joint task (i.e., the function or algorithm) will be computed and which parties are to receive the result before contributing their data.

Third, **data sovereignty and privacy are inherently maintained** in MPC, since only the final computation output is revealed. The security guarantees of MPC protocols ensure that private data remains protected – depending on the protocol, even if up to all parties except one are compromised and colluding.

Finally, **MPC fundamentally changes the economics of data collaboration**. Traditional data-sharing settings require significant upfront costs, time, and effort, especially if a trusted third party is necessary. The costs of these arrangements occur upfront in such settings, while the potential benefits of data collaboration remain unknown or insufficiently quantifiable. Secure multi-party computation (MPC) allows parties to perform, validate, and quantify potential benefits with lower upfront costs. The governance component remains critical for every MPC calculation, as organizations must establish consensus on data input formats, categorization schemes, and other semantic standards. The ability to perform informed cost-benefit analyses earlier is especially beneficial in low-trust environments or competitive industries where direct data collaboration is infeasible due to confidentiality concerns or regulatory barriers.

In summary, MPC enables secure, cost-effective, and privacy-preserving collaboration by embedding privacy into the computation itself. It eliminates the need for trusted intermediaries, reduces compliance and negotiation costs, and ensures that data remains both useful and protected – addressing the classic tradeoff between utility and confidentiality in data-driven collaboration.

4 SINE's Technology Stack for Secure Data Collaboration

SINE is developing open source software and services to make MPC more usable for inter-organizational data collaboration on sensitive data, especially related to health and environmental impact such as emissions transparency, or impact investing.

In this section, we introduce Polytune, SINE's MPC engine, and Garble, a compiler for translating functionalities described in a high-level language to MPC programs. It is important to note that Polytune and Garble are integrated building blocks but can also be used independently of each other.

4.1 Polytune

Implemented in Rust, Polytune [23] is an open-source MPC Engine that implements a secure multi-party computation protocol that protects the inputs of the computing parties even if all but one of the participants are corrupted and collude. The underlying protocol of Wang et al. [26] guarantees security and confidentiality of the input data even in the case of full threshold corruption among the participants. This means that even if all but one of the parties are dishonest and collude, i.e., alter computations and try to infer confidential data, they cannot learn any information about the honest party's inputs other than what the output of the computation reveals. In this case, an attack is detected and the computation fails, safeguarding the integrity of the process.

Security was Polytune's primary focus during its first stages of development. We therefore deferred performance optimizations to later stages and maintained strict adherence to Wang et al.'s protocol. We currently work on heavily optimizing our protocol implementation to achieve better scalability and performance for real-world use cases.

Wang et al. [26] mention an extension to the original protocol that allows not only one party, but an arbitrary subset of pre-defined participants to retrieve the correct output of the computation. To enable real-world use cases that require flexibility in determining the output parties, we contacted the authors of [26] who specified this extension, which we incorporated into Polytune.

Polytune's architecture balances advanced cryptographic techniques with flexibility, providing a robust foundation for privacy-preserving computation where data confidentiality is critical.

4.2 Garble

To reduce the complexity in writing software for Polytune and MPC in general, SINE provides an open source high-level description language and Boolean circuit compiler. This language, called Garble [22], enables software engineers to write MPC programs in a high-level language inspired by the Rust programming language. These high-level program descriptions are then compiled into Boolean circuits – the fundamental building blocks used by garbled circuit-based MPC protocols (such as the Wang et al.'s protocol [26] implemented in Polytune).

The compiler focuses on optimizing Boolean circuits by minimizing the number of AND gates, a crucial factor for the performance of MPC protocols. One key feature of Garble is its support for private join operations, which allow two or more parties to compute the join or intersection of their datasets without revealing any additional information about their private inputs. This is based on the sort-compare-shuffle protocol by Huang et al. [12]. In many use cases cross-organizational data aggregation is to be performed, i.e., the join is not returned but specific entries in the join are counted or aggregated in a certain way. In these cases, the final shuffle step of the sort-compare-shuffle protocol can be omitted since the joined output is directly used in subsequent computations.

4.3 Example Usage

We do not prescribe any form of communication strategy in Polytune, but provide examples to demonstrate different Polytune integration scenarios `https://polytune.org/examples/channel.html`, including a HTTP channel-based implementation and a second using WASM for Polytune integration into a browser. This version is also deployed at `benchmarking.sine.dev`.

Moreover, we aim at providing an easy-to-configure method for data analysis – a flexible component designed to simplify and streamline the deployment of MPC computations across diverse use cases. It allows stakeholders to define and manage secure computation sessions by specifying:

- **What private computation to perform in Polytune** – defined as a Garble program.
- **Who participates in the computation** – identified by IP addresses and ports.
- **Who can access the result** – agreed upon in advance.
- **Which format the inputs and output are provided** – we give examples to accessing these from a database or provided by an HTTP API.

These can be defined dynamically and adapted when necessary. To lower the barrier to adoption, Polytune's codebase includes example configurations (`https://github.com/sine-fdn/polytune/tree/main/examples`) that demonstrate how different MPC computations can be initiated and managed. This makes integrating secure multi-party computation into real-world workflows both intuitive and efficient.

5 Use Cases

At SINE, we explore use cases where secure data collaboration unlocks valuable insights for data-driven decision-making. Our use case explorations demonstrate that privacy-preserving technologies are not only a compliance measure but also a driver of new opportunities.

5.1 Privacy-Preserving Data Analysis in the Public Sector

As part of the ATLAS project [8], funded by the German Federal Ministry of Research, Technology and Space (former Federal Ministry of Education and Research), SINE's role is to implement open-source technologies for the privacy-preserving analysis of municipal data and implement use cases with the German public sector. Our project partner published an intermediate report on the use case identification process [18], which we use as inspiration for this section. Even though identifying a suitable use case where real-world data was allowed to be used in a pilot turned out to be more complex than expected due to data protection law uncertainties and concerns, we have identified multiple directions where MPC could provide interesting and valuable insights. Among others, a main concern was the unresolved debate if MPC is a pseudonymization or anonymization technique according to the GDPR [3, 21].

Measles vaccination data correctness: Under the German Measles Protection Act, certain groups must provide proof of measles vaccination, otherwise public health offices are notified and follow-up actions are initiated. In this pilot, we aim to correlate measles vaccination data from the school entry examination database with the vaccination database to identify missing reports. It is expected that this will reduce unnecessary follow-up checks by the health department. We are piloting this use case in 2025 with the health department of Frankfurt am Main, Germany.

Preventative care and social status: Though preventative health check-ups are generally covered by health insurance in Germany, attendance is not compulsory. Correlating these preventive health data with other datasets, such as socioeconomic or socio-democratic data, could give insight into what influences participation in preventive care and help tailor public health campaigns to underserved groups.

Early childhood support and school entry exam: The school entry examination dataset in Germany is a key dataset in child health, that provides comprehensive information on early development, medical history, etc. The impact of early childhood preventative measures could also be correlated with these datasets, i.e., to see if missed early childhood preventative examinations have an impact on developmental delays, special education needs, etc.

The value of preventative care in education: Several ideas arose while considering correlating school entry examination data with educational success data. Interesting directions could be: analyzing how pre-existing conditions affect school success, how kindergarten attendance affects educational progress, and what the impact of support programs on educational outcome is.

Disaster protection: Disaster response teams must support individuals with special needs during evacuations, such as when unexploded ordnance is discovered during construction. We identified several cases in which MPC can assist civil protection agencies with capacity planning and mission optimization.

These examples illustrate just a fraction of the potential applications for privacy-preserving data analysis in the public sector. Many other use cases could be envisioned across healthcare, education, social services, and crisis management, helping policymakers make data-driven decisions while respecting privacy regulations.

5.2 Secure and Collaborative Verification of Emissions Data with MPC

For regulatory and climate mitigation purposes, companies require access to carbon footprints at product level [24, 16]. Different industry initiatives [28, 25] promote the use of so-called product carbon footprints (PCFs) for this purpose. PCFs quantify and declare a product's greenhouse gas emissions, typically expressed in carbon dioxide equivalents

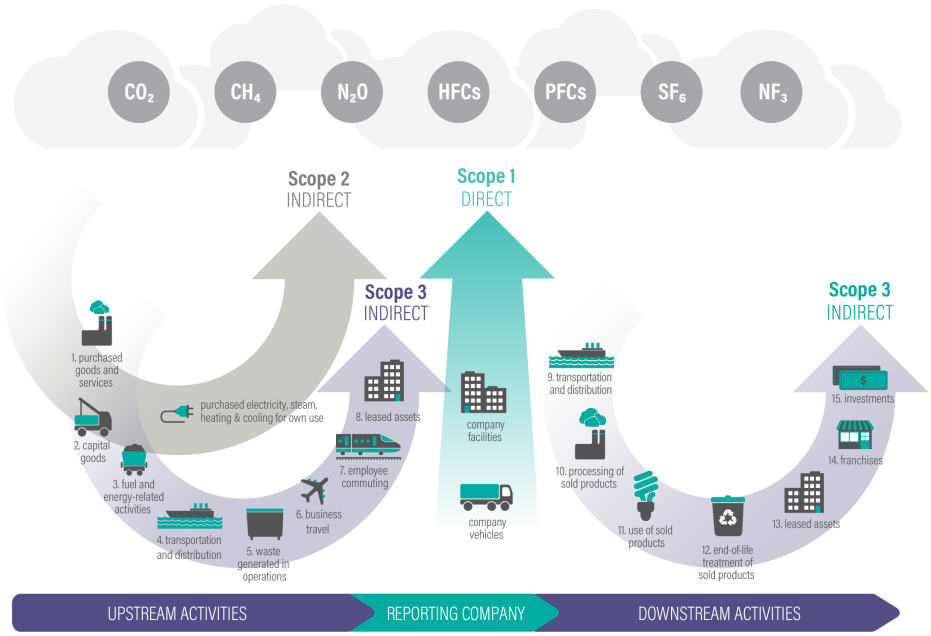

Figure 1: Scopes 1, 2, and 3 as introduced by the Greenhouse Gas Protocol [19]

(CO2e), generated throughout a product's lifecycle of raw material extraction, production, and distribution (see Figure 1).

Specifically, to calculate a PCF, information about the carbon intensities of all pre-products, and their distribution, needs to be known. Such emissions are also called Scope 3 emissions. For many product categories, Scope 3 emissions are 80% or more of a product's total carbon footprint. To improve the accuracy of a PCF, the emissions, especially in Scope 3, should be calculated from actual measurements, also called **primary data** [16].

Crucially, to make PCFs usable and trusted for carbon mitigation management purposes [24, 16], they need to be verifiable. However, companies then often face a critical challenge: while accurate carbon footprint calculations require transparency, including data from multiple stakeholders, sharing primary data is not feasible, since it frequently contains trade secrets – such as supply chain details, production processes, and energy consumption patterns – that businesses cannot disclose, even for collaborative environmental efforts [24].

MPC can address the privacy and transparency dilemma by enabling collaborative calculations over encrypted data, especially emissions and primary data as its input data. The following are some of the use cases that could be possible with MPC.

Detecting statistical outliers in PCF values: Customers collaborate to compare the PCF values received by their suppliers – while keeping each supplier's PCF private. This helps identify anomalies and ensure realistic carbon footprint reporting.

Benchmarking product PCFs: Producers can securely compare their PCF values to industry benchmarks, allowing e.g., classification into leading, typical, or lagging categories. This enables fair comparisons without exposing proprietary data.

Validating inputs to PCF calculations: MPC can also be used to benchmark key inputs – such as energy use, waste, and logistics – against expected ranges to detect irregularities.

Benchmarking and comparing product CO_2 intensities: Some companies attempt to

lower reported PCFs by reallocating emissions. MPC can help compare CO_2 emissions relative to retail cost, ensuring that reported figures are realistic.

Aligning PCF data with verified corporate emissions: This use case cross-checks a company's PCF data with its verified emissions reports (e.g., CSRD reports). By comparing PCFs with revenue and reported emissions using MPC, stakeholders can detect gaps and ensure consistency in a privacy-preserving manner.

Verifying Primary Data Share (PDS): A customer seeks assurance that a producer's reported primary data (e.g., material use, emissions, or energy consumption) is accurate, while the producer wants to prove its validity without revealing sensitive details. Using MPC, the producer and customer – along with other producers in the value chain – collaborate to securely compute the PCF. This allows verification without exposing proprietary data, ensuring trust and transparency in sustainability reporting.

PCF Calculation from Scope 1 and Scope 2 emissions only: Since Scope 3 emissions (indirect emissions from the supply chain) make up the majority of a company's footprint, complete verification is difficult. If a full manufacturing graph were available, PCF calculations could be verified using only Scope 1 and 2 emissions, reducing complexity.

Using open-source PCF calculation methods: In this process, the PCF is verified through collaboration between producers and customers. The customer checks the PCF by running an open-source calculation and comparing the results against statistical outliers. The customer or verification system can also validate the inputs to ensure they are within expected ranges.

MPC provides an approach to verifying sustainability claims without compromising sensitive business information. By enabling secure, collaborative calculations, MPC allows stakeholders to benchmark emissions, detect inconsistencies, and validate carbon footprint data with greater confidence. As regulatory requirements for emissions transparency continue to grow, leveraging MPC for verification can help companies meet compliance standards while maintaining competitive confidentiality. Ultimately, this approach fosters a more trustworthy and data-driven sustainability landscape, where businesses can work together to reduce their environmental impact without exposing proprietary data.

6 Future Directions

Privacy-enhancing technologies such as secure multi-party computation (MPC) offer a promising solution for many carbon accounting challenges, enabling organizations to collaborate on environmental data while maintaining confidentiality. As sustainability reporting demands increase and supply chain emissions become harder to ignore, MPC provides a path to shared insights driven by primary data, without compromising competitive advantages. It is important to note that MPC primarily addresses technical and privacy barriers rather than fundamental incentive misalignments. Effective implementation requires robust governance frameworks that establish clear participation incentives, data quality standards, and equitable value distribution among participants[1].

The technology's potential in sustainability contexts remains largely unexplored. We invite researchers, sustainability professionals, and industry leaders to investigate applications for cross-organizational data collaboration on sensitive primary data. Early experimentation and cross-sector dialogue will be crucial for realizing the transformative potential of privacy-enhancing technologies such as MPC in climate action.

[1] `https://sine.foundation/datacommons`

Authors

Main authors: Ágnes Kiss, Martin Pompéry
Contributing authors: Jonathan Heiß, Raimundo Henriques, Robin Hundt, Frederic Kettelhoit, Aurel Stenzel
Contact: polytune@sine.foundation

Acknowledgments

During this work, we received support from the German Federal Ministry of Research, Technology and Space (BMFTR) (formerly Federal Ministry of Education and Research (BMBF)) through funding of the ATLAS project under reference number 16KISA037.

References

[1] Pranay Ahlawat, Justin Borgman, Samuel Eden, Steven Huels, Jess Iandiorio, Amit Kumar, and Philip Zakahi. A new architecture to manage data costs and complexity. https://www.bcg.com/publications/2023/new-data-architectures-can-help-manage-data-costs-and-complexity, 2023. Accessed: 2025-07-22.

[2] Donald Beaver, Silvio Micali, and Phillip Rogaway. The round complexity of secure protocols (extended abstract). In STOC, pages 503–513. ACM, 1990.

[3] Sebastian Becker, Christoph Bösch, Benjamin Hettwer, Thomas Hoeren, Merlin Rombach, Sven Trieflinger, and Hossein Yalame. Multi-party computation in corporate data processing: Legal and technical insights. IACR Cryptology ePrint Archive, page 463, 2025.

[4] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In STOC, pages 1–10. ACM, 1988.

[5] Bertin Martens and Alexandre De Streel and Inge Graef and Thomas Tombal and Nestor Duch Brown. Business-to-business data sharing: An economic and legal analysis. https://publications.jrc.ec.europa.eu/repository/handle/JRC121336, 2020. Accessed: 2025-07-24.

[6] Cleardata. Is interoperability the future of healthcare? https://www.cleardata.com/blog/interoperability-in-healthcare/, 2025.

[7] European Commission. Commission staff working document impact assessment report. https://ec.europa.eu/newsroom/dae/redirection/document/83524, 2022. Accessed: 2025-07-02.

[8] Atlas Project Consortium. Atlas project website. https://www.polyteia.com/resources/atlas-project. Accessed: 2025-07-02.

[9] Ivan Damgård and Claudio Orlandi. Multiparty computation for dishonest majority: From passive to active security at low cost. In CRYPTO, volume 6223 of Lecture Notes in Computer Science, pages 558–576. Springer, 2010.

[10] Ivan Damgård, Valerio Pastro, Nigel P. Smart, and Sarah Zakarias. Multiparty computation from somewhat homomorphic encryption. In CRYPTO, volume 7417 of Lecture Notes in Computer Science, pages 643–662. Springer, 2012.

[11] Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game, or a completeness theorem for protocols with honest majority. In Providing Sound Foundations for Cryptography, pages 307–328. ACM, 2019.

[12] Yan Huang, David Evans, and Jonathan Katz. Private set intersection: Are garbled circuits better than custom protocols? In NDSS. The Internet Society, 2012.

[13] Ilka Jussen, Frederik Möller, Julia Schweihoff, Anna Gieß, Giulia Giussani, and Boris Otto. Issues in inter-organizational data sharing: Findings from practice and research challenges. Data & Knowledge Engineering, 150:102280, 2024.

[14] Marcel Keller, Emmanuela Orsini, and Peter Scholl. MASCOT: faster malicious arithmetic secure computation with oblivious transfer. In CCS, pages 830–842. ACM, 2016.

[15] Bitkom Servicegesellschaft mbH. Datenökonomie - ergebnisse einer unternehmensbefragung. https://www.bitkom.org/sites/main/files/2023-05/Bitkom-ChartsDatenoekonomie.pdf, 2023. Accessed: 2025-07-02.

[16] OECD. The carbon footprint of everything. In OECD Net Zero+ Policy Papers, No. 6. OECD Publishing, Paris, 2025.

[17] Antti Poikola, Ville Takanen, P J Laszkowicz, and Teemu Toivonen. The technology landscape of data spaces. https://media.sitra.fi/app/uploads/2023/10/sitra-technology-landscape-of-data-spaces.pdf, 2023.

[18] Polyteia. Erkenntnisse aus der Anwendungsfallrecherche im Forschungsprojekt ATLAS – Datentreuhänder für anonymisierte Analysen in kommunalen Datenräumen . https://25504841.fs1.hubspotusercontent-eu1.net/hubfs/25504841/Forschung/Zwischenbericht%20ATLAS%20Projekt.pdf. Accessed: 2025-07-22.

[19] Greenhouse Gas Protocol. https://ghgprotocol.org/sites/default/files/inline-images/Diagram%20of%20Scopes%20and%20Emissions%20Across%20the%20Value%20Chain_updated.png, 2024. Accessed: 2025-07-24.

[20] OECD Publishing. Enhancing access to and sharing of data: Reconciling risks and benefits for data re-use across societies. https://www.oecd.org/en/publications/enhancing-access-to-and-sharing-of-data_276aaca8-en.html, 2019.

[21] RWMPC. Panel discussion – MPC and GDPR. Video recording. https://vimeo.com/1078973800/49d7f95cbd, 2025. Accessed: 2025-07-22.

[22] SINE Foundation. Garble. https://github.com/sine-fdn/garble-lang. Accessed: 2025-07-22.

[23] SINE Foundation. Polytune. https://github.com/sine-fdn/polytune. Accessed: 2025-07-22.

[24] Aurel Stenzel and Israel Waichman. Supply-chain data sharing for scope 3 emissions. npj Climate Action, 2(1):7, 2023.

[25] Together for Sustainability AISBL. TfS Initiative. https://www.tfs-initiative.com/. Accessed: 2025-07-02.

[26] Xiao Wang, Samuel Ranellucci, and Jonathan Katz. Global-scale secure multiparty computation. In CCS, pages 39–56. ACM, 2017.

[27] Danny Wong. Eight lessons from building data spaces. https://www.sitra.fi/en/articles/eight-lessons-from-building-data-spaces/, 2024.

[28] World Business Council for Sustainable Development. PACT Project. https://www.carbon-transparency.org/. Accessed: 2025-07-02.

[29] Andrew Chi-Chih Yao. Protocols for secure computations (extended abstract). In FOCS, pages 160–164. IEEE Computer Society, 1982.

[30] Andrew Chi-Chih Yao. How to generate and exchange secrets (extended abstract). In FOCS, pages 162–167. IEEE Computer Society, 1986.