Replacing Organizational Trust with Technical Guarantees

Long-term relationships can no longer sufficiently guarantee trust in digitized networks. While traditional mechanisms such as contracts remain important, they are increasingly reaching their limits in dynamic platform ecosystems. With the exchange of sensitive data, however, technical trust anchors are gaining importance in order to secure trust in a scalable, transparent, and digital manner.

Keywords
data ecosystems, data spaces, privacy-enhancing technologies, data sharing, trust, organizational security, data sovereignty, Internet of Production

Hajeong Jeon, MS is a PhD student at the Chair of Communication and Distributed Systems (COMSYS) at RWTH Aachen University. As part of her research, she applies trusted execution environments (TEEs) and confidential computing to introduce verifiable guarantees into data ecosystems.

Johannes Lohmöller, MS is a PhD student at the Chair of Communication and Distributed Systems (COMSYS) at RWTH Aachen University. His research centers around applying privacy-preserving methods and understanding their implications, especially in the context of medical use cases.

Prof. Klaus Wehrle holds the Chair of Communication and Distributed Systems (COMSYS) at RWTH Aachen University. His interests include (but are not limited to) engineering of networking protocols, (formal) methods for protocol engineering and network analysis, reliable communication software, and all operating system issues of networking.

Dr. Jan Pennekamp is a Postdoc at the Chair of Communication and Distributed Systems (COMSYS) at RWTH Aachen University. His research covers security and privacy aspects in the Industrial Internet of Things (IIoT), particularly privacy-enhancing technologies, the design of privacy-preserving protocols, and secure computations as well as their application.

Contact
jeon@comsys.rwth-aachen.de
comsys.rwth-aachen.de

DOI: 10.30844/I4SE.26.4.8

The ORCID identification numbers of the authors of this article can be viewed at https://doi.org/10.30844/I4SE.26.4.8

AdobeStock/Lomb

Replacing Organizational Trust with Technical Guarantees

Privacy-enhancing technologies for dynamic industrial value networks

Hajeong Jeon, Johannes Lohmöller, Klaus Wehrle and Jan Pennekamp, RWTH Aachen University

Industrial value networks are undergoing a fundamental transformation from stable, long-term supply chains to short-lived, data-driven collaborations across organizational boundaries. Traditional trust mechanisms—contracts, non-disclosure agreements, audits, and reputation—remain indispensable yet insufficient as the sole foundation for trust in such environments. We thus identify privacy-enhancing technologies (PETs) as a technical basis for providing verifiable guarantees to all stakeholders. We examine how industrial value networks can leverage PETs to enable secure, reliable collaborations amid sensitive data sharing. Organizational trust remains necessary despite a shift toward non-technical enforcement mechanisms such as governance, liability, and ethical guidelines. By combining technical guarantees with these organizational measures, we aim to empower organizations to maintain control over sensitive information in digitized, dynamic platform ecosystems.

Digitalized industrial ecosystems are fundamentally changing how companies collaborate, from shallow collaboration to coopetition [1], developing into value-creation networks [2]. Rather than relying on inflexible supply chains and networks with a limited number of long-term partners, organizations increasingly form short-lived collaborations while simultaneously sharing data across organizational boundaries **(Fig. 1)** [3]. The Internet of Production [4] envisions a setting where process data, product models, and production data are utilized globally, across organizations and even across domains, i.e., involving suppliers, customers, and service providers.

The most valuable insights in such environments often emerge only when data from multiple organizations is combined. Accordingly, they facilitate advancements in quality prediction, sustainable lifecycle optimization, and workload optimization and maintenance.

However, maintaining data confidentiality in this context is challenging. Ensuring data security and privacy becomes particularly critical as collaboration and competition among organizations intensify [3]. The data in question is often highly sensitive, ranging from personal and privacy-relevant information to confidential intellectual property (IP) and trade secrets. In the absence of a prior long-term relationship or in cases of only minor contractual agreements, related questions are crucial to enable data sharing in the first place.

Today, organizational trust mechanisms dominate the landscape: complex contracts, non-disclosure agreements (NDAs), bilateral agreements, and audits, which are all costly and time-consuming, are usually the only sources of trust, alongside informal reputation [5]. These instruments are well-established, but they are slow and expensive and thus do not scale to ecosystems in which organizations establish relationships more dynamically, potentially even only for hours or days rather than months or years.

A key question, therefore, is how to adapt, evolve, or replace existing trust mechanisms to fit the needs of increasingly dynamic value networks. As shown in **Figure 2**, organizational mechanisms alone cannot provide sufficient data security and verifiability. We thus suggest a shift toward new approaches. Specifically, we call for introducing accountability by establishing explicit, enforceable, and verifiable technical guarantees.

Building on this vision, we propose relying on privacy-enhancing technologies (PETs) [6] that verifiably provide confidentiality, integrity, and usage-control guarantees to dynamic value-creation networks. Organizational measures remain important in a different role: they govern what cannot be enforced technically and provide the framework within which technical guarantees operate.

In this article, we provide a conceptual synthesis of research on industrial data ecosystems, organizational trust, and PETs to analyze how trust in dynamic industrial value networks can be transformed into technical guarantees. In doing so, we point out which aspects of trust, especially confidentiality, integrity, usage control, and accountability, can be technically supported, and which remain dependent on organizational governance. Based on these insights, decision-makers can gradually adapt their organizations' strategies and workflows.

Trust in dynamic industrial value networks

Industrial value creation is changing to incorporate flexible business relations across supply chains (horizontal collaboration), complementing the established focus on linear supply chains (vertical collaboration) [3]. Organizations dynamically establish, join, and leave

DOI: 10.30844/I4SE.26.4.8

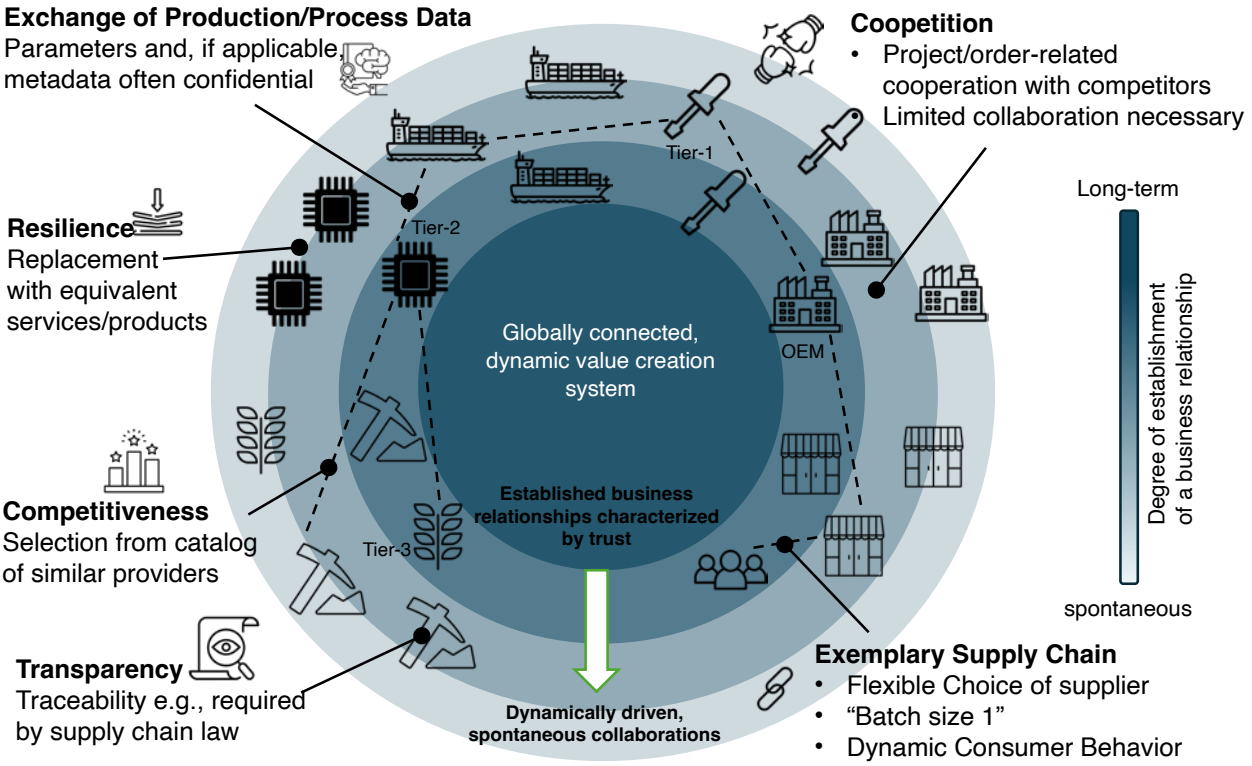

Figure 1: *Conceptual overview of a dynamic industrial value network. Supplier relationships are increasingly being replaced by short-lived, dynamic collaborations, reducing the role of long-term trust in value networks.*

collaborations to share and reuse data on demand through various channels and data ecosystems. The latter introduces a new type of intermediary, i.e., a (cloud) service provider. Large-scale initiatives like Manufacturing-X and GAIA-X embody this trend toward federated data infrastructures [7] that prioritize interoperability, sovereignty, and FAIR data principles [8] while emphasizing data sovereignty [9], security, and privacy.

In such settings, trust is multidimensional. Here, we consider organizational trust as a concept that enables organizations to collaborate and share data via technical mechanisms while reducing the risk and uncertainty of other parties [10]. In fact, trust involves multiple actors (organizations and service providers), implemented security and privacy mechanisms, and data governance properties. Stakeholders must not only be confident that their data remains confidential and is not disclosed to unauthorized parties. They also need assurance that data and computational results maintain their integrity and cannot be modified by adversaries.

Furthermore, data should be used only for agreed purposes, within approved contexts and timeframes. Any misuse or policy violation should thus be detected and attributed appropriately. In other words, confidentiality, integrity, proper use (often captured by the concept of data use control [11]), and accountability together constitute the practical meaning of "trust" in industrial value networks. In turn, established trust drives collaboration and data sharing, thereby greatly affecting innovation, productivity, and, potentially, societal progress [12].

Traditional mechanisms [13, 14] for implementing organizational security address these concerns only inadequately. Contracts can specify what is allowed and what is prohibited, while audits can occasionally verify compliance, and certifications can attest that certain processes are in place. However, these measures tend to be coarse-grained, reactive, and without any actionable technical guarantees. They may deter or punish misconduct (if detected) but provide little support in preventing it in the first place, particularly in environments with many (mutually distrusting) organizations. Even worse, in industrial value creation networks, organizations may have an incentive to misbehave for monetary gain, as long as they are not caught (as captured in the malicious-but-cautious attacker model) [5].

As the number of participants grows and their relationships become more dynamic and opaque, the attack surface expands further. Conducting thorough due diligence for

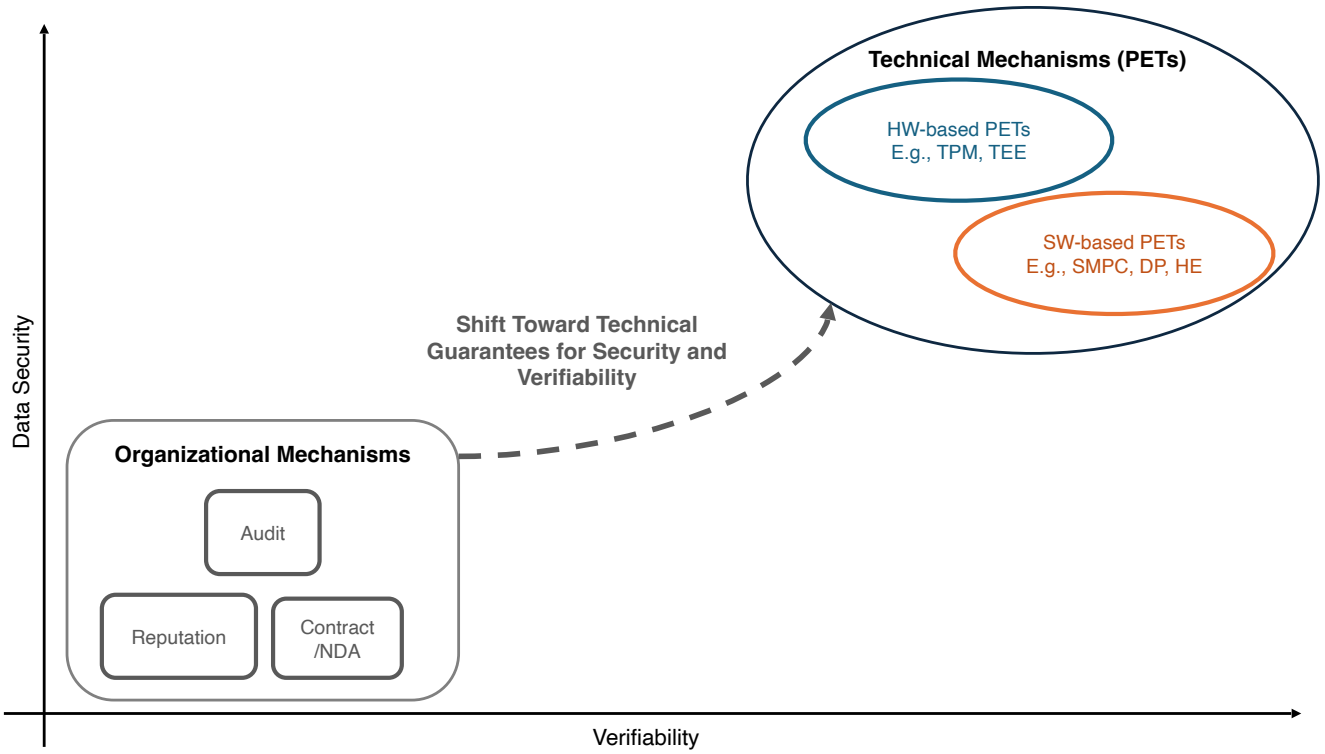

Figure 2: *High-level contrast of organizational trust with technical guarantees (PETs), including hardware- and software-based approaches. For enhanced data security and verifiability, trust establishment should shift from organizational to technical mechanisms.*

every new collaboration partner has become impractical. At the same time, relying solely on mutual trust or reputation is no longer realistic when sensitive IP or personal data is at stake. In such dynamic, large-scale ecosystems, significant parts of what used to be handled implicitly through organizational trust must therefore be replaced by technical means: rather than assuming that organizations "will behave," participants need reliable, verifiable assurances built into how collaborations are established, maintained, and monitored.

Privacy-enhancing technologies to establish reliable "trust" guarantees

Privacy-enhancing technologies (PETs) offer building blocks for establishing such technical guarantees. At a high level, PETs enable computation, data processing, and data sharing without exposing raw data beyond agreed boundaries. Additionally, depending on the building block, they can even provide verifiable evidence that computations were carried out as promised.

Several families of PETs are particularly relevant for industrial platforms [4, 5, 15]. Trusted Execution Environments (TEEs) provide hardware-backed isolation, with code and data residing in specifically protected parts of the operating system. In terms of software-based concepts, Secure Multi-Party Computation (SMPC) enables multiple parties to jointly compute a function over their inputs, ensuring that no party learns anything beyond the final output. Similarly, Homomorphic Encryption (HE) enables operations directly on encrypted data, such as computations to be offloaded to distrusted infrastructure (including data ecosystems).

Taking a different approach, Differential Privacy (DP) adds noise to data in a way that prevents the presence or absence of individual records from being reliably inferred. Lastly, Zero-Knowledge Proofs (ZKPs) can demonstrate that a statement is true—for example, that a computation was carried out according to a policy—without revealing underlying data.

Figure 3 summarizes how each technology addresses the aforementioned trust components (i.e., confidentiality, integrity, proper usage, accountability). For a more detailed overview, we refer to prior work on the feasibility of these building blocks for adoption in industrial value creation networks [5, 16, 17].

Jointly, these technologies support a shift from organizational security ("trust us") to technical guarantees

("here is the evidence"). Instead of relying on the service provider or collaboration partner not to look at the data, TEEs and HE can significantly prevent unauthorized data access. Other building blocks, such as SMPC or ZKPs, can cover other aspects of the data lifecycle, effectively providing reliable guarantees across each state.

Particularly in areas where organizational security and implicit trust were common, PETs are unlikely to replace all prior practices. However, introducing PETs to value creation networks promises to provide guarantees to collaborative settings that are otherwise not realistically achievable.

Implications for future industrial data ecosystems

Despite extensive academic discussion [6, 15], practical adoption of PETs in industry remains inconsistent [16]. For example, based on 34 empirical studies on PET perceptions, Lohmöller et al. [16] derive that PET adoption is constrained not only by technical issues but also by organizational integration challenges, such as a lack of training and education (41%) and workflow changes (32%). This gap indicates that the challenge concerns selecting suitable PETs, as well as embedding their functionalities into the architecture and operational workflows of industrial data ecosystems.

If PETs are to be integrated into the landscape, the design of platforms and ecosystems must change. Systems must shift from trust by assumption (organizational security [18]) to designs that achieve trust by design (using technical guarantees) [5]. Then, security and privacy mechanisms are directly integrated into the core of a dynamically collaborating landscape, while also offering mechanisms for verification and accountability—aspects that are paramount in dynamic settings [15].

Concretely, this shift requires rigorous threat modeling. Platform designers must make explicit who is to be trusted and in which respects. How trusted is the service provider? Which malicious actions would organizations take? Are insider threats a concern?

Again, the choice of PETs depends on the goals and the threat model considered, since they address different adversaries. TEEs protect against a compromised system; SMPC helps with mutually distrusting partners; DP protects against inference; and transparency logs ensure observability [19]. Hence, an important step is to derive an accurate threat model, so that PETs can be selected and configured accordingly. Otherwise, the shift from organizational security will not succeed in practice, as unaddressed security and privacy threats will continue to hinder real-world use.

Equally important for deployment are performance requirements (including how they scale to dynamic settings with many participating organizations) and operational challenges. PETs, especially SMPC and HE, can incur significant overhead compared to plaintext computation. TEEs face other limitations related, for example, to memory storage sizes [20]. Industrial data ecosystems must therefore differentiate between applications where the strongest PET guarantees are necessary—for example, IP-sensitive model training across competitors—and those where more lightweight mechanisms suffice. They must

Figure 3: *Mapping of trust components in industrial value networks to organizational and technical (PET) solutions. The table demonstrates how the core aspects of trust are addressed, with organizational approaches providing governance and PETs delivering verifiable technical guarantees.*

Trust Component	Definition	Organizational Mechanism	Technical Mechanism (PETs)
Confidentiality	Undisclosed data to unauthorized parties	Contract, NDA	Trusted Execution Environments, Homomorphic Encryption, Secure Multi-Party Computation
Integrity	Data/computation results cannot be modified undetectably	Audit	Zero-Knowledge Proofs, Trusted Execution Environments
Proper Usage	Used only for agreed purposes/contexts/timeframes	Contract, Policy	Zero-Knowledge Proofs, Usage Control
Accountability	Detectable and attributable misuse/policy violations	Contract, Policy	Zero-Knowledge Proofs

also define acceptable latency and throughput constraints and consider how PETs can be optimized or combined to meet them in practice.

Trust by design is not a one-off decision but requires constant reassessment throughout the ecosystem's operation. Specifically, it encompasses the secure onboarding of new collaboration partners, including the distribution and management of keys and trust anchors. Continuous verification is also involved to ensure that computations are executed in the expected environments. Audit mechanisms are required to reconstruct who performed which actions, when they occurred, and under what guarantees.

Recent work [16] highlights adoption recommendations and sheds light on perceptions and practical uses of PETs. In the beginning, incremental integration of PETs, starting with high-value, high-risk applications, is a worthwhile adoption path. Broader use can follow once organizations are convinced that technical guarantees can replace or at least complement organizational security. Consequently, industrial value creation networks should pursue a step-by-step adoption, rather than a single disruptive overhaul.

The technical aspects of trust

To properly set the stage, we must emphasize that PETs, despite their promise, are not perfect. They can significantly reduce the need for trust by assumption, but they cannot eliminate all trust concerns since data governance strategies also play a crucial role.

Implementation flaws, overlooked threats, and user errors can undermine the achievable guarantees and reduce confidence in them. Such flaws and misconfigurations in each mechanism can even lead to PET-specific security threats, such as side-channel attacks (TEEs), inference (SMPC), decryption failures (HE), residual disclosure risks (DP), and false verification (ZKPs) [15, 20–22], undermining trust in technologies originally perceived as secure. Technical guarantees, i.e., the strive for trust by design, are only as strong as the weakest component and configuration in the entire ecosystem.

Moreover, PETs primarily address the technical aspects of trust. In other words, they specify the authorized entity for data access, permitted computations, and the extent to which additional information can be inferred. However, PETs are irrelevant to governance, responsibility, liability, and ethical constraints. Such challenges still depend on organizational strategies, legal frameworks, and human judgment. Data usage control and data sovereignty may address these additional angles to a certain extent but cannot entirely substitute for them.

Looking beyond initial data sharing, trust still inherently remains organizational. No PET can guarantee the partners' responsibility for sourcing or using data or for reasonable management decisions for all stakeholders. Similarly, PETs cannot fully resolve disputes arising from incomplete evidence or divergent policy interpretations. Even in a PET-driven ecosystem, organizations will still need governance processes and dispute-resolution mechanisms to address discoveries of malicious behavior.

The right goal, therefore, is not to eliminate organizational trust entirely but to complement and adapt it to modern needs **(Fig. 3)**. PETs allow value creation networks to replace a large portion of the implicit, unverifiable trust that currently governs them with reliable, verifiable technical guarantees. What remains of organizational trust is smaller in scope but more clearly defined and better supported by evidence and thus more manageable in dynamic environments. Instead of trusting that the ecosystem will not misbehave, organizations can trust that, given the outlined threat model and PET configuration, the ecosystem is highly constrained in enabling any respective misuse. Thus, organizational trust can rather focus on strategic, ethical, and governance dimensions.

The next generation of industrial ecosystems

Dynamic industrial value creation networks hold considerable promise for efficiency, innovation, and resilience. Realizing this promise, however, requires that sensitive data can be shared across organizational boundaries without causing unacceptable risks. Traditional organizational trust mechanisms, while essential, are increasingly insufficient when collaborations are short-lived and involve many organizations and highly sensitive data.

PETs offer a promising approach to addressing this challenge. For many aspects of industrial collaboration, organizational security can be replaced by technical guarantees. We argue that PETs should serve as a foundation for modern ecosystems, providing reliable, verifiable trust among collaborators. While technical guarantees are responsible for the operational aspects of data sovereignty, security, and privacy, organizational trust should shift to high-level governance and strategic alignment.

Looking ahead, AI and large language models (LLMs) could also become a crucial enabler in realizing this shift at scale. Although PETs are powerful, they are inherently complex [16]. Configuring such technologies properly requires an advanced understanding of cryptography, threat models, and regulations. Here, LLM-based assistants could help non-experts specify their purposes and intentions,

translating such intentions into machine-enforceable policies and PET configurations. Moreover, the LLM-based assistants could also guide the selection of the most feasible mechanisms based on threat models and performance requirements.

Designing the next generation of industrial ecosystems with both PETs and AI-assisted configuration in mind is, therefore, a major and timely challenge. Only by deliberately replacing implicit organizational trust with explicit technical guarantees can dynamic industrial value creation networks become truly collaborative and rigorously secure.

This work was funded by the German Federal Ministry of Research, Technology and Space (BMFTR) under funding reference number 02J24A030. The responsibility for the content of this publication lies with the authors. Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC-2023 Internet of Sustainable Production – 390621612.

Bibliography

[1] Meena, A.; Dhir, S.; Sushil, S.: A review of coopetition and future research agenda. In: Journal of Business & Industrial Marketing 1 (2023) 38, pp. 118–136. DOI: https://doi.org/10.1108/JBIM-09-2021-0414.

[2] Schneider, M.; Mittag, T.; Lee, T.; Gausemeier, J.: Value Creation Design: Modeling of Value Networks. In: Journal of Strategic Innovation and Sustainability 1 (2017) 12, pp. 111–125.

[3] Pennekamp, J. et al.: An Interdisciplinary Survey on Information Flows in Supply Chains. In: ACM Computing Surveys 2 (2024) 56, pp. 1–38. DOI: https://doi.org/10.1145/3606693.

[4] Pennekamp, J. et al.: Dataflow Challenges in an Internet of Production: A Security & Privacy Perspective. Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy - CPS-SPC'19 (2019), pp. 27–38. DOI: https://doi.org/10.1145/3338499.3357357.

[5] Lohmöller, J. et al.: The unresolved need for dependable guarantees on security, sovereignty, and trust in data ecosystems. In: Data & Knowledge Engineering (2024) 151, pp. 102301. DOI: https://doi.org/10.1016/j.datak.2024.102301.

[6] Heurix, J.; Zimmermann, P.; Neubauer, T.; Fenz, S.: A taxonomy for privacy enhancing technologies. In: Computers & Security (2015) 53, pp. 1–17. DOI: https://doi.org/10.1016/j.cose.2015.05.002.

[7] Braud, A.; Fromentoux, G.; Radier, B.; Le Grand, O.: The Road to European Digital Sovereignty with Gaia-X and IDSA. In: IEEE Network 2 (2021) 35, pp. 4–5. DOI: https://doi.org/10.1109/MNET.2021.9387709.

[8] Wilkinson, M. D. et al: The FAIR Guiding Principles for scientific data management and stewardship. In: Scientific Data 1 (2016) 3, p. 160018. DOI: https://doi.org/10.1038/sdata.2016.18.

[9] Hummel, P.; Braun, M.; Tretter, M.; Dabrock, P.: Data sovereignty: A review. In: Big Data & Society 1 (2021) 8, p. 205395172098201. DOI: https://doi.org/10.1177/2053951720982012.

[10] Latusek, D.; Vlaar, P. W. L.: Uncertainty in interorganizational collaboration and the dynamics of trust: A qualitative study. In: European Management Journal 1 (2018) 36, pp. 12–27. DOI: https://doi.org/10.1016/j.emj.2017.10.003.

[11] Jung, C.; Dörr, J.: Data Usage Control. In: Designing Data Spaces, pp. 129–146. DOI: https://doi.org/10.1007/978-3-030-93975-5_8.

[12] Fimmers, C.; Pennekamp, J.: Sichere industrielle Zusammenarbeit - Ein Paradigmenwechsel. In: Factory Innovation. URL: https://factory-innovation.de/artikel/paradigmenwechsel-datenaustausch/, accessed 13.02.2026.

[13] De Leon, V.; Williamson, J.: Contractual Strategies to Protect Business Secrets. In: Business Secrets Management, pp. 165–178. DOI: https://doi.org/10.1007/978-3-031-82512-5_6.

[14] Ollivier, P. et al.: Protecting Business Secrets to Improve Value Creation. In: Business Secrets Management, pp. 93–164. DOI: https://doi.org/10.1007/978-3-031-82512-5_5.

[15] Pennekamp, J.: Secure collaborations for the industrial Internet of Things. DOI: https://doi.org/10.18154/RWTH-2024-03585.

[16] Lohmöller, J. et al.: Between Promise and Practice: Challenges and Misperceptions of Applying Privacy Enhancing Technologies in Business Contexts. Proceedings of the 59th Hawaii International Conference on System Sciences (2026), DOI: https://doi.org/10.24251/HICSS.2026.744

[17] Lohmöller, J. et al.: Complementing organizational security in data ecosystems with technical guarantees. Proceedings of the 1st conference on building a secure and empowered cyberspace (BuildSEC '24) (2024), pp. 49–56. DOI: https://doi.org/10.1109/BuildSEC64048.2024.00016

[18] Cram, W. A.; Proudfoot, J. G.; D'Arcy, J.: Organizational information security policies: a review and research framework. In: European Journal of Information Systems 6 (2017) 26, pp. 605–641. DOI: https://doi.org/10.1057/s41303-017-0059-9.

[19] Lohmöller, J.; Vlad, E.; Dahlmanns, M.; Wehrle, K.: Poster: Bridging Trust Gaps: Data Usage Transparency in Federated Data Ecosystems. Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (2023), pp. 3582–3584. DOI: https://doi.org/10.1145/3576915.3624371.

[20] Schneider, M. et al.: SoK: Hardware-supported Trusted Execution Environments. DOI: https://doi.org/10.48550/ARXIV.2205.12742

[21] Sun, X. et al.: A Survey on Zero-Knowledge Proof in Blockchain. In: IEEE Network 4 (2021) 35, pp. 198–205. DOI: https://doi.org/10.1109/MNET.011.2000473.

[22] Dwork, C.; Kohli, N.; Mulligan, D.: Differential Privacy in Practice: Expose your Epsilons! In: Journal of Privacy and Confidentiality 2 (2019) 9. DOI: https://doi.org/10.29012/jpc.689.