6-22-2020

User-Centric Network-Model for Data Control with Interoperable Legal Data Sharing Artefacts

Harrie Bastiaansen
TNO, harrie.bastiaansen@tno.nl

Simon Dalmolen
TNO, simon.dalmolen@tno.nl

Maarten Kollenstart
TNO, maarten.kollenstart@tno.nl

T.M. van Engers
TNO, tom.vanengers@tno.nl

User-Centric Network-Model for Data Control with Interoperable Legal Data Sharing Artefacts

Improved Data Sovereignty, Trust and Security for Enhanced Adoption in Interorganizational and Supply Chain IS Applications

Completed Research

Dr. H.J.M. Bastiaansen
Netherlands Organisation for applied scientific research TNO
Eemsgolaan 3
9727 DW Groningen
The Netherlands
harrie.bastiaansen@tno.nl

S. Dalmolen, MSc
University of Twente
Drienerlolaan 5
7522 NB Enschede
The Netherlands
simon.dalmolen@tno.nl

M. Kollenstart, MSc
Netherlands Organisation for applied scientific research TNO
Eemsgolaan 3
9727 DW Groningen
The Netherlands
maarten.kollenstart@tno.nl

Prof. Dr. T.M. van Engers
Netherlands Organisation for applied scientific research TNO
Anna van Buerenplein 1
2595 DA The Hague
The Netherlands
tom.vanengers@tno.nl

Abstract

Organizations increasingly collaborate in digital ecosystems, whilst being aware that data is becoming a key asset. They require improved data control capabilities that prevent their shared data from being misused. Currently, such capabilities are typically realized as situation-specific closed ecosystem solutions in a 'hub-model' approach. This, however, hinders adoption of inter-organizational data sharing as end-users are faced with potential customer lock-in and major integration efforts to manage data sovereignty, trust and security over multiple data sharing relationships. As alternative, an open 'network-model' approach provides end-users a single entry-point for simultaneously controlling data sharing over multiple relationships with clear operational advantages in user-friendliness, complexity, efficiency and costs. However, it poses strong interoperability requirements on the legal concepts of data sharing agreements and usage contracts (terms-of-use). This paper contributes to the development of the network-model by identifying and assessing architectural options for realizing interoperability on the legal concepts for controlled data sharing.

Keywords: Data Sharing; Control; Sovereignty; Trust; Security; Hub-Model; Network-Model; User-Centric; Legal; Data Sharing Agreement; Usage Contract; Terms-of-Use; Access Policies; Usage Policies; Interoperability; Semantics; Governance.

Introduction

Changing market dynamics, brought about by increasing digital connectivity, force organizations to take strategic actions. A shift from optimizing internal business processes into a more collaborative optimization across business ecosystems is becoming more common (Loebbecke et al. 2015). This leads to organizations shifting from a strategy of competitiveness to a more collaborative strategy: organizations are collaborating to serve customers through mutually dependent and co-operative supply chains, both within business ecosystems and across industry sectors.

Nevertheless, despite their advantages, agile and flexible digital supply chain collaborations also pose real challenges, both from an organizational and a technical/IT perspective (Luftman et al. 2017), as organizations are becoming ever more aware that data is one of their most valuable assets and should be managed and controlled as such (Grover et al. 2018). Data control capabilities for data sovereignty, trust and security are necessary to prevent the misuse of shared data and are, as such, the sine qua non conditions for organizations to be prepared to share potentially competitive and sensitive information (Mannhardt et al, 2019). Enabling data control is a evermore considered as key prerequisite for data owners to adopt data sharing for interorganizational and supply chain IS applications.

Data sovereignty is a natural person's or organization's capability of being entirely self-determined with regard to its data (Otto et al. 2019), i.e. it allows a legal entity to exclusively decide about the usage of its data as an economic asset. It requires organizations to be in control of the conditions under which their data is shared and how it may be processed by other parties. Trust is the ability to rely that the entities (persons, organizations or systems) with which data is shared are who they claim to be and that they will act accordingly. Trust relies on adequate identification, authentication and certification capabilities. Security is the capability to provide assurance that actual sharing of data is protected against unauthorized mis-use of data through (malicious or accidental) security breaches. It includes aspects such as encrypted data transport and storage and software certification and attestation.

These data control capabilities are mainly provided by IT vendors for closed sector-specific ecosystems, each with its own specific solutions. However, this 'hub-model' approach (Liezenberg et al. 2019), or hub-and-spoke model, poses major challenges for end-users and organizations that share data in multiple ecosystems: they are faced with both a threat of vendor lock-in by their IT providers, and with major integration efforts to define, manage and enforce data sovereignty, trust and security solutions across multiple data sharing relationships (Zrenner et al. 2019).

An alternative to the closed ecosystem-specific hub-model approach is the open 'network-model' approach, providing a single entry point to the end-user with common and agreed upon protocols for defining and enforcing data control capabilities across multiple data sharing relationships (Liezenberg et al. 2019; Dalmolen et al. 2019; IDSA 2019). As such, a network-model approach with generic and re-usable infrastructural capabilities for defining and enforcing data sovereignty, trust and security in multi-lateral data sharing may offer significant advantages from the end-user perspective. As such, it may be referred to as being more 'user-centric'. Because of this, the network-model approach is currently attracting industry attention in overcoming the challenges associated with the hub-model for multilateral data sharing. Various initiatives are currently emerging, of which the International Data Spaces (IDS) initiative has major international attention.

As will be described in this paper, a network-model approach will be implemented in a federated manner, i.e. with multiple instances of (interacting) functions provided by independent organizations. Therefore, the user-centric network-model approach for controlled data sharing poses various interoperability challenges. Especially, it is highly interrelated to the topic of interoperability for the legal concepts of data sharing agreements and usage contracts (also referred to a 'terms-of-use'). As such, this paper addresses the following research question: "How can an open model approach for data sharing with interoperability of data sharing agreements and usage contracts be developed for wide scale multi-organization adoption?". This research encompasses an assessment of the network-model approach on the interoperability of legal data sharing aspect, i.e., data sharing agreements and usage contracts. This extends beyond the capabilities of existing data sharing architectures based on the network-model approach where data control mostly applies to security by means of encrypted data transactions, sometimes augmented with end-user identification and authentication (Jarke et al. 2019).

Interoperability in a federated data sharing environment: legal, organizational, semantic and technical

Data sharing in a federated data sharing environment can be characterised as a system-of-systems, in which a multitude of dedicated systems pool their resources and capabilities together to create a new, overarching, system with value adding functionality and performance. In scientific research, various frameworks have been developed from the perspective of realizing interoperability for such system-of-systems architectures. An approach that is well accepted is the new European Interoperability Framework as developed by the European Commission (EC 2017). It distinguishes four interoperability levels that must be implemented, as depicted Figure 1: legal, organizational, semantic and technical interoperability under an overarching integrated governance approach.

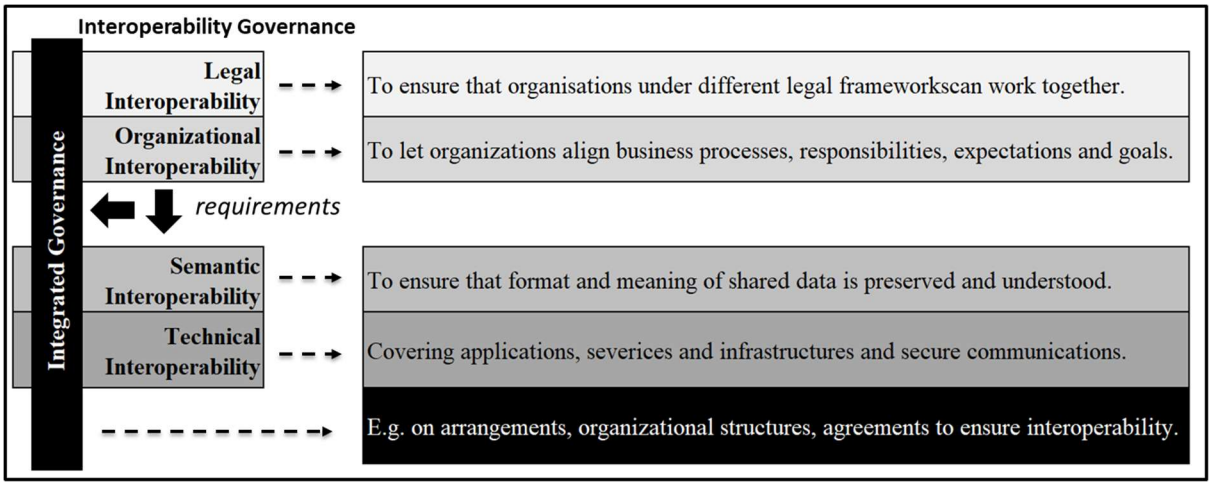


Figure 1. Interoperability Model as Defined in the New European Interoperability Framework.

The various levels of interoperability are further elaborated in the remainder of this paper from the perspective of providing a user-centric approach in a federated network-model approach with infrastructural data sovereignty, trust and security. As the figure indicates, the legal and organizational aspects (as addressed in the following subsections) set the requirements on both technical interoperability and semantic interoperability thereof. This provides a new contribution to the development of a federated data sharing environment. Therefore, it is elaborated more in depth in the subsequent sections.

Legal interoperability: frameworks for data sharing agreements and usage contracts

Over the complete data sharing life-cycle, a broad set of support processes for managing data sharing agreements and data transactions is required, from publishing data sources up to the logging of data transactions. As they determine their perception of the overarching data sharing processes, they form the basis for the user-centric data sharing architecture approach as described in this paper.

In (Dalmolen et al. 2019), the main data sharing support processes have been categorized according to the subsequent life-cycle stages in data sharing, together with the metadata artefacts they generate, which contains potentially sensitive information from the data provider perspective. It described how data sovereignty, trust and security of this metadata can be maintained in an open network-model approach. This paper extends and builds upon this work by addressing the important aspects of a user-centric architectural perspective on the legal concepts of data sharing agreements and usage contracts, aimed at preventing misuse of the shared data. As described in the introduction, the network-model approach with a single entry point will improve end-user friendliness in simultaneously managing data control capabilities across multiple data sharing relationships. Such a user-centric single entry point however, requires interoperability on these legal concepts over the multitude of data consumers with which data is shared in the highly federated network-model approach.

Hence, seamless interoperability on the legal concepts of data sharing agreements and the usage contracts becomes highly intertwined with user-centricity. Both are catch-all terms encompassing various specific elements, as listed and described in Table 1.

Data sharing agreement: Specifying the conditions under which specific data will be shared, consisting of the contractual conditions and the usage contract.	
	Commercial conditions: Stating the commercial conditions under which the data will provided, including the costs of the data and the invoicing and payment conditions.
	Legal conditions: Stating the legal aspects required (to avoid) conflict resolution, e.g. the IPR-conditions, the applicable law, …
	Service level: Stating the quality parameters of the data provided, including completeness, accuracy and timeliness.
Usage contract: Combining the access control policies and usage control policies, expressing the data provider's internal (business) data sharing policies and the external (regulatory) policies.	
	Access control policy: Stating which individuals, roles or systems are allowed access to the data provided.
	Usage control policy: Stating how the data may be used or distributed after access has been given to individuals, roles or systems.
	Security profile policy: Stating the requirements on the security profile of the data consumer.

Table 1. Elaboration and Description of the Legal Artefacts of the Data Sharing Agreement and the Usage Contract Metadata Artefacts.

Frameworks on (schemes for) data sharing agreements and usage contracts are currently emerging in various sectors. An overview on such frameworks with comparison on supported features is for instance provided in (MIN EACP 2018). As a prominent example, the Dutch iSHARE initiative is currently being adopted in the Netherlands (NLIP 2019). It realizes a uniform set of agreements for identification, authentication and authorization, such that organizations can share logistics data in a simple and controlled way, including with (previously unknown) partners.

Organizational interoperability: federated and multilateral interoperability in a network-model approach

As described in Figure 1, organizational interoperability refers to the way in which organizations align their business processes to achieve common goals on improved collaboration. As such, organizational interoperability can be considered from two perspectives, as depicted in Figure 2. Both perspectives are addressed in the following paragraphs, subsequently.

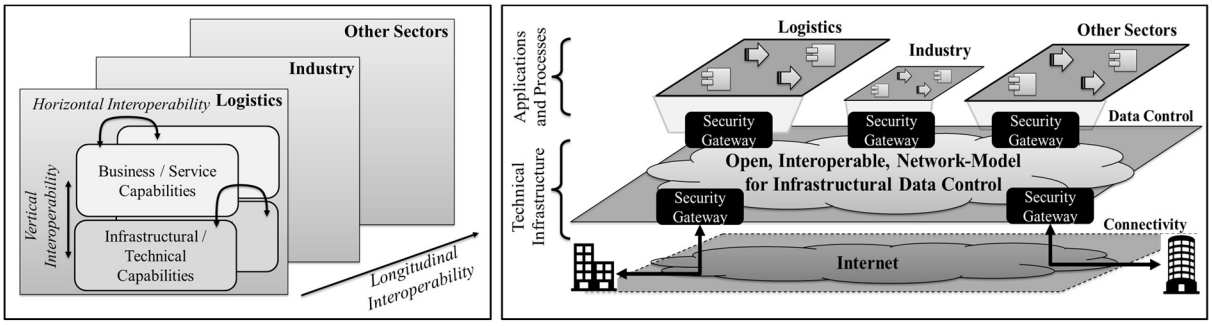


Figure 2. Organizational Interoperability Perspectives: The Multilateral Data Sharing Perspective (l) and the Network-Model Perspective for Infrastructural Data Control (r).

Multilateral interoperability: vertical, horizontal and longitudinal

As shown in the left side of Figure 2, three types of organizational interoperability in multilateral data sharing may be distinguished, referred to as vertical, horizontal and longitudinal interoperability.

Vertical interoperability applies to the interoperability of the applications and processes with the technical infrastructure within the same organization, i.e. 'intra-organizational interoperability'. Vertical interoperability can be achieved through exposing 'generic' capabilities of technical infrastructure to be used by multiple applications and processes simultaneously by means of well-defined Application Programming Interfaces (APIs). As such, the APIs must support both the legal concepts on data sharing agreements and usage contracts and the data control functions on data sovereignty, trust and security.

Horizontal interoperability applies to the interoperability between different organizations, i.e. 'inter-organizational interoperability'. For supporting the data control capabilities to manage and enforce data sovereignty, trust and security over data provider and consumer, this implies that the data provider and consumer are within the same trust domain at the technical level. Additionally, interoperability of applications and processes enabling real-time engagement in business partnerships may be achieved through agreed upon process (semantic interoperable) choreographies (Hofman et al. 2016). Again, this must be supported by organizational interoperability on the legal concepts and the data control functions.

Longitudinal interoperability applies to the interoperability between organizations that do not have a direct / bilateral data sharing relationship, i.e. 'supply chain interoperability'. Data is proliferated along the supply chain, possibly in processed format, towards data consumers that don't have a direct bilateral (legal) data sharing agreement with the original data provider. Hence, proliferation of agreements in combination with trust of the data provider in the supply chain partners becomes crucial, as the control over sharing data to organizations along the supply chain can no longer be technically enforced directly by the data provider. Using state-of-the-art data provenance concepts may give the data provider some basic insight in how his data is handled and proliferated in the supply chain, providing him a basic level of trust for sharing his sensitive data.

In summary: Vertical interoperability allows multiple applications and processes to use the multilateral data sharing infrastructure simultaneously. Through horizontal interoperability, more organizations can (seamlessly) share data over it. Longitudinal interoperability enables data to be shared with organizations further along the supply chain. For each of these, organizational interoperability on the legal concepts of data sharing agreements and usage contracts is required.

Network-model interoperability: peer-to-peer data sharing with federated intermediary roles

The transition from a solution specific hub-model approach towards an open network-model approach for controlled data sharing with a single entry point is illustrated in Figure 3 (Liezenberg et al. 2019). Its aim is to improve end-user centricity in simultaneously managing multiple data sharing relationships.

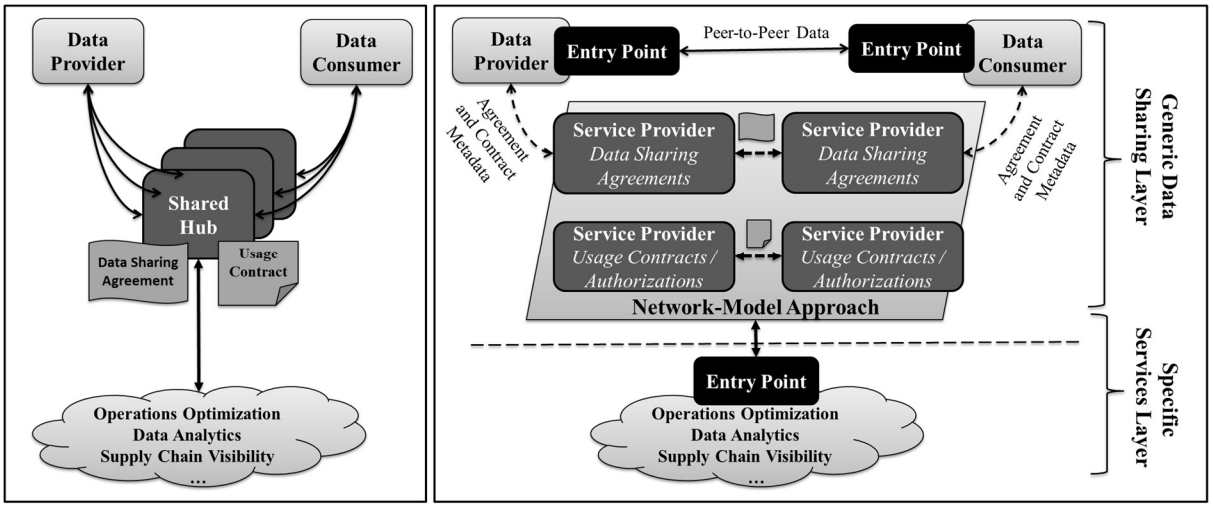


Figure 3. Transition from a Hub-Model (l) to a Network-Model (r) Approach for Data Sharing.

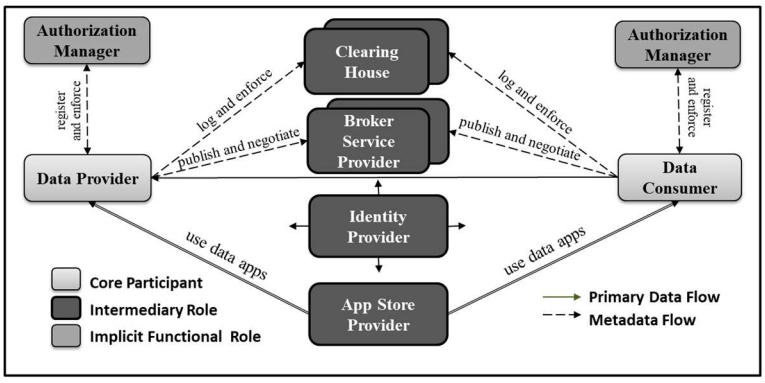
The right part of Figure 3 shows the leading architectural principles of the network-model approach:

- peer-to-peer data sharing, and
- federation of the supporting legal concept on data sharing agreements and usage contracts.

In the network-model approach, data sharing is done on a peer-to-peer basis. Nevertheless, this peer-to-peer data sharing may be used to populate a centralized data lake to support value adding services. This is depicted in the lower part of Figure 3, showing a multitude of specific value adding services that can be supported, e.g. for operations optimization, data analytics and supply chain visibility. This may seem contradictory and make the generic data sharing layer superfluous. It is noted however, that also in these cases there is added value in the generic data control capabilities of the network-model approach: (1) in the aligned and standardized mechanisms of communicating from data provider to service provider the data sharing agreements and usage contracts under which the data is shared, (2) in the enforcement thereof in the domain of the service provider, and (3) in the added value of providing supporting functions for data sharing by external trusted roles as independent party.

The right part of Figure 3 shows the federated architecture for the network-model approach. Multiple instances of the intermediary roles will coexist and are fulfilled by separate service providers. The data provider and the data consumer will in general be subscribed to different service providers, which may be considered as their 'home' intermediary roles. As the figure shows, this federated implementation also applies for providing the supporting services on the legal concepts of data sharing agreements and usage contracts. In (Dalmolen et al. 2019), it is described how this federation of intermediary roles may be realized using a service-oriented architecture, whilst the data provider maintains sovereignty over the associated metadata on the data transactions that is generated in these processes.

The International Data Spaces (IDS) initiative may be considered as an initial case study for the network-model approach. It is currently gaining major international traction for multi-lateral data sharing. The IDS reference architecture (Otto et al 2019) describes a network-model approach with infrastructural data control capabilities for data sovereignty, trust and security. It builds upon the interoperability principles as described in the previous subsections: peer-to-peer and federated data sharing. Moreover, the IDS reference architecture can be considered an architectural elaboration of the Trusted Multi-Tenant Infrastructure (Trusted Computing Group, 2013). Figure 4 depicts the IDS enabling ecosystem with (trusted) intermediary roles as distinguished in the IDS reference architecture, together with a high-level description of the functions they provide.



Role and Functions
Broker Service Provider
- Registration and publication of data sources and profiles
- Definition, negotiation and signing of data sharing agreements
Clearing House
- Logging of data sharing agreements
- Clearing and settlement of data transactions
- Auditing, reporting and conflict resolution
Authorization Manager
- Definition and registration of usage contracts
- Enforcement of usage contracts
Identity Provider
- Manage identities of participants
- Validate identities of participants
App Store Provider
- Publication and provisioning of data apps

Figure 4. Roles in the IDS Reference Architecture (l)), together with a Functional Description for the Intermediary Roles (r) (Otto et al. 2019).

The 'Intermediary Roles' in the IDS reference architecture as depicted in the figure act as trusted entities and are assumed to be provided by trusted third parties (TTPs). The IDS intermediary role of identity provider supports the trust function, together with an additional IDS-role for providing certification and remote attestation functions (not depicted in the figure). The intermediary roles broker service provider fulfils the functions for managing data sources and data agreements to the point that a formal data sharing agreement has been agreed upon between data provider and consumer. The clearing house fulfils the functions for managing data sharing after a mutual data sharing agreement has been made, i.e. managing actual data sharing transactions in accordance with the data sharing agreements and

logging and reporting thereof. A separate IDS intermediary role for registering authorizations as part of the usage contracts is not identified in the IDS reference architecture. These are implicitly incorporated in the role of the data provider and consumer as shown in the left side of Figure 4.

In (Dalmolen et al. 2019) it is described how the IDS run-time environment (based on standardized security gateways, referred to as 'IDS connectors') can realize a service-oriented architecture supporting the IDS intermediary roles. This is also applicable for the service provider for the legal concepts of data sharing agreements and usage contracts, as will be shown in the following section. An initial operational implementation is currently provided by the Smart Connected Supplier Network, SCSN, (BIC 2020), a fieldlab initiative to enable improved supply chain cooperation behind large high-tech companies in the Eindhoven, The Netherlands, area.

Technical interoperability: Interaction topologies for data sharing agreements and usage contracts

In a federated network-model approach for multilateral data sharing as depicted in the right side of Figure 3, seamless interoperability on the legal concepts of data sharing agreements and usage contracts is key for enabling wide scale adoption. An overarching interoperability approach is required that on the one hand is user-centric by minimizing implementation complexity and integration efforts, whilst on the other hand serving the needs for the various (intermediary) roles in the network-model. Adequate interaction topologies form the technical basis for the overarching technical interoperability. The subsequent subsections describe their typology and evaluate the options. In addition, the International Data Spaces (IDS) initiative is described that enables the suggested options.

Interaction topologies in a federated architecture

Various technical interaction topologies to support (interoperability of) the exchange of legal concepts on data sharing agreements and usage contracts within a federated network-model for multilateral data sharing can be distinguished. These are referred to as 'Role Interaction Topologies' (RITs) and are illustrated in Figure 5.

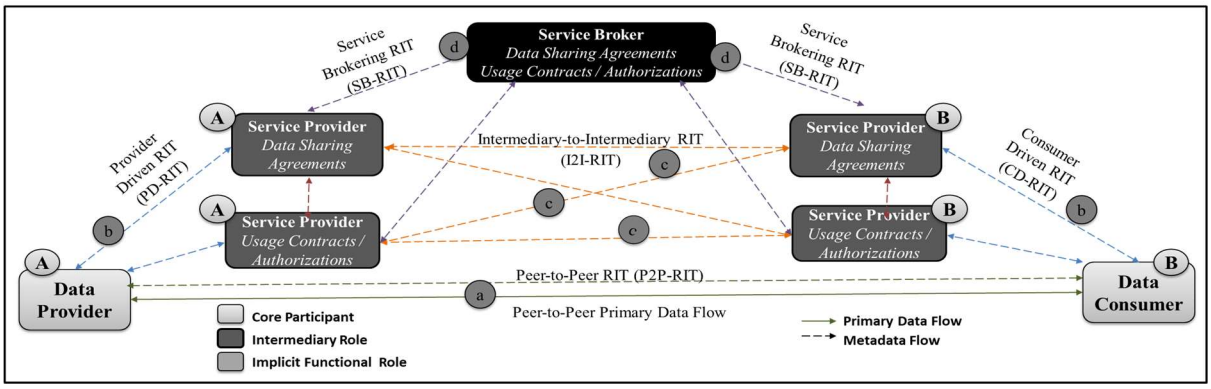


Figure 5. Four types of 'Role Interaction Topology' (RITs) for Legal Concepts in a Federated Network-Model Approach for Multilateral Data Sharing.

The four types of RITs which are applicable in an open network-model as depicted in the figure, are:

(a): *Peer-to-Peer RIT (P2P-RIT),* in which the data provider and the data consumer share metadata directly without involvement of intermediary roles. Not only can this apply to the primary data flow, also the metadata on legal concepts may be shared on a peer-to-peer basis between the data provider and the data consumer.

(b): *Provider and Consumer Driven RIT (PD-RIT / CD-RIT),* in which the data provider orchestrates the sharing of metadata with the intermediary roles it has subscribed to. For these RITs, it is the data provider's consumer's responsibility to subscribe to (trusted) intermediary roles that provide adequate service options for the legal processes on data sharing agreements and usage contracts that match the data provider's and consumer's business policies. For instance, for the data provider

this applies to templates for (negotiation of) data sharing agreements and logging of data transactions. For the data consumer, this may apply to data provenance, i.e. the (trustworthy) logging and accounting of the handling, processing and proliferation of shared data along the supply chain for conflict resolution and financial settlement

(c): *Intermediary-to-Intermediary RIT (I2I-RIT),* in which the intermediary roles of the various data providers and consumers that support the data sharing and agreements and usage contracts orchestrate the sharing of metadata amongst themselves. Some functions on data sharing and agreements and usage contracts may not only require interactions between the data provider or consumer and their subscribed intermediary roles. Rather, they may require direct interaction between intermediary roles. For instance, this may apply to metadata related to negatiation of data sharing agreement elements and pricing.

(d): *Service Broker RIT (SB-RIT),* in which the interactions between the intermediary roles of the various data providers and consumers are not handled on a bilateral basis but by means of an intermediary broker orchestrating the sharing of metadata associated to data sharing agreements and usage contracts.

For maintaining sovereignty over metadata in an open network-model, the four types of RITs for sharing legal concepts on data sharing agreements and usage contracts (as listed in Table 1) are not equally suitable and applicable. They can be evaluated on the following criteria:

- *Maintaining sovereignty over the legal concepts by the data provider and consumer.*

  Maintaining sovereignty over metadata and being in control over the proliferation chain thereof is essential for data providers and consumers. This applies to legal metadata concepts on data sharing agreements and usage contracts as well. Proliferation along a chain of interconnected intermediary roles by means of I2I-RITs implies loss of such control and having to trust and rely on intermediary roles that are potentially not even known to the data provider or consumer. Restricting proliferation of the metadata to their 'home' intermediary roles that a data provider or data consumer has subscribed to, will prevent such loss of control and will therefore increase the level of data sovereignty.

- *Complexity of the overarching interoperability architecture.*

  The widescale adoption of agreed-upon (and preferably standardized) role interaction protocols strongly depends on the implementation complexity and number of standardized interfaces to be realized between intermediary roles in in the highly federated infrastructure of the open network-model approach. This applies to the interfaces between intermediary roles as denoted as (c) (I2I-RIT) and (d) (SB-RIT) in Figure 5. It is to be noted that using the Service Broker RIT will on the one hand reduce the number of direct Intermediary-to-Intermediary RITs, but on the other hand leads to an additional layer of interfaces to be standardized, i.e. between multiple SB-RIT instances.

  Having to implement and adhere to standardized interaction protocols for a multitude of types and instances of intermediary-to-intermediary RITs may become (too) complex, both from the development and deployment perspective. This complexity may be technically overcome as has been demonstrated in the 'old-school' world of pre-divestiture telecommunications at the end of the previous millennium. In their regulated environment, a limited number of (mostly non-competitive) major telco's had a common interest in closely collaborating in developing standards for interoperability to achieve globally interoperable services. In the current liberalized situation for data services however, such a centrally governed development and deployment process is non-existent. Hence, definition and adoption of agreed-upon intermediary-to-intermediary interoperability protocols is a far less viable option.

On these criteria, the observation is that the PD-RIT and CD-RIT are to be preferred as the default-to-be-used metadata interaction topologies over the I2I-RITs. Figure 6 illustrates how the resulting interaction topologies in a federated, open, network-model approach are to be realized by means of the PD-RIT and CD-RIT, whilst avoiding the necessity for realizing an I2I-RIT and SB-RIT interaction topology.

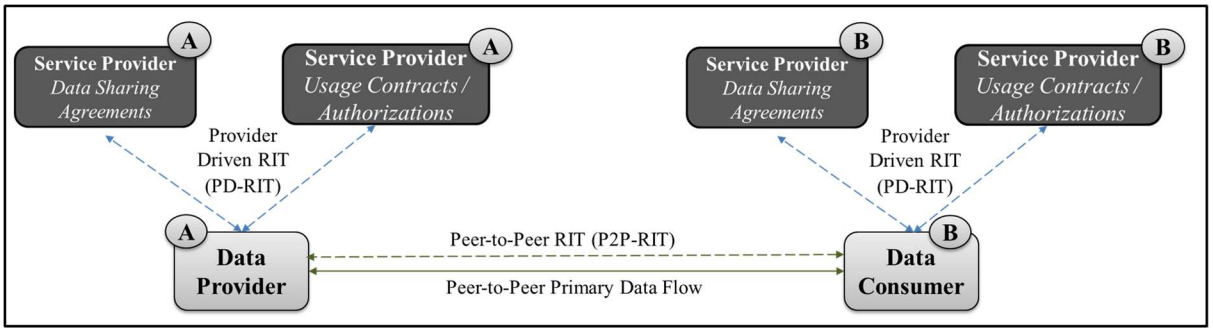


Figure 6. The Preferred 'Role Interaction Topologies' PD-RIT and CD-RIT for Legal Concepts in a Federated Network-Model Approach for Multilateral Data Sharing.

The figure illustrates that with the preferred provider PD-RIT and consumer driven CD-RIT, all sharing of metadata is through orchestration and under control of the data provider and the data consumer. This gives them the required control and sovereignty over the metadata concepts on data sharing agreements and usage contracts. No direct intermediary-to-intermediary metadata sharing beyond the direct control of the data provider and data consumer is required, preventing them from having to rely on external trusted third parties or requiring complex I2I-RIT and SB-RIT interface implementations.

Semantic interoperability: machine-readable and machine-executable data-sharing agreements

As described in the previous section, PD-RIT and CD-RIT are the preferred interaction topologies for organizational interoperability of legal concepts in a federated, network-model approach. These interaction topologies are based on bilateral collaborations requiring agreement on and enforcement of the terms and conditions between data provider and data consumer with intervening intermediary roles. Therefore, a strong and formalized semantic fundament is essential to make sure that various organizations operating in different sectors and jurisdictions unambiguously understand each other.

A machine-readable interpretation of the data sharing agreement and the usage contract is required, as this enables automatic reasoning to be executed on the complex system of rules and obligations.

Making a semantic model of the data sharing agreements is difficult, as these contain norms that are typically written in natural language. Data sharing agreements are embedded in jurisdiction specific as well as general regulatory frameworks, such as the General Data Protection Regulation (GDPR) and many others depending on the application domain. The complex set of norms that are stated in various sources of norms, including those of the data sharing agreements, make it difficult to create a consistent and comprehensible normative model, certainly if the collaborating parties operate in different jurisdictions.

Researchers have developed various standards for structuring and modelling sources of norms. In order to improve accessibility of legal documents, different meta-standards have been developed, that are intended to improve searchability of these documents through annotations, such as Formex (EU 2019a), European Legislation Identifier (EU 2019b), the European Case Law Identifier (ECLI), Metalex (CEN 2019) and its derived standards such as Akomo Ntoso (Akoma Ntoso 2019). These meta-data standards and the refencing mechanisms they incorporate allow users to establish links between and across legal documents. The EU sponsored Open Laws project has established a European wide consortium that promotes interoperability between sources of norms (Open Laws 2019). Structuring and meta-dating sources of norms was an enormous improvement allowing for better accessibility. Furthermore the machine-readable form enabled the various services that require the presentation in appropriate formats in all kind of use-contexts, e.g. explaining the argument of a decision in terms of the legal sources applied to the case. Machine-readable however doesn't make these source texts machine executable.

Machine executable norms are essential for more advanced services such as compliance checking, e.g. checking certain data sharing agreements from different parties in different jurisdictions are compatible to each other, or compliant to national and international law, etc.. Also case assessment (e.g. deciding

if a certain data request can/should be fulfilled given a certain data sharing agreement), requires machine executable norm representation and normative reasoning capabilities.

Researchers in the domain of normative systems study norm representation and normative reasoning and develop formal languages and automated reasoners that are intended to support tasks such as compliance checking, case assessment, legal planning and many other tasks. Their studies typically focus on generic approaches that allow for normative reasoning in a very broad application context. Consequently, they have developed formal representations for argumentation, essential in conflict resolution (e.g. Prakken 2010, Bench-Capon and Dunne 2007), basing their work on the fundamental legal concepts as introduced by Hohfeld (Hohfeld 2019; Doesburg et al. 2019).

The formal representation languages that are currently mostly used are certainly less expressive and build upon practical considerations rather than sound theoretical ones. One could argue that for managing usage contracts (expressing the access, usage and security profiles as listed in Table 1) one could do with such limited languages, accepting the consequences thereof, including the disability to express and resolve conflicts, the disability to accept that norms have meaning within a certain social context where the actors may not comply with the norms, etc..

The Open Digital Right Language (ODRL) and the eXtensible Access Control Markup Language (XACML) are two of the most used standards for expressing such usage contracts. These two languages are similar to each other, except that XACML also defines the messages that are used to enforce policies. ODRL consists out of four main constructs: permissions, prohibitions, duties, and actions. A policy contains rules that permit or prohibit certain actions on resources. Duties indicate actions that should be taken. In the ODRL standard, all of the constructs and the relations between them have been defined and described in a formal, machine-interpretable, manner. Table 2 provides the mapping of the legal artefacts in Table 1 on ODRL constructs.

Data Sharing Agreement	Usage Contract
Commercial conditions Duties can describe the commercial conditions, e.g. the costs of the data, that have to be fulfilled.	*Access control policy* Access control rules are permissions or prohibitions that can be enforced at the data provider.
Service level The service level can be formalized by creating rules where the data provider has specific duties regarding its service level.	*Usage control policy* Usage control rules are predominantly duties, either generic duties or duties linked to permissions.
Legal conditions Only certain aspects can already be formally described, e.g.: • IPR conditions in terms of Creative Commons licenses, e.g. commercial use and distribution rights, exclusivity. • Jurisdiction and the license document in the form of the Dublin Core Metadata Initiative model.	*Security profile policy* Security profiles would logically be modelled in duties, however, at this moment there are no constructs for stating security profiles in either ODRL or XACML. This means that extensions on ODRL or XACML are needed to incorporate security profile aspects in the policy languages.

Table 2. Mapping of the Legal Artefacts in Table 1 on ODRL Constructs.

It must be mentioned here that the notions permissions, prohibitions and duties are the typical notions widely used in deontic logic, and extremely problematic as pointed out in (Doesburg et al. 2019). But even if one would limit oneself to these notions a reduction would be possible as prohibitions and duties are correlated (the Duty to X is equal to the Prohibition to NOT X). The pre-Hohfeldian interpretation that the Permission to do A is equal to NOT the Duty to do A, lacks the potentiality aspect connected to permissions, which is exactly the reason for Hohfeld to introduce the concept Power, as well as preferential notions often connected to permissions (Boer 2009). Within the context of this paper we skip a more in-depth discussion of the essential deontic concepts required, and for now accept the limitations of the deontic constituents of ODRL.

Integrated governance: development and deployment

The required basic technology for realizing the user-centric network-model approach for infrastructural data control as presented in this paper is rapidly maturing, as exemplified by IDS-initiative case. Hence, the successful introduction is clearly within reach from the technical perspective. Nevertheless, for its

actual widescale operational realization, adequate governance of its development and deployment is a prerequisite, which currently mainly seems to be lacking. The following subsections elaborate how adequate governance of development and deployment can stimulate widescale adoption, respectively.

Development: design for scale, scope and reach

The federated and interoperable network-model approach to infrastructural data control for multi-lateral data sharing as addressed in this paper, can be considered as a system-of-systems, in which multiple and independent participants govern their own services and components. Enabling interoperability and scalability requires the governance of development for a minimal rule set for the infrastructural data control capabilities. As such, the main premises for the governance of development, include:

- *Design for scale, scope and reach*

  The scope and reach of the infrastructure for multi-lateral data sharing can be optimized by enabling the various perspectives of multilateral interoperability: vertical ('intra-organizational') interoperability to allow multiple applications and processes to use the multi-lateral data sharing infrastructure, horizontal ('inter-organizational') interoperability to enable 'global' reach as more organizations can (seamlessly) share data over it, and longitudinal ('supply chain) interoperability enabling data to be shared with organizations further along the supply chain.

- *Openness for low barriers to participate*

  To lower the barriers to participate, the network-model approach should be 'open'. It has to be noted that for the various stakeholders in the federated infrastructure 'openness' has its specific meaning (National Research Council 1994): open to end-users, open to solution providers and open to service providers and to innovation. It does not force end-users into closed groups or deny access to any sectors of society but permits universal connectivity. This is also referred to as creating a 'level playing field'. It allows any solution provider to meet the requirements to provide enabling components in the federated infrastructure under competitive conditions. It provides an open and accessible environment for service providers to join and for new applications and services to be introduced. This applies to both the cost levels for participation and to the ease-of-access to the (basic) resources for joining (onboarding), e.g. through by providing the (basic) resources as open source.

- *Standardization of interactions and interfaces*

  Standardization provides the means for openness to enable low barriers to participate. From a user-centric perspective, the focus of standardization must be on accessibility of the functionality provided by the intermediary organizations providing services on the legal concepts of data sharing agreements and usage contracts. This includes both the protocols to support the preferred interaction topologies (as described in the section on technical interoperability) and the semantics of the legal data artefacts (as listed in Table 1 and elaborated in the previous section).

  For widescale acceptance, standardization should follow an open standard design and maintenance process. A plethora of varying definitions is available for characterizing an 'open standard'. The concept of 'open standard' is here meant in the sense of fulfilling the requirements as defined by the European Union within its new European Interoperability Framework for Pan-European eGovernment Services (EC 2017): The standard is developed, adopted and will be maintained by a not-for-profit organization on the basis of an open decision-making procedure. The standard has been published and the standard specification document is available either freely or at a nominal charge. The intellectual property, i.e. possible patents of (parts of) the standard, is made irrevocably available on a royalty-free basis. There are no constraints on the re-use of the standard. The road to be followed may resemble the approach to the governance for the development of the Internet-related standards. Existing models for governance of open standards (Folmer 2012) could be extended to cover all governance aspects for such system-of-systems.

Deployment: towards wide-scale adoption

This paper set out to assess the recent development of the network-model approach. The network-model approach involves a federated ecosystem of data providers, data consumers and intermediary organizations providing services on the legal concepts of data sharing agreements and usage contracts, supporting legal, organizational, semantic and integrated governance interoperability. The required set of technology developments is technically maturing and becoming. Nevertheless, its operational realization has not (yet) been fulfilled. For the widescale adoption of this network-model approach to be achieved, two important deployment governance challenges have to be solved.

First, adequate alternatives for closed ecosystems need to be provided for. This means that network-model data sharing technologies are required that follow the principles of design for scale, scope and reach and that adhere to standardization of both interactions and interfaces. For the IDS initiative we conclude that these requirements are fulfilled, with the data sharing architecture and the 'IDS connector' currently being standardized under the terminology of 'Security Gateway' (DIN 2019). Nevertheless, current data sharing ecosystems making use of the 'hub-model' approach have considerable market penetration and significant investments have been made by users to join and collaborate in such ecosystems. Hence, alternatives following the network-model approach will only succeed if they are adequately attractive for both users and IT providers to support. For example, providers of responsible data sharing solutions may see opportunities in offering higher level value added services, such as those based on enhancing inter-organizational relationships, instead of merely enabling trusted data sharing.

A second governance challenge is that initial implementations with sufficient scale are required if they are to attract sufficient investment and lead to the scaling-up of the network-model approach. The introduction of the open network-model infrastructure for trusted data sharing requires initial investments which may not be possible or attractive for individual organizations, specific ecosystems or even industry sectors to make. The overarching benefits of such an open and interoperable data sharing infrastructure to society as a whole may demand alternative public investment and deployment strategies, reflecting the ambition and vision to position the data sharing infrastructure as a common utility. A coordinated public-private development strategy, with several types of organizations each having their own role to fulfil, may be the answer.

In this scenario, we see that the network-model approach with infrastructural data control capabilities may be a natural extension of the service portfolio of *telecommunication service providers*. Traditionally, these organizations operate across a wide range of industry sectors, they have extensive knowledge and experience of large-scale operational support processes for intermediary roles and they have considerable market power to stimulate adoption over various sectors. However, they will need to integrate new capabilities into their core business; specifically, in order to fulfil the required intermediary roles for providing the legal concepts of data sharing agreements and usage contracts as well as support functions.

A second role in the coordinated public-private development strategy is that of *early adopters*, that may include major companies and joint ventures or alliances, sometimes termed field labs. The introduction of the open and federated network-model approach can be spurred through the involvement of such early adopters as, on the one hand, this provides a learning trajectory for both the service providers and the end-users and, on the other hand, it provides opportunities to demonstrate and promote its new functionality with the potential to stimulate interest and adoption for new customers.

Finally, *governmental organizations* have the potential to fulfil several roles in stimulating adoption. They can be an early adopter, as described above, as they have a major need for trusted data sharing with numerous organizations. Hence, the adoption of network-model data sharing solutions by governmental organizations may have major impact on the adoption by the organizations that are sharing data with them. Additionally, they can drive the deployment by stimulating its usage in subsidized innovation projects and by setting stringent requirements for data sovereignty, trust, security and interoperability, including the interoperability of the legal concepts, in their procurement projects. By defining its deployment as prerequisite for granting subsidies, both at the national and the supranational level, the network-model of data sharing may become part of additional innovation developments in various sectors of society that require trusted data sharing.

Conclusion

A primary objective of this paper has been to describe the need and architecture for user-centric data control based on an open, federated and interoperable network-model approach with infrastructural data sovereignty, trust and security capabilities as prerequisite for data owners to adopt data sharing for interorganizational and supply chain IS applications. It has shown that user-centricity is highly intertwined with interoperability on the legal concepts of data sharing agreements and the usage contracts. Hence, focus has been on interoperability of the legal concepts of data sharing agreements and usage contracts. An elaboration has been provided based on the new European Interoperability Framework, distinguishing legal, organizational, semantic and technical interoperability under an overarching integrated governance approach. The concepts as described in this paper will provide data providers with more user-centric options and flexibility in realizing their data control policy, in a world in which data is seen as a valuable asset that needs to be protected. As such, with adequate governance of the development and deployment of the network-model, it may lower the barriers for organizations to share their data in the transition towards a data-centric global information society.

Acknowledgements

The work as presented in this paper has been done as part of the Dutch NWO Research project 'Data Logistics for Logistics Data' (DL4LD, www.dl4ld.net), supported by Dutch Institute for Advanced Logistics 'TKI Dinalog' (www.dinalog.nl) and the Dutch Commit-to-Data initiative (www.dutchdigitaldelta.nl/big-data/over-commit2data).

References

Akoma Ntoso 2019. "XML for parliamentary, legislative & judiciary documents", URL: http://www.akomantoso.org/ (visited on 01/11/2019).

Bench-Capon, T. J. M. and Dunne, P. E. 2007. "Argumentation in artificial intelligence," *Artificial Intelligence,* 171 (10–15), pp. 619–641.

Boer, A. 2009. *Legal theory, sources of law and the semantic web*, Amsterdam: IOS Press.

BIC 2020. "Smart Connected Supplier Network," *Brainport Industry Campus Eindhoven*, URL: https://smartindustry.nl/fieldlabs/8-smart-connected-supplier-network (visited on 02/05/2020).

CEN 2019. "Open XML Interchange Format for Legal and Legislative Resources – CEN Metalex," *European Committee for Standardization (CEN)*, URL: https://joinup.ec.europa.eu/solution/cen-metalex/about (visited on 21/01/2020).

Dalmolen, S., Bastiaansen, H. J. M., Kollenstart, M. and Punter, M. 2019. "Infrastructural Sovereignty over Agreement and Transaction Data ('Metadata') in an Open Network-Model for Multilateral Sharing of Sensitive Data," in *Proceeding of the International Conference on Information Systems (ICIS) 2019*, Munich, Germany, 15th – 18th December 2019. URL: https://aisel.aisnet.org/icis2019/economics_is/economics_is/23/ (visited on 02/16/2020).

DIN 2019. "DIN SPEC 27070: Reference Architecture for a Security Gateway for Sharing Industry Data and Services,". *DIN Standardization Body*, https://www.din.de/en, (visited on 21/11/2019).

Doesburg, R. van, and Engers, T. van 2019. "The False, the Former, and the Parish Priest," in *Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law – ICAIL*, New York: ACM, pp. 194.

EC 2017. "New European Interoperability Framework (EIF) – Promoting seamless services and data flows for European public administrations," *European Union,* 2017, Brussels. URL: https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf (visited on 29/11/2019).

EU 2019a. "Formalized Exchange of Electronic Publications – FORMEX", *European Union Vocabularies*, URL: https://op.europa.eu/en/web/eu-vocabularies/formex (visited on 07/12/2019).

EU 2019b. "European Legislation Identifier – ELI," *European Union Vocabularies*, URL: https://op.europa.eu/en/web/eu-vocabularies/eli (visited on 07/12/2019).

Folmer, E. 2012. "BOMOS: Management and Development Model for Open Standards," *Handbook of Research on E-Business Standards and Protocols: Documents, Data and Advanced Web Technologies, Hershey*, PA: IGI Global, pp. 102-128.

Grover, V., Chiang, R. H. L., Liang, T. P., and Zhang, D. 2018. "Creating strategic business value from big data analytics: A research framework," *Journal of Management Information Systems,* 35 (2), pp. 388–423.

Hillegersberg, J., Moonen, H., and Dalmolen, S. 2012. "Coordination as a Service to Enable Agile Business Networks," in *Proceedings of the International Workshop on Global Sourcing of Information Technology and Business Processes*, Springer, Berlin, Heidelberg, pp. 164-174.

Hofman, W., Punter, M., Bastiaansen, H. J. M., Cornelisse, E., and Dalmolen S. 2016. "Semantic technology for enabling logistics innovations – towards Intelligent Cargo in the Physical Internet," *International Journal of Advanced Logistics,* 5 (2), pp. 58–69.

Hohfeld, W. N., and Cook, W. W. 1919. *Fundamental legal conceptions as applied in judicial reasoning, and other legal essays*, New Haven: Yale University Press.

Loebbecke, C., and Picot, A. 2015. "Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda," *The Journal of Strategic Information Systems* 24 (3), pp. 149–157.

Jarke, M., Otto, B., and Ram, S. 2019. "Data Sovereignty and Data Space Ecosystems," *Business & Information Systems Engineering*, 61 (5), pp. 549–550.

Liezenberg, C., Lycklama, D., and Nijland, S. 2019. *Everything transaction,* Amsterdam, Lannoo Campus.

Luftman, J., Lyytinen, K., and ben Zvi, T. 2017. "Enhancing the Measurement of Information Technology (IT) Business Alignment and Its Influence on Company Performance," *Journal of Information Technology* 32 (1), pp. 26–46.

Mannhardt, F., Koschmider, A., Baracaldo, N., Weidlich, M., and Michael, J. 2019. "Privacy-Preserving Process Mining," *Business & Information Systems Engineering,* 61 (5), pp. 595–614.

MIN EACP 2018. "Generiek afsprakenstelsel voor datadeelinitiatieven als basis van de digitale economie," Dutch Ministry of Economic Affairs and Climate Policy URL: https://www.rijksoverheid.nl/documenten/rapporten/2018/12/30/generiek-afsprakenstelsel-voor-datadeelinitiatieven-als-basis-van-de-digitale-economie (visited on 02/02/2020).

National Research Council 1994. *Realizing the Information Future: The Internet and Beyond.* Washington, DC: National Academies Press.

NLIP - Dutch Neutral Logistics Information Platform 2019. "iSHARE Data Sharing Initiative," *iSHAREworks*, URL: https://www.iSHAREworks.org/en/ (visited on 29/11/2019).

Open Laws 2019. "Compliance – Manage legislation, case law and contracts with ease", *Open Laws*, URL: https://openlaws.com/home (visited on 09/01/2020).

Otto, B., Steinbuss, S., Teuscher, A., and Lohmann, S. 2019. "International Data Spaces: Reference Architecture Model Version 3," *International Data Spaces Association – IDSA*, URL: https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf (visited on 29/11/2019).

Prakken, H. (2010). "An abstract framework for argumentation with structured arguments," *Argument & Computation* 1 (2), pp. 93–124.

Zrenner, J., Möller, F., Jung, C., Eitel, A., and Otto, B. 2019. "Usage Control Architecture Options for Data Sovereignty in Business Ecosystems," *Journal of Enterprise Information Management,* 32 (3), pp. 477–495.