Approaches to Good Data Governance in Support of Public Sector Transformation through Once-only

Maria A. Wimmer[1][0000-0002-8460-1027] Alessia Neuroni[2] Jan Thomas Frecè[3]

[1]Institute for IS Research, University of Koblenz-Landau, Koblenz, Germany
wimmer@uni-koblenz.de
[2]Institute Public Sector Transformation, Berne Univ. of Applied Sciences, Berne, Switzerland
alessia.neuroni@bfh.ch
[3]Institute Sustainable Business, Berne University of Applied Sciences, Berne, Switzerland
jan.frece@bfh.ch

Abstract. The Once Only Principle (OOP) drives current public sector modernization through the reduction of administrative burdens. It requires public authorities not to ask citizens and companies to repeatedly provide information to the public authorities. Instead, public authorities shall share and re-use data among themselves in due respect of data protection regulation. The sharing and re-use of sensitive and non-sensitive data among public administrations demands for broad acceptance by all stakeholders. Trust and transparency are key success criteria in such data-driven public sector transformation. Establishing proper governance mechanisms for the data infrastructures that enable the sharing and re-use in public service provisioning, and that provide the necessary transparency and trust levels is expected to effectively improve public service. This research investigates approaches for establishing a good data governance in OOP settings tackling the sharing and re-use of sensitive or personal data. Geographical focus is on the European Union and Switzerland.

Keywords: Digital transformation, once only principle, OOP, sharing and re-use of sensitive data, data infrastructure, data governance, good data governance

1 Introduction

In the eGovernment Action Plan 2016-2020, the European Union commits to seven principles of public sector transformation in order to modernize governments across Europe and therefore to contribute to economic growth, jobs as well as sustainable and resilient societies [1]. The Once Only Principle (OOP) is one of these principles, aiming at the reduction of administrative burdens by asking citizens and companies to provide certain (standard) information to the public authorities only once. Likewise, public authorities "*take action if permitted to internally re-use this data, in due respect of data protection rules, so that no additional burden falls on citizens and businesses*" [1]. The sharing and re-use of sensitive and non-sensitive data of citizens and companies – such

data has to be differentiated from open and big open linked data (!) – among the actors in public service provisioning demands for broad acceptance by all stakeholders. Trust and transparency are key success criteria in such data-driven public sector transformation. Establishing proper collaborative governance mechanisms for data infrastructures that enable the sharing and re-use in public service provisioning is expected to effectively improve the success of digital transformation in governments.

Fostering data-driven innovation with a successful OOP realization requires coherent data governance to balance openness and public value, as well as privacy and data security [2]. Lending from the good governance principles [3], *good* data governance refers to data governance, which embodies the good governance principles (accountability, coherence, effectiveness, openness, participation, transparency [4]) and caters for the necessary privacy and data security. Good data governance is particularly important when dealing with citizen data, since data access, security, ownership and privacy are more acute for such data [5], [6].

With the vision of the OOP creating value for society and economy through a data-driven transformation of the public sector, trust and transparency become crucial vehicles for success and acceptance. The motivation for this paper is therefore to elicit relevant approaches for a data-driven public sector transformation, which inform a comprehensive good data governance concept for OOP realization. The research question for this paper is: "What prerequisites for sharing and re-using sensitive or personal data in inter-agency collaboration in the public sector exist and how can good data governance mechanisms support a successful OOP implementation therewith nurturing trust and transparency?".

To answer this research question, we investigate scientific literature, strategic policies and case studies of data governance and OOP implementations with the aim to understand the crucial elements for a good data governance concept supporting OOP. The paper employs systematic literature analysis [7]–[9], gathering also insights from existing research on data infrastructures for open data. However, the focus of this paper is on sharing and re-use of sensitive or personal data (not open data). The selection of literature and of strategic documents for this study is based on the one hand on previous research, which the authors conducted in relevant studies (e.g. [10]–[15]). On the other hand, google scholar was scanned and the snowball principle was applied on identified literature to enrich the research with current findings from the literature and with recent strategic documents on public sectors' digital transformation from the EU and Switzerland. The findings from literature were complemented and refined along virtual and physical discussion sessions among the three authors and along asynchronous reviews.

The remainder of the paper is as follows: Section 2 investigates needs for data sharing and re-use concepts for OOP implementations by studying literature on data as an infrastructure and on data-driven transformation. Section 3 reviews digitalization concepts and trends in public sector transformation. It also elaborates challenges and needs of collaboration and stakeholder engagement in order to tackle trust and transparency in OOP settings. The synthesis elicits further needs for good data governance in OOP contexts. Section 4 synthesizes elements of good data governance for OOP realization in inter-agency collaboration. The paper concludes with a discussion and outlook into future research towards a comprehensive good data governance concept.

2 Foundations of Data Sharing and Re-use

The following subsections review academic literature and policy documents regarding data as infrastructure asset and data-driven transformation in the public sector. Each subsection concludes with a synthesis of needs for a comprehensive good data governance concept.

2.1 Data as an Infrastructure Asset in the Public Sector

According to OECD, data has become an essential driver of innovation, and it is considered as one of the society's central infrastructure resources [16]. Shin stresses that data infrastructure is a community-wide need [16] and even a public good.

Data meets typical characteristics of infrastructure resources [17]–[19]: First, data is a non-rival good and it may be consumed for an appreciable range of demands. Second, the social demand for data is driven primarily by downstream productive activities that require them as an input. Third, data may serve as input to a wide range of goods and services. OECD argues that data can serve as a transparent vehicle in the interaction with the sovereign, as an asset for policy making and in the provision of better public services, and/ or – through data exchange – as a bond for strengthening collaboration among public agencies [2].

In the last few years, e-government researchers address infrastructure development in a digital environment, stressing that such infrastructures are to be flexible and evolve over time in accordance with the needs of their multiple users [20]. Zuiderwijk criticizes, though, that there is no common understanding of what an infrastructure comprises [21]. Interestingly, little research addresses data as infrastructure asset in the public sector.

Bekkers stresses that data infrastructures entail both technical and social elements [22]. This understanding is extended by Jetzek, who adds a regulatory infrastructure besides the IT infrastructure [23]. The regulatory infrastructure is crucial for trustworthiness, transparency and accountability in sharing sensitive or personal data. However, in a digitalized world, the operationalization of the regulatory or social elements need to be mapped to, and be holistically intertwined with the technical infrastructure.

Data-exchange infrastructures enabling inter-agency collaboration [24] in OOP contexts (i.e. sharing and re-using personal and sensitive data of citizens or business) provide the foundations for interoperable and re-usable solutions of seamless public service provisioning. They embody base registers and directories as key components that are legally controlled and maintained by public administrations and provide authentic sources of information on items such as persons or companies. Along these lines of digital transformation, authentic sources are a key enabler for enhanced service provision. Next, we therefore outline the political significance of data-driven transformation.

While the current research on data as infrastructure focuses mostly on public and open data (see e.g. [19], [21], [25]), the realization of the once-only principle demands for the sharing and re-use of data that is sensitive and that falls under the data protection regulations. We therefore resume that a comprehensive governance for data infrastruc-

tures (that enables the sharing and re-use of sensitive and personal data) requires mechanisms to address trustworthiness, transparency as well as data protection to ensure the acceptance by the users. Furthermore, such governance mechanisms must provide appropriate support of inter-agency collaboration. Accordingly, governance mechanisms therefore need to operate in two directions: towards the customer of public service and in the interplay among public agencies.

2.2 Political Significance of Data-driven Transformation with the OOP

While, as mentioned before, the discussion in the area of data-driven transformation so far focuses on open data infrastructure, the once-only principle addresses sensitive and non-sensitive data. Subsequently, we review the discourse of data as an infrastructure asset with focus on the public sector, highlighting the political relevance of data-driven transformation in an international setting.

A customer-centric approach conveys the proposition of creating value for society and economy. The once-only principle demands that citizens and companies will only have to provide certain standard information to the public agencies once. The once-only principle therefore requires to re-use and exchange (sensitive and personal) data within public authorities to reduce administrative burden for citizens and businesses [1], [26]–[29]. However, sharing and re-use of such data must be done with due respect of data protection regulations [30], as otherwise trustworthiness of public service provisioning would be hampered tremendously. Hence, trust plays an essential role in inter-agency collaboration.

The implementation of the once-only principle in the European Union is a policy goal settled in the eGovernment Action Plan 2016-2020 [1] and one of the pillars of the strategy for the Digital Single Market [31]. It has been reinforced in the "Tallinn Declaration" signed by the European digital ministers [32] in 2017. The OOP principle is also the underlying vision for the Single Digital Gateway (SDG) Regulation [33], which requires European Member States to build up and connect to a single European portal and infrastructure, through which citizens, businesses and public administrations can execute public services across borders with the OOP as underlying principle.

While the overall implementation of the OOP and of the SDG are still fragmented across the EU, and cross-border applications are limited to a few cases and services, mature infrastructure exists for example in Belgium, Estonia or the Netherlands [12], [34], [35]. In Switzerland, data as infrastructure and data governance play a key role in national strategic papers such as the "Digital Switzerland Strategy" (cf. [19], [36]) and the renewed "E-Government Strategy 2020-2023". Even though Switzerland is not an early adopter regarding digital transformation of the public sector [37], data-centric public sector transformation is gaining political awareness and importance.

To realize the SDG or the Swiss E-Government Strategy, a successful implementation of the OOP requires transfer and re-use of sensitive or personal data between government agencies across borders involving actors on different levels of a political system. Significant effort for the development of a technical infrastructure as well as organizational frameworks are currently developed in several research projects. In an analysis of drivers and barriers for OOP implementation in the SCOOP4C project, trust

is stressed as underlying condition [12], [38], [39]. In the TOOP project, trust is addressed with a technical approach by defining a trust architecture as part of the system design [40], [41]. In a broader perspective, TOOP also links the question of trust to the organizational culture of government agencies. However, a systematic and scientifically grounded rigorous analysis of the organizational challenges is currently lacking.

To investigate and elicit the requirements of interoperable data and information sharing along a structured approach, the European Interoperability Framework (EIF) provides a conceptual model for public services and considers data-related services as a basic component for service provision [42]. The SCOOP4C and TOOP projects rely on this EIF to structure their investigations of barriers, enablers and architecture for a comprehensive OOP implementation.

The investigation of the political significance of data-driven transformation with the OOP unveils, in addition to trust, the need for architectural features and interoperability to be addressed in a comprehensive good data governance concept.

3 Digitalization & Collaboration Concepts in the Public Sector

Research on public sector digitalization is continuously changing to reflect how governments react to social, economic, political and other pressures, and how they transform themselves in the process [43]. In this section, we review digitalization concepts and trends of the public sector, and introduce collaboration as a core asset and challenge in the digital transformation. Stakeholder engagement is the third concept, which we see highly relevant when implementing the OOP through data infrastructures in systems interacting across different borders (federal, cross-border in the EU, and similar).

3.1 Digitalization Concepts and Trends in Public Sector Transformation

In literature, scholars discuss the e-government evolution along different models (information, interaction, transaction, integration; e.g. [44]–[46]). Janowski [43] argues that the concept of electronic government evolves toward more complexity and greater contextualization and specialization. His evolution model comprises digitalization (i.e. technology in government), transformation, engagement and contextualization (i.e. policy-driven digital governance). While digital transformation in the private sector is mostly associated with the need to use new technologies to stay competitive, the goal in the public sector can be manifold: transforming service delivery, transforming organizational culture and relationships with citizens, or value creation as a transformation outcome [47]. These different aspects need integration into a comprehensive good data governance concept.

Recent annual OECD reports spot relevant digitalization trends. The 2017 report stresses new approaches to activating citizens as a partner to shape the future together [48]. In 2018, improving identity, systems approaches and enablers, and inclusiveness are identified as key trends [49]. The 2019 report argues trends such as more transparency, new technologies / open government data / new business models for new ways of

public value creation, and transforming policy-making and legislation to be machine-readable and based on algorithms [50]. Exchange of sensitive or personal data between agencies touches upon all of these trends and needs thorough investigation of trustworthiness and data governance.

3.2 Collaboration as Core Asset for Transformation

Inter-agency information sharing is discussed in e-government literature as critical to helping solve complex challenges that are beyond the capacities and capabilities of a single agency. While hierarchical structures continue to have value for government, they do hinder efforts to respond to those policy problems and demands that require collaborative approaches. Clarity of roles and responsibilities nurtures the success of inter-organizational efforts by enabling other relevant determinants, such as building trust among members, increasing their willingness to participate, and mitigating concerns about security [51].

Even though cooperation and collaboration have been addressed in research in the context of digitalization of government, there are few validated results about the determinants of effective governance in inter-organizational settings, especially in the public sector [18]. Research in the field deals with the challenges for inter-organizational cooperation and/or formulates strategies on how to deal with identified key barriers. It often focuses on issues related to cross-agency information sharing in the context of service delivery [52]. Generally, there is a consent that inter-organizational cooperation is demanding: it often combines competition, questions of autonomy, and interdependence [53] and relates to issues associated with the notion of trust [54], [55]. Accordingly, governing and managing in inter-organizational arrangements is different from management within organizations. Enabling leadership is important, since there is no central authority [24]. To illustrate the specific requirements with regard to leading inter-organizational e-government projects, Thomson and Perry identify key dimensions of collaboration, focusing on concrete activities and processes from collaborative governing and administration over forging mutually beneficial relationships to establishing social norms [56].

Klievink and Janssen [57] elaborate on the need for a coordinated e-government service delivery and propose an analytical framework of coordination. They stress that coordination creates dependencies at various levels, including channels for contacting government agencies, business processes, information (systems) and infrastructural dependencies within and among governmental organizations. The most recent version of the European Interoperability Framework (EIF) embodies the concepts of interoperability governance and public service governance as key pillars to ensure interoperability in inter-agency collaboration [13], [42], [58], [59].

3.3 Stakeholder Engagement

The term ‘stakeholder’ stems from organizational theory and has become an integral concept of information systems research. Freeman defines stakeholder as *“any group or individual who is affected by or can affect the achievement of an organization’s*

objectives" ([60], p. 3). Bryson argues that stakeholders and their concerns "*must be taken into account by leaders, managers and front-line staff*" [61].

In particular along the transition to deliver online public services basing on the OOP, public services need to be designed 'customer-centric by default', encompassing simplification and seamless combinations of service building blocks from different government entities [62] and with the customer's needs at focus. Concepts like co-creation and co-production can help to engage citizens and other stakeholders in the innovation of public service routines [63].

The SCOOP4C project studied different stakeholder roles along the provision and consumption of data in public services as well as the supervision of compliance towards data protection and privacy [14]. The study comprises case studies to elicit stakeholders and their roles in four public service contexts with sharing and re-use of sensitive or personal data. Subsequently, Panopolou et al. developed a stakeholder engagement plan, which guides strategic decision-makers and project managers in how to involve relevant stakeholders with their different roles in the design and implementation of OOP-driven public services [15].

Stakeholder engagement is a core concept of architecture frameworks like The Open Group Architecture Framework [64]. Such architecture frameworks must provide methods and tools to identify and manage the stakeholder concerns and their interrelationships [61], [64] on the data sharing and re-use contexts.

4 Good Data Governance for OOP Realization

Wang investigates six driving forces or barriers in inter-agency government information [data] sharing: administrative pressure, legal power, department capacity, department interest, risk and accountability, and information demand [65]. The author puts these forces into a dynamic mechanism model of interagency government data sharing and argues that these cross-boundary views need to be properly addressed in an architectural framework supporting good data governance, which include effective mechanisms for incentives, empowerment, institutional enablement, accountability, pulling of data demands, and feedback. In view of implementing the OOP, fostering data-driven innovation therefore requires coherent good data governance to balance access to data and public value, as well as ownership, privacy and data security [2], [5]. Rosenbaum describes this as the process of conceptualizing and realizing data stewardship responsibilities [5], providing a set of governance policies, principles, functions and structures to steer data use and re-use in inter-agency collaborations. To create public and economic value, incentive systems for cooperation and collective action to realize the OOP are needed, covering the entire data life-cycle, as stressed e.g. in [22], [24], [66]–[68].

Implementing the sharing and re-use of data in inter-agency contexts demands for appropriate organization-wide and inter-agency data governance policies, principles, functions and structures that ensure data quality (through data quality governance) (see e.g. [69]), data availability (data access), adherence to the data principles, data life-cycle and proper use of semantics/metadata [70], [71]. In a literature review, Brous et

al. spotted 25 core concepts and principles of data governance, which they clustered into four data governance principles: organization, alignment, compliance, and common understanding [72]. Similarly, Thomson et al. identified three pillars of effective data governance: people, standards and compliance [73].

IT governance research suggests three concepts for preparing, making and implementing decisions on strategic and tactical level, namely: structures, processes, and relational mechanisms [71]. These components are also relevant to data governance. While company-wide data governance frameworks (incl. data quality) have been a topic in information science for decades [69], the inter-organizational use of distributed data raises new challenges. Data governance therefore needs to focus on the key elements that are relevant for cross-boundary common views of reality [74]. In a case study, a set of governance roles and functions was identified [59] and different governance structures were depicted for the digitization of public service and interoperability along four levels of governance: policy (legislation), strategic, tactical and operational [13], [58]. Good data governance needs to provide respective organizational models (structures) for governance and the corresponding roles and functions assigned to the responsible actors to ensure effective and sustainable enablement of sharing and re-use of (sensitive or personal) data in public service provisioning [75]. A relevant framework guiding in the implementation of the OOP is the EIF [42]. The four layers serve as a structure to address open issues in the sharing and re-use of data in inter-agency collaboration.

5 Discussion and Future Research

This paper aimed at reviewing existing literature, policy documents and case studies of data governance and digital transformation in the public sector with a scope of implementing the once-only principle. The objective was to identify factors for a comprehensive good data governance concept, which tackles relevant aspects related to the sharing and reuse of sensitive or personal data in public service provisioning, where the once-only principle is applied.

In answering the research question posed in the introduction, the review of relevant literature identified the following factors, which a comprehensive good data governance concept should address when sharing and reusing sensitive or personal data in public service provisioning based on the OOP:

- To effectively realize digital transformation in the public sector, data is a central infrastructure asset. The different roles data play in public service require a differentiated approach to data infrastructures and to data governance:
  - Open data infrastructures require their peculiar data governance as is discussed largely in literature;
  - The sharing and reuse of sensitive or personal data in inter-agency collaboration demands for its own data infrastructures and good data governance mechanisms. In particular, trustworthiness, transparency and data protection are concepts that must be embodied in a comprehensive good data governance concept.

  - Furthermore, a comprehensive good data governance needs to encompass diversified mechanisms of granting access to data from base registers vs. data being collected from normal sources or form the users.
- The once-only principle builds on data sharing and re-use in inter-agency collaboration of public sector actors. To effectively enable inter-agency collaboration in OOP settings, governance mechanisms need to address stakeholder engagement and data governance in two directions: towards the customer of public service (citizens and business) and in the interplay among public agencies.
- Since the OOP is put forward and politically promoted at European Union level, interoperability is an asset that needs to ensure interoperability and common approaches to data infrastructures at EU and in Member States (and affiliated countries such as Switzerland) alike. The European Interoperability Framework provides a good basis for this. However, in the individual countries, interoperable implementations need to reach out also to the local level actors. A comprehensive good data governance concept needs to reflect this differentiating structural dimension. It needs to accommodate the application of available standards and it needs to ensure compliance of solutions with the political, legal and organizational foundations.
- To master the complexity resulting from the manifold views and viewpoints of sharing and reusing sensitive or personal data in public services, a comprehensive good data governance concept should be closely connected with a supportive architectural framework. Such an architectural framework can guide in the handling of different views and viewpoints, in particular in data sharing in inter-agency collaboration, to tackle the necessary trust, transparency and data protection needs.
- With the new trends in digital transformation as reported in section 3.1, a good data governance concept becomes even more important to ensure trustworthiness and transparency, and ultimately user acceptance of new ways and models of delivering public services. Therefore, stakeholder engagement and co-creation mechanisms need to form integral components of such a governance concept.
- A comprehensive good data governance concept needs to embody clear roles, responsibilities and functions of the actors that interact in data sharing and reuse in OOP contexts and in inter-agency collaborations at different levels of government.
- Beyond individual considerations along the above needs, a good data governance concept has to tackle the interdependencies and mutual influences among these aspects, leading to a comprehensive framework that is actionable. This includes governance policies, principles, functions (or processes) and structures to steer data use and re-use in inter-agency collaboration (including data infrastructures) along the entire data life-cycle.

To sum up the findings in this paper, good data governance not only needs to clarify who can have access to what data for what purpose and under what conditions. It also needs to assign responsibilities and retribution mechanisms for data maintenance and enhancement to ensure the sustainability, trustworthiness and transparency of the common data infrastructure along with the implementation of the good governance principles. All these aspects need to be integrated into a comprehensive concept for a trustworthy and transparent data infrastructure enabling the sharing and re-use of (sensitive

or personal) data. The development of such a comprehensive good data governance concept, which also embodies the relevant data and IT security mechanisms, is a next step of our research. The result is envisaged as a framework for good data governance, which addresses the good data governance principles and relevant implementation mechanisms. Along this next step of research, the differentiation of sensitive and non-sensitive data needs to be revisited and examined in more detail. The examination of the resulting good data governance concept is planned through case study research and qualitative empirical research.

References

1. European Commission: EU eGovernment Action Plan 2016-2020 - Accelerating the Digital Transformation of Government. COM/2016/0179 final, Brussels (2016).
2. OECD: Data-Driven Innovation: Big Data for Growth and Well-Being. Paris (2015).
3. Agere, S.: Promoting Good Governance: Principles, Practices and perspectives. Management and Training Services Division, Commonwealth Secretariat, London (2000).
4. European Commission: European Governance - A white paper. Official Journal of the European Communities, Brussels (2001).
5. Rosenbaum, S.: Data governance and stewardship: Designing data stewardship entities and advancing data access. Health Services Research 45 (5), 1442–1455 (2010).
6. Schintler, L. A., Kulkarni, R.: Big data for policy analysis: The good, the bad, and the ugly. Review of Policy Research 31(4), 343–348 (2014).
7. Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., Linkman, S.: Systematic literature reviews in software engineering – a systematic literature review. Information and Software Technology 51(1), 7–15 (2009).
8. Webster, J., Watson, R. T.: Analyzing the Past to Prepare for the Future: Writing a literature review. MIS Qarterly 26(2), iii–xiii (2002).
9. Müller-Bloch, C., Kranz, J.: A Framework for Rigorously Identifying Research Gaps in Qualitative Literature Reviews. In: Proceedings of Thirty-Sixth International Conference on Information Systems (2015).
10. Estermann, B., Fraefel, M., Neuroni, A. C., Vogel, J.: Conceptualizing a national data infrastructure for Switzerland. Information Polity (2018).
11. Klievink, B., Neuroni, A., Fraefel, M., Zuiderwijk, A.: Digital strategies in action - A Comparative analysis of national data infrastructure development. In: Proceedings of the 18th Annual International Conference on Digital Government Research (2017).
12. Roustaei, A. et al.: Gap analysis report of challenges, needs and benefits of the OOP4C analysis. SCOOP4C Consortium, https://scoop4c.eu/sites/default/files/2019-06/SCOOP4C_D4.1_v1.1.pdf (2019).
13. Wimmer, M. A., Scanlon, M., Boneva, R., Rigole, C.: Interoperability governance models. Deliverable for ISA2 Action, European Commission (2017).
14. Kalampokis, E. et al.: Identification and mapping of stakeholders. SCOOP4C Consortium, https://scoop4c.eu/sites/default/files/2018-01/SCOOP4C_D2.1.pdf (2017).
15. Panopoulou, E. et al.: Strategic stakeholder engagement plan. SCOOP4C Consortium, https://scoop4c.eu/sites/default/files/2019-10/SCOOP4C_D22_v1.14_final_0.pdf (2019).
16. Shin, D. H.: A critique of Korean National Information Strategy: Case of national information infrastructures. Government Information Quarterly 24(3), 624-645, DOI: 10.1016/j.giq.2006.06.011 (2007).

17. Frischmann, B. M.: An Economic Theory of Infrastructure and Commons Management. Minnesota Law Review 89(4), 917–1030 (2005).
18. Estermann, B., Riedl, R., Neuroni, A. C.: Integrated and Transcendent e-government: Keys for Analyzing Organizational Structure and Governance. In: Proceedings of DG.O, pp. 162–171 (2009).
19. Klievink, B., Neuroni, A. C., Fraefel, M., Zuiderwijk, A.: Digital Strategies in Action – a Comparative Analysis of National Data Infrastructure Development. In Proceedings of DG.O, pp. 129–138 (2017).
20. Janssen, M., Chun, S. A., Gil-Garcia, J. R.: Building the next generation of digital government infrastructures. Government Information Qarterly 26(2), 233-237 (2009).
21. Zuiderwijk, A.: Open data infrastructures: The design of an infrastructure to enhance the coordination of open data use. Doctoral Thesis, TU Delft, 's-Hertogenbosch, https://doi.org/10.4233/uuid:9b9e60bc-1edd-449a-84c6-7485d9bde012 (2015).
22. Bekkers, V.: Flexible information infrastructures in Dutch E-Government collaboration arrangements: Experiences and policy implications. Gov. Inform. Qu. 26(1), 60-68 (2009).
23. Jetzek, T.: Managing complexity across multiple dimensions of liquid open data: The case of the Danish Basic Data Program. Government Information Quart. 33(1), 89-104 (2016).
24. Neuroni, A. C., Fraefel, M., Riedl, R.: Inter-organizational cooperation in Swiss eGovernment. In: Proceedings of IFIP EGOV, LNCS 6846, pp. 259-272 (2011).
25. Zuiderwijk, A., Janssen, M.: Open data policies, their implementation and impact: A framework for comparison. Government Information Quarterly 31(1), 17-29 (2014).
26. Wimmer, M. A., Marinov, B.: SCOOP4C: Reducing administrative burden for citizens through once-only - Vision & challenges. Jusletter IT (2017).
27. Stocksmeier, D., Wimmer, M. A., Führer, M., Essmeyer, K.: Once-Only in Deutschland und Europa: Eine Roadmap grenzüberschreitender Vernetzung im Bereich Steuern. In: Digitalisierung von Staat und Verwaltung, pp. 87–98 (2019).
28. Kalvet, T., Toots, M., van Veenstra, A. F., Krimmer, R.: Cross-border e-Government Services in Europe: Expected Benefits, Barriers and Drivers of the Once-Only Principle. In: Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance (ICEGOV'18), pp. 69-72 (2018).
29. Krimmer, R., Kalvet, T., Toots, M., Cepilovs, A., Tambouris, E.: Exploring and Demonstrating the Once-Only Principle: A European Perspective. In: Proceedings of the 18th Annual International Conference on Digital Government Research, pp. 546–551 (2017).
30. European Union: Regulation 2016/679 of the European parliament and the Council of the European Union. Official Journal of the European Communities, https://eur-lex.europa.eu/eli/reg/2016/679/oj (2016).
31. European Commission: A Digital Single Market Strategy for Europe. COM(2015) 192 Final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192 (2015).
32. Tallinn Declaration: Tallinn Declaration on eGovernment at the Ministerial Meeting during Estonian Presidency of the Council of the EU. https://ec.europa.eu/newsroom/document.cfm?doc_id=47559 (2017).
33. European Union: Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services. Official Journal of the European Communities, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.295.01.0001.01.ENG (2018).
34. Cave, J., Botterman, M., Cavallini, S., Volpe, M.: EU-wide digital Once-Only Principle for citizens and businesses. Study for the European Commission, https://ec.europa.eu/esf/transnationality/filedepot_download/1671/1692 (2017).

35. Vallner, U. et al.: State of play report of best practices. SCOOP4C Consortium, https://scoop4c.eu/sites/default/files/2018-01/SCOOP4C_D1.2_0.pdf (2017).
36. Schweizerische Eidgenossenschaft: Strategie „Digitale Schweiz“. Bundesrat, Bern, https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/strategie-digitale-schweiz.html (2018).
37. Neuroni, A., Kissling-Näf, I., Riedl, R.: E-Government und smarter Staat: Die Schweiz auf halbem Weg. In: Stember, J. et al. (eds.): Handbuch E-Government. Springer Gabler, Wiesbaden, pp. 163-180 (2019).
38. Wimmer, M. A., et al.: Roadmap for future areas of actions, and policy recommendations. SCOOP4C Cons., https://scoop4c.eu/sites/default/files/2019-11/SCOOP4C_D4.2_v1.2.pdf (2019).
39. Wimmer, M. A. et.al.: Vision of the once-only principle for citizens, including key enablers and major barriers. SCOOP4C Consortium, https://scoop4c.eu/sites/default/files/2018-01/SCOOP4C_D1.1.pdf (2017).
40. Pavleska, T., Aranha, H., Masi, M., Grandy, E., Sellitto, G. P.: Cybersecurity Evaluation of Enterprise Architectures: The e-SENS case. In: Proceedings of PoEM 2019, pp. 226–241 (2019).
41. Grandy, E. et al.: Generic Federated OOP Architecture. TOOP Consortium, http://www.toop.eu/sites/default/files/D22_Generic_Federated_OOP_Architecture_Final.pdf (2018).
42. European Commission: New European Interoperability Framework - Promoting seamless services and data flows for European public administrations. Publications Office of the European Union, Luxemburg (2017).
43. Janowski, T.: Digital government evolution: From transformation to contextualization. Government Information Quarterly 32(3), 221-236 (2015).
44. Layne, K., Lee, J.: Developing fully functional E-government: A four stage model. Government Information Quarterly 18(2), 122-136 (2001).
45. Andersen, K.V., Henriksen, H. Z.: E-government maturity models: Extension of the Layne and Lee model. Government Information Quarterly 23(2), 236–248 (2006).
46. Scholta, H., Mertens, W., Kowalkiewicz, M., Becker, J.: From one-stop shop to no-stop shop: An e-government stage model. Government Information Qu. 36(1), 11-26 (2019).
47. Mergel, I., Edelmann, N., Haug, N.: Defining digital transformation: Results from expert interviews. Government Information Quarterly 36(4), 101385 (2019).
48. OECD: Embracing Innovation in Government - Global Trends 2017 (2017).
49. OECD: Embracing Innovation in Government - Global Trends 2018 (2018).
50. OECD, Embracing Innovation in Government. Global Trends 2019 (2019).
51. Gil-Garcia, J. R., Guler, A., Pardo, T. A., Burke, G. B.: Characterizing the importance of clarity of roles and responsibilities in government inter-organizational collaboration and information sharing initiatives. Government Information Quarterly 36(4), 101393 (2019).
52. Karlsson, F., Frostenson, M., Prenkert, F., Kolkowska, E., Helin, S.: Inter-organisational information sharing in the public sector: A longitudinal case study on the reshaping of success factors. Government Information Quarterly 34(4), 567-577 (2017).
53. McGuire, M.: Collaborative public management: Assessing what we know and how we know it. Public Administration Review 66(s1), 33-43 (2006).
54. Agranoff, R., McGuire, M.: Big Questions in Public Network Management Research. Journal of Public Administration Research and Theory 11(3), 295-326 (2001).
55. Gil-Garcia, R. J., Chengalur-Smith, I. S., Duchessi, P.: Collaborative e-Government: Impediments and benefits of information-sharing projects in the public sector. European Journal of Information Systems 16(2), 121-133 (2007).

56. Thomson, A. M., Perry, J. L.: Collaboration processes: Inside the black box. Public Administration Review 66(s1), 20-32 (2006).
57. Klievink, B., Janssen, M.: Developing Multi-Layer Information Infrastructures: Advancing Social Innovation through Public-Private Governance. Information Systems Management 31(3), 240-249 (2014).
58. Wimmer, M. A., Boneva, R., di Giacomo, D.: Interoperability Governance: A Definition and Insights from Case Studies in Europe. In: Proceedings of 19th Annual International Conference on Digital Government Research (2018).
59. Wimmer, M. A., Zamboni, A., Boneva, R.: Organisational interoperability guidelines. Deliverable for ISA2 Action, European Commission (2016).
60. Freeman, E. R.: Strategic Management: a Stakeholder Approach. Pitman, New York (1984).
61. Bryson, J. M.: What to do when stakeholders matter: stakeholder identification and analysis techniques. Public Management Review 6(1), 21–53 (2004).
62. Kavanaugh, A. L. et al.: Social media use by government: From the routine to the critical. Government Information Quarterly 29(4), 480-491 (2012).
63. Wimmer, M. A., Scherer, S.: Supporting communities through social government in co-creation and co-production of public services: The SocialGov concept and platform architecture. International Journal of Public Administration in the Digital Age 5(1), 18–35 (2018).
64. The Open Group: The TOGAF® Standard. Version 9.2, 11th edition, Van Haren Publishing (2018).
65. Wang, F.: Understanding the dynamic mechanism of interagency government data sharing. Government Information Quarterly 35(4), 536–546, 2018.
66. Cordella, A., Bonina, C. M.: A public value perspective for ICT enabled public sector reforms: A theoretical reflection. Government Information Qu. 29(4), pp. 512-520 (2012).
67. Millard, J.: Open governance systems: Doing more with more. Government Information Quarterly 35(4), 577–587 (2018).
68. Klievink, B., Bharosa, N., Tan, Y.-H.: The collaborative realization of public values and business goals: Governance and infrastructure of public–private information platforms. Government Information Quarterly 33(1), 67–79 (2016).
69. Weber, K., Otto, B., Österle, H.: One Size Does Not Fit All---A Contingency Approach to Data Governance. Journal of Data and Information Quality 1(1), Article 4, https://dl.acm.org/doi/10.1145/1515693.1515696 (2009).
70. Cheong, L. K., Chang, V.: The need for data governance: a case study. In: Proceedings of 18th Australasian Conference on Information Systems, pp. 999–1008 (2007).
71. Khatri, V., Brown, C.: Designing data governance. Communications of the ACM 53(1), 148–152 (2010).
72. Brous, P., Janssen, M., Vilminko-Heikkinen, R., Coordinating Decision-Making in Data Management Activities: A Systematic Review of Data Governance Principles. In: Electronic Government, Proceedings. LNCS 9820, Springer Verlag, pp. 115–125 (2016).
73. Thompson, N., Ravindran, R., Nicosia, S.: Government data does not mean data governance: Lessons learned from a public sector application audit. Government Information Quarterly 32(3), 316–322 (2015).
74. Soma, K., Termeer, C., Opdam, P.: Informational governance – A systematic literature review of governance for sustainability in the Information Age. Environmental Science & Policy 56, 89–99 (2016).
75. Spichiger, A., Rötzer, H. J., Neuroni, A.: Hoheitliches Handeln und Registerführung. In: Stember, J. (eds): Handbuch E-Government. Springer Gabler, Wiesbaden, pp. 229–244 (2019).