

Evgeniia Rudenko

Architectural Blueprint of a One-stop government in Germany, aligning the implementation of the Once-only and the Privacy by design principles

Master Thesis

at the Chair for Information Systems and Information Management
(Westfälische Wilhelms-Universität, Münster)

Supervisor: Dr. Hendrik Scholta
Tutor: Marco Niemann, M.Sc.

Presented by: Evgeniia Rudenko
Schlossplatz 2
48149 Münster
+49 251 8338100
e_rude01@uni-muenster.de

Date of Submission: 2020-05-30

Content

Figures

Abbreviations

BDSG	Bundesdatenschutzgesetz – Federal Act on Data Protection
CEF	Connecting Europe Facility
DSR	Design Science Research
eID	Electronic identification
eIDAS	Electronic Identification, Authentication and Trust Services Regulation
EIF	European Interoperability Framework
EIRA	European Interoperability Reference Architecture
EU	European Union
G2B	Government-to-business
G2C	Government-to-citizen
G2G	Government-to-government
GDPR	General Data Protection Regulation
IS	Information Systems
ISA	Interoperability solutions for public administrations
OOP	Once-only principle
OSG	One-stop government
OZG	Online-Zugangsgesetz – Online Access Law
PbD	Privacy by design
SDG	Single Digital Gateway
TOOP	The Once-only Principle (Project)

1 Introduction

As well as many other areas of public sector reform, the development of eGovernment is confronted with many imperatives for designing processes and information systems to achieve high acceptance among the users. User-centricity. Availability. Security. Some of these imperatives are straightforward and easily understood, drawing on practice and digital experiences from the private sector. Some of them are, however, highly obscure and require contextualization.

The experience of digital public services in some member states of the European Union, particularly of Estonia, shows that there are principles in digital administrative service provision that endorse use and satisfaction with electronic government. Due to the fact that adhering to them promises efficiency and effectiveness gains in public service provision, national eGovernment projects try to integrate these best practice solutions. Moreover, they are supported by and promoted on the European Union level, as their implementation in the national contexts contributes to the establishment of the Digital Single Market. One of such principles is the Once-only principle, seen as a strategic building block in the development of the Single Digital Gateway.

Indeed, requiring citizens to supply the same data to public administrations only once with the potential for being reused in providing other government services, the Once-only principle reduces the bureaucratic burden associated with public services. However, being appealing in its implementation it raises several concerns. Identifying requirements, which need to be fulfilled in different national contexts in order to achieve the necessary level of administrative integration, is complicated. Simultaneously, administrative reuse of data is often associated with losing transparency of data handling, which raises privacy concerns. Such an image of a digital administration that processes citizen data in an obscure manner is especially critical in privacy-sensitive society, such as Germany.

One of the ways to address this issue is to implement privacy-sensitive administrative processes and information systems, which ensure privacy protection by design, also known as the Privacy by design principle. This notion has long been debated in the German public discourse, being often brought up by the Data Protection institutions as an essential element of the German eGovernment. Nevertheless, its fundamental requirements remain as unclear to practitioners, as in the case of the Once-only principle.

This thesis has taken up a two-fold objective of addressing these issues. On the one hand, this work aligns the implementation of the Once-only principle with privacy sensitivity, bringing together the introduction of the Once-only and the Privacy by design principles. On the other hand, this work strives to achieve a profound practical understanding of the

two high-level supra-national principles in the national context of Germany. Thus, the ultimate goal of this research is to bring together the operational meaning of the two principles and align their implementation to demonstrate the possibility for greater acceptance of digital public services.

In order to achieve this goal, the author will be utilizing the methodological framework of design science research. It means that the author will, drawing upon scientific contributions, 1) identify a practical problem and motivate the required solution. This will be achieved by analyzing the existing eGovernment infrastructure and strategy in Germany. Furthermore, the author will 2) provide further details on the methodological underpinnings of this work, including the methods used for the solution development. In what follows 3) the objectives for the solution will be defined by conducting a literature review on the OOP and the PbD. These requirements will be presented, as they appear in the EU and national regulation in Germany in order to frame further development of the artifact and delineate the set of regulatory documents addressed. Then, 4) the artifact will be developed. The desired outcome is to create an architectural blueprint of the OOP and PbD implementation in Germany, which addresses the previously identified requirements, fulfilling the two principles. Following the blueprint development, the author will 5) demonstrate the application of the architectural blueprint through selected administrative procedures. Finally, 6) the limitations of this work and the solution, in particular, will be discussed. The author will then conclude by outlining the research agenda on the topic and in relation to the developed artifact.

In addition, it is worth highlighting that the understanding of principles in this work is grounded on the research from the area of public administration, seeing them as a regulatory mechanism, requiring compliance with. Thus, this work builds on the German national and EU-level regulatory underpinnings of every requirement, fulfilling the implementation of the Once-only and the Privacy by design principles. This circumstance defines the method selected for the artifact development - the legal specification method.

Finally, the developed solution will be utilizing the already existing eGovernment infrastructure and strategy in Germany. Nevertheless, while this thesis is drawing on conclusions from the previous empirical research, which accompanied EU-level eGovernment projects, related to the implementation of the Once-only principle, the notion of the One-stop government portal will be introduced additionally. Research findings and the EU regulatory requirements point out that the OOP has been viewed as an inherent part of the OSG concept, with the citizen using a single portal to request administrative services. Thus, this work proceeds with suggesting an OSG interface for Government-to-Citizen interaction as a future direction for the OOP implementation.

2 Research Background: OOP and PbD in the German eGovernment.

2.1 Effective eGovernance with OOP and PbD.

Building eGovernment, which promises higher internal efficiency of the public sector and increases the quality of services provided to citizens and businesses, has been one of the highest strategic priorities along with the development of the EU Digital Single Market (European Commission, 2016a). Moreover, eGovernment has proven to be capable of unlocking a single country's economic and societal potential, while "being integrated into governments' modernization strategies" (European Commission, 2016a). However, striving to reduce administrative burden and increase transparency in communication between citizens and businesses and public administrations by applying digital technology, governments of all administrative levels often face challenges. Implementation of eGovernment practices crosses as a red line through different spheres of public sector services - from legal to processual, to technical. Thus, building eGovernment is not an easy effort, and issues, encountered along these processes can be both similar among countries and individual and, therefore, cannot always be solved, relying on high-level principles or best practices.

Public e-services development in the EU context has proven that the success factors of eGovernment efforts cannot be defined solely by vast economic and infrastructural potential. Neither does the use of digital technology define usability and eagerness to use online public services as an alternative to traditional public-private communication channels. According to the recent evaluations of the EU eGovernment Benchmark, for instance, "Germany's relative indicators show a country with almost all environmental characteristics (User characteristics, Government characteristics and Digital context characteristics) in line with the European average" with the quality of government actions exceeding the European average (European Commission, 2019). According to the analysis of these characteristics, one could see Germany as a front-runner in digital government solutions and service provision (European Commission, 2019). Nevertheless, Germany is still underperforming in Penetration and Digitization, understood in the eGovernment Benchmark study as an outcome of non-consolidated and unexploited eGovernment services. Such condition requires policies, targeted at "increasing the number of citizens using online services and the level of the back-office and the front-office digitization" (European Commission, 2019).

Although the reasons for low levels of Penetration and Digitization in German administrations are not specified in the eGovernment Benchmark study, there have been numerous independent research efforts, focusing on challenges of the German public e-

service development. In order to address them, the current government has taken a strategic stance towards eGovernment implementation by confirming its commitment to put eGovernment tools in place in the Coalition Treaty (Stocksmeier et al., 2019). Moreover, in order to stir digital public services development efforts on all administrative levels, the current government adopted the regulation on Online Access (Online Access Law - Online-Zugangsgesetz (OZG)), which requires administrations of all levels to enable 575 digital government services by 2022 (Onlinezugangsgesetz – OZG, 2017).

This regulation suggests not only that the range of public services available online will be increased for the convenience of citizens (Rüscher, 2017). The OZG-implementation with a 2022 target aims at increasing local and state government efforts in digitalizing their services and processes, as well as coordinating the set-up of online access among multiple stakeholders, embracing government-to-government (G2G), government-to-business (G2B) and government-to-citizen (G2C) interactions. Thus, with the adoption of the Online Access Law the German government takes action towards increasing the availability of online services, exploring the online potential of public administrations and ultimately improving country's performance on the front-office digitization.

Furthermore, the OZG is providing a basis for linking service portals of different administrative levels together. The administrative portals, providing interfaces to online administrative services, will be connected in an integrated portal network (Portalverbund), which lays the national ground for the creation of the EU-wide Single Digital Gateway (SDG) (Das Single Digital Gateway der Europäischen Union, n.d.). The Online Access Law is, thus, intended to provide the basis for building e-government services, based on EU- and Germany-wide reference architectures, principles and governance models. One of such principles that government e-services are expected to be built upon is the Once-only principle (OOP), which has been formulated by the European Commission in the eGovernment Action Plan 2016-2020 (Stocksmeier et al., 2019). The implementation of the **Once-only principle**, or the **non-recurrent sharing of personal data and information by citizens and its reuse by government authorities**, has been part of the administrative agenda in Germany for several years, as it promises advantages to implement truly seamless digital public services (Digitale Verwaltung und öffentliche IT, 2018). It embraces all channels of data exchange, including those between different administrative bodies (G2G), as well as those in communication with businesses (G2B) and citizens (G2C). Aligned with previous projects on building digital administrative services solutions and being applied to existing authentication methods, the Once-only principle could, therefore, facilitate data collection and sharing (Krimmer et al., 2017b) and boost Germany's performance in the digitization of back-office.

Unlike dealing with digitization, when it comes to penetration and increasing the number of citizens, engaging with digital administrations, it is vital to focus on the government-to-citizen context (Akkaya & Krcmar, 2018). According to research, conducted by Akkaya & Krcmar (2018), who have been studying concerns of citizens regarding the introduction of eGovernment in the DACH region (Germany, Austria and Switzerland), one of the most important challenges posed to the digitalization of public services is related to privacy and data protection. These concerns are growing even more in the context of enabling cross-border services, which directly impacts the implementation of the Once-only principle (Akkaya & Krcmar, 2018).

While Germany is considered to be highly advanced in ensuring the respect for privacy of its citizens and was the first country to define data protection in the sense of "information self-determination" in its regulatory landscape, privacy concerns are still viewed as an obstacle to digital service provision (Cavoukian, 2011). German Data Protection Commissioner in 2003-2013 has seen an effective way of overcoming these obstacles in "developing clever technical solutions, incorporating them into systems and examining very early in the planning process whether and how to limit the amount of personal data to the absolute minimum necessary" (Cavoukian, 2011, p. 6). Besides, a recent communication from the German Data Protection Committee has been calling upon fulfilling the provisions of the Online Access Law on the national, state and municipal levels with greater respect for "Privacy by default and by design", which also focus on data minimization (DSK, 2017, p. 761).

Although not meant to solely tackle difficulties, remaining on the road towards fully functional eGovernment, the Privacy by design principle has been finding its application in European eGovernment projects, as prescribed by the EU General Data Protection Regulation (GDPR). These include several projects in the German context, where the respect for personal data has been entrenched into information systems from the design stage through the application of the blockchain technology in digital public services (Sichere Lösung für Bürgerkonten nach dem Once only-Prinzip, 2018).

Especially vital the issues of use and exchange of sensitive identity-related data become against the background of delivering seamless eGovernment services, such as One-stop government and No-stop government portals and services. Just like in the supply chain management in the private sector, One-stop government portals require great coordination and cooperation efforts, which in their turn need to consider legal provision data protection laws as well (Otjacques et al., 2007). Therefore, while considering OOP and Privacy by design implementation, public sector organizations should take into account both organizational and cooperation processes among each other, which puts the

problem of implementing OOP and PbD into the category of principles' alignment, discussed in the following section.

2.1 Challenges of OOP and PbD in the European and German Perspectives.

All in all, the regulatory and policy actions of the German government are recently targeting a robust buildup of the public e-services based on digitizing G2G, G2B, and G2C communication and transaction channels. These actions aim to embrace the EU-wide initiatives on cross-border eGovernment services and the existing regulatory landscape and technical infrastructure on the national level, which includes, but is by no means limited to the Once-only and Privacy by design principles. Mainly, the Online Access Law's implementation until 2022 aims at embracing the notion of Single Digital Gateway in connecting federal, state, and municipal service portals, while safeguarding security and privacy of personal data:

"In order to enable the lawful … exchange of evidence and information by means of the Union-wide application of the 'once-only' principle, the application of this Regulation and the 'once-only' principle should comply with all applicable data protection rules, including the principle of data minimization, accuracy, storage limitation, integrity and confidentiality, necessity, proportionality and purpose limitation. Its implementation should also comply fully with the principles of security by design and of privacy by design, and should also respect the fundamental rights of individuals, including those related to fairness and transparency" (Council Regulation (EU) 2018/1724, 2018, p. 9).

Certain doubts, however, exist regarding the practical application of these two high-level eGovernment architecture principles, which results in unclear policy actions on the local level. The preliminary results of the MonLightGrid project in Monheim am Rhein in North-Rhine Westphalia, which is considered to be a frontrunner in digitizing municipal services in the state, provide a bright example of such lack of clarity. In Monheim further digitization of municipal services is held back by uncertainty regarding privacy compliance, and the project managers call upon a better understanding of the OOP-implementation with regard for Privacy by design in developing OOP-driven municipal services (Project MonLightGrid, 2019).

Although reference architectures regarding the implementation of the Single Digital Gateway have already been designed throughout the ISA^2 Program (European Interoperability Reference Architecture and the OOP Reference Architecture), their scope is highly focused on the cross-border availability of administrative services in the EU. Moreover, their regard for privacy concerns and the respective regulation is minimal and focused on the required efforts from the side of the private sector (Common architecture

for the Single Digital Gateway, 2017). Thus, these projects fail to explicitly address privacy concerns in the eGovernment implementation, as well as miss out on national specifics, both regulatory and technical, which puts limitations on their applicability in the national context.

Moreover, the issue of the OOP-enabled Single Digital Gateway implementation in line with Privacy by design remains mainly unaddressed by scientific research. Kalvet et al. (2018) point out three significant hindrances to the implementation of the Once-only principle, noted within the course of the TOOP project (Krimmer et al., 2017a). Firstly, "the implementation of the OOP needs to follow the principle of accountability, i.e., ensure all participants' awareness of their obligations and the right to restitution of damages caused by noncompliance" (Kalvet et al., 2018, p. 3). Secondly, "according to the principle of justice, the OOP solution must ensure the right to recourse for the persons relying on the OOP and include appropriate enforcement mechanisms" (Kalvet et al., 2018, p. 3). The authors conclude that it is the legal contradictions that are perceived to represent a danger to the Once-only sharing of citizen data, highlighting, in particular, the respect for underlying privacy regulation, which requires implementers to proceed with caution and establish corresponding safeguards (Kalvet et al., 2018).

This problem is pointed out by the researchers of the Fraunhofer Institute, who listed all advantages and disadvantages of the eGovernment service delivery based on the Once-only principle. The two major concerns listed are 1) the increased need for standardization and implementation of related interfaces for data exchange; 2) data protection related concerns (Fromm et al., 2015).

Similar concerns are raised by Akkaya & Krcmar (2018), who, in their study of the OOP-implementation in the DACH countries, highlight high privacy concerns in the German context. They indicate the need for further research on mitigating risks of rollbacks by addressing data protection regulation in the context of OOP-implementation (Akkaya & Krcmar, 2018). Digging deeper into the context of Germany, Schallbruch (2017) finds out in his research that "the majority of respondents would not be ready to save their government documents or private documents on a citizen portal, on which some government authorities would have access to. Although we have explicitly stated such an access would only be possible in case of an explicit consent of the person, the majority of respondents stated that they would not feel comfortable storing private documents on a citizen portal" (Schallbruch, 2017, p. 654). Schallbruch (2017) concludes in his research that single data protection measures (such as just receiving the citizen consent to access data) are not sufficient to ensure trust in eGovernment services, and more complex privacy considerations are needed to boost uptake.

Moreover, Martini & Wenzel (2017), who juxtapose the benefits of the Once-only and "only once", highlight the need for further studying and developing measures for accommodating the Once-only principle in the privacy-sensitive environment. More precisely, the authors are skeptical regarding the possibility of safeguarding privacy along the OOP-implementation and suggest introducing full procedural transparency of data usage by publishing protocols, or more radically - even completely manual steering of data use (Martini & Wenzel, 2017).

The problem, however, appears underexplored not only in the national contexts, where the implementation of the Once-only principle needs to be operationalized, but also in the cross-border services. Krimmer et al. (2017a) point out that personal data transfers need to be based on data protection principles, such as purpose specification, data minimization (which are an essential component of privacy by design), and data security, especially as far as sensitive data is concerned. Similarly, Cave et al. (2017) dedicate a whole chapter of their work to discussing the influence of GDPR on the implementation of the Once-only principle, highlighting the potential challenges the OOP-implementation will have to face with the introduction of the GDPR. The question of aligning the OOP implementation and PbD, nevertheless, remains unanswered by the authors.

Such doubts and privacy concerns from citizens might appear surprising, as research on privacy in both public and private sectors shows that online systems require "less data than their analog counterparts" (Gürses et al., 2011, p. 6). "Organizations may find that when they transpose some of their workflows to the digital realm, certain information is not needed" to deliver particular services (Gürses et al., 2011, p. 6). Such a phenomenon, also understood as "data minimization", is an element of privacy by design, which minimizes the exposure of personal data and can be enabled through minimized storage of private information. This phenomenon also reflects the essence of the Once-only principle and will be discussed in further detail later in this work.

As also highlighted in the EU-studies and policy documents (primarily, in the Tallinn Declaration, 2017), while the OOP-implementation contributes significantly to the reduction of administrative burden and saves time and financial resources of administrations and capabilities, enabled by re-use of data in public administrations, "it becomes important to remain focused on building and maintaining trust in government" (European Commission, 2019). European administrations need to demonstrate their appreciation for privacy, "allowing every citizen to be able to see who consulted and used their personal data, when, and for what purpose - and eventually allowing the user to authorize access to public entities" (European Commission, 2019).

To sum up, the relationship between the OOP-based SDG-implementation and addressing privacy concerns of citizens by implementing Privacy by design measures has been established in several practical applications and large-scale projects, as well as research. Enabling OOP is seen as essential for the implementation of the Single Digital Gateway regulation for cross-border EU services. It requires more thorough consideration of the principles of data protection, including the PbD principles. **Nevertheless, the simultaneous implementation of the OOP and the PbD is often seen as controversial. Moreover, their application to the national context, which is vital to ensure efficient cross-border administrative services remains unclear in several EU countries**. Germany's struggle to ensure trust in and greater usability of digital administrative services is only one of the examples.

Taking into account the identified research gap, the author of this thesis aims **to create an architectural blueprint of the data collection and data use processes in the federal One-stop government portal in Germany, based on the OZG-driven portal integration, to align and comply with the EU-wide Once-only and Privacy by design principles and regulatory requirements to implementing them.** The desired architectural blueprint will be a product of the requirements analysis of the German national and EU-wide regulation, related to digital government services, electronic identification, data exchange and reuse (the Once-only principle), as well as the Privacy by design. Its ultimate purpose is to guide the implementation of the local, state, and national service portals throughout the implementation of the Online Access Law.

While undertaking the goal of mapping legal requirements to an architectural blueprint of an OSG portal, the author would like to highlight two primary assumptions. Firstly, while the OSG development for the eGovernment service provision to citizens is not part of the current eGovernment policy planning, it is still considered to be prospectively addressed due to the growing interest in OOP-based eGovernment services (as indicated in Hunnius (2017); Digitale Verwaltung und öffentliche IT (2018)). As will be discussed further, while OSG implementation cannot be viewed as a requirement to implement the benefits of the Once-only principle, it is the only applicability context existing. Secondly, the author is highlighting the regulatory nature of both OOP and PbD while extracting legal requirements to enable process and information systems design. Nevertheless, the author does not highlight that the existing regulation sufficiently allows for their implementation. Therefore, further use of the architectural blueprint developed in this thesis is seen as a means to identify gaps in existing regulation, while realizing the two EU-level principles.

3 Research Design.

Having an ambitious goal of developing an architectural blueprint for translating and complying with the EU-wide requirement of enabling the OOP, as well as the data protection principle of Privacy by design, in setting up an OSG portal, this large-scale project requires a robust methodological framework. Although no published evidence of work in this domain has been found, this research relies on the research efforts in the area of information systems research. In this context, methodology has been defined as "a system of principles, practices, and procedures applied to a specific branch of knowledge", which allows information systems (IS) researchers to achieve valuable, rigorous and actionable results and conclusions (Hevner, 2007, p. 87).

Taking into account that this research project is aimed at producing an architectural blueprint, or an artifact, the author will be following methodological guidelines, set out by design science academia. Design science research (DSR) has been gaining acceptance among information systems scholars and is considered to be an established IS paradigm (Gregor & Hevner, 2013). It "involves the construction of a wide range of socio-technical artifacts such as decision support systems, modeling tools, governance strategies, methods for IS evaluation, and IS change interventions" (Gregor & Hevner, 2013, p. 337). The methodological principles, practices, and procedures are, thus, aimed at achieving research outcomes of a practical nature and include "conceptual principles to define what is meant by design science research, practice rules, and a process for carrying out and presenting the research" (Hevner, 2007, p. 87).

Nevertheless, being an evolving methodological framework, design science research has been covering academic work in two domains: design-theory research and practical design research (Gregor & Hevner, 2013). Design-theory research emphasizes developing design theories of various application domains. It assumes strong ties between artifact creation and theory development, with all the essential steps of artifact design (technology invention, technology evaluation and problem identification) being part of the theory building process and ultimately contributing to theory development (Kuechler & Vaishnavi, 2008). As explained by Gregor & Hevner (2013), the contributions of this type of research comprise 1) well-developed design theories about embedded phenomena, 2) nascent design theories, which produce knowledge on operational principles and architectures as well as 3) artifact implementation principles and practice. Kuechler & Vaishnavi (2008) further argue that design theory research produces contributions of explanatory and prescriptive nature, which cover the gap between the developed artifact and the application domain. Therefore, theoretical research within the design theory field

works with existing artifacts and advances the academic understanding of their applicability.

The second domain, identified by Gregor & Hevner (2013), deals with practical artifact design. In the course of scientific projects of this nature, socio-technical artifacts, such as 1) instantiations (software products and applied processes), 2) constructs, models, design principles and technological rules, as well as 3) mid-range theories are developed as an academic contribution. This thesis is situated within the second domain, as it aims at producing an artifact of mid-level abstraction (architectural blueprint as a model), which is why further development of the methodological framework will focus on principles, practices, and procedures, relevant for artifact development.

To begin with, the design science research methodology for developing an artifact comprises a set of principles that encompass high-quality research standards. According to Hevner et al. (2004), the central principle is the development of an artifact itself. Furthermore, a design science research project should aim at creating an artifact in a way that helps to address a "heretofore unsolved and important problem", that produces an outcome of high "utility, quality, and efficacy" (Hevner et al., 2004, p. 94). At the same time, the development process should draw upon existing research and knowledge, and the outcomes must be verifiable and communicated appropriately (Pfeffers et al., 2007). These principles are central to this thesis, as the author addresses a vital, unsolved issue in the eGovernment field, produces an artifact of broad application scale (justified by its abstraction level), while relying heavily on research contributions of academics, working with OSG, OOP and PbD issues and transparently outlining research steps.

Moreover, according to Gregor & Hevner (2013), being an outcome of a design science research, an artifact is a "thing that has, or can be transformed into, a material existence as an artificially made object (e.g., model, instantiation) or process (e.g., method, software)" (Gregor & Hevner, 2013, p. 341). In their work the researchers have identified four types of possible artifacts developed in a design science research study, depending on the application domain maturity and the solution maturity: an improvement, an invention, an exaptation, and a routine design. An improvement refers to a solution, which has been newly developed to solve a well-known problem. An invention solves a newly identified problem with a new solution. An exaptation in its turn contributes to design science research field by expanding a well-known solution to a new application domain, which has not been addressed previously. Finally, a routine design is understood as an applied known solution to a known problem and has a minimal impact on solving the issue (Gregor & Hevner, 2013). Although vague in its conceptualization, the issue addressed in this thesis is well known. At the same time, the solution has not been

developed yet, and, therefore, the architectural blueprint developed in this thesis should be viewed as an improvement.

According to the study of Gregor & Hevner (2013), conducted through a review of a variety of design science research papers a design science research project aimed at creating an improvement often produces models and guidelines as an artifact. In case of this thesis, the author aims at creating an architectural blueprint, which is intended to serve both as a reference model and as a guideline for the decision-makers in the area of legislation, as well as process and IS reengineering. Additionally, Gregor & Hevner (2013) highlight that artifact development with the aim of addressing a known problem and producing a new solution to it should be heavily reliant on previous research conducted on the issue. This work will, therefore, be integrating an extended literature review section, which will view contributions on One-stop government, Once-only principle and Privacy by design works in greater detail.

Furthermore, depending on the type of artifact, developed within the research project, different research procedures are being applied in the artifact development. On the one hand, Baskerville et al. (2009) suggest that the design science research should be based on four activities: (1) Search, (2) Ex Ante Evaluation, (3) Construction, and (4) Ex Post Evaluation. In such design science research much emphasis is put on evaluation. Ex-ante evaluation takes place before the design decision and serves primarily the purpose of assessing cost-benefit parameters in technology development and application. In its turn ex-post evaluation should assess organizational change and adaptation of the technology (Pries-Heje et al., 2008). These considerations on evaluation in design science research clearly show that the artifact development is understood as 1) development of an instantiation, which is to be applied in a 2) particular organizational context. Since this is not the case, which this thesis is preoccupied with, such research design appears rather inappropriate for the purpose of this study.

Another procedure has been proposed by Pfeffers et al. (2007) and is, according to Gregor & Hevner (2013), a widely accepted research guideline, also known as the design science research cycle. The design science research cycle consists of (1) Problem identification and motivation; (2) Defining objectives for the solution; (3) Design and development; (4) Demonstration; (5) Evaluation; (6) Communication. Firstly, problem identification and motivation step's primary objective is to define the research problem and provide justification for the solution in question. At this step, the researcher needs to clearly communicate the problem, which would motivate them, together with the audience to seek the solution, and is, therefore, based on a profound understanding of the issue (Pfeffers et al., 2007). Secondly, (2) Defining objectives for the solution serves as a step,

conceptualizing the requirements for the developed solution to proceed with its evaluation. This step is of a rather theoretical nature and is expected to be built upon the academic literature of the knowledge field concerned. Thirdly, (3) Design and development step deals with the artifact creation itself. This step includes identifying the artifact's desired functionality and then developing the actual artifact. After the artifact creation, a design science research should proceed with (4) Demonstration, which shows, how the artifact can be applied in practice. The demonstration step can be carried out using the methods of experimentation, scenario development, or case study. A design science research project then proceeds with the (5) Evaluation step. Evaluating the artifact means creating indicators and criteria to assess its problem-solution fit and its utility and robustness and carrying out the evaluation itself. Finally, an essential step in design science research is (6) Communication, which presents the problem, its importance, and the solution developed within the research project (Pfeffers et al., 2007).

In the context of the methodological framework for this scientific project, the author should highlight the episodic nature of the design science research, as opposed to the iterative design process (Baskerville et al. 2009). This means that each step of the design practice occurs in a non-linear manner and usually spreads across several research projects, taking place at different points in time. Such a remark is made at this point in order to highlight that a single thesis cannot include all of the six steps foreseen for a design science project, and the scope of this work must be delineated.

In this thesis (1) Problem identification and motivation have already been presented in previous sections. The solution motivation will follow in the coming chapter, which presents the As-Is eGovernment infrastructure in Germany and demonstrates its relation to the EU objectives. As far as (2) Defining objectives for the solution is concerned, the author will proceed with this step in the literature review section to capture the precise meaning of the OOP and the PbD principle. These requirements will be furthermore presented as they appear in the EU and national regulation in Germany in order to frame further development of the artifact and delineate the set of regulatory documents addressed. While (3) Designing and developing the artifact in this work, the author will outline the desired functionality of the artifact based on the literature review and first review of the relevant regulation. Primarily, this substep should deal with identifying, which levels of the solution architecture will be included in the scope. Furthermore, the author will proceed with carrying out the artifact design. (4) Artifact demonstration will be included in the section, following artifact design and development in order to present the application of the solution in particular environments. Since the artifact application is not observed, or even planned in any of the German administrative contexts at this point, the author will use the method of scenarios, when it comes to step (4) (Hevner et al.,

2004). With respect to step (5) Evaluation the author will touch upon several aspects of the evaluation process in the discussion section. A full-scale evaluation is not included in this thesis's scope due to the uncertainty of extracting all necessary information from the legislation and potential need to provide recommendations on enriching the regulation related to OOP or PbD. Finally, this whole thesis is expected to serve as a (6) Communication of the identified problem and its potential solution.

Architectural Blueprint as an Artifact. As mentioned previously, the artifact, which is to result from this thesis, is one of an "improvement" type and will be developed in the form of an architectural blueprint. Although being related to artifact types "models", it still remains explored only in a limited way. Therefore, the author sees the need to elaborate on the nature of the "architectural blueprint" as an artifact and point out its key features. For this purpose, this subsection will review research contributions, where an architectural blueprint has been developed.

To begin with, according to Cleven et al. (2009), models in the context of design science research should be understood as a particular abstraction of reality, in which relations between different elements are identified and explained. As artifacts in design science research, models can have various foci: technical, organizational, or strategic, or cover all of the aspects (Cleven et al., 2009). Often researchers opt out for the development of conceptual models of information systems, which stress "the core terms or concepts which characterize an application domain while neglecting technical aspects that are related to the implementation of corresponding software systems" (Frank, 2007, p. 119). This understanding of a conceptual model is also reflected in previous research, where an architectural blueprint was selected as an artifact.

Coming from the field of architecture, an architectural blueprint, according to Scarduzio et al. (2011), refers to a set of principles for design. Nevertheless, it has also been applied in IS research, referring to IS architecture. Computing (2006) has created an architectural blueprint of autonomic computing, which integrates architectures and standards for IS development. Similarly, Gasmelseid (2006) has created an architectural blueprint of multiagent web-based decision support systems for global enterprises. Gluhak et al. (2011) have also developed an architectural blueprint of the real-world internet, which captures the main features of the respective information systems. These research projects have been working primarily with the development of IS architectures, which, unlike reference architecture, have a higher degree of abstraction from particular entities, but do have a well-defined context (e.g., global enterprises). According to Tepandi et al. (2019), an architectural blueprint is a broader definition for reference architectures, which can include one or a set of solution architectures.

However, architectural blueprints, developed by previous researchers, do not only deal with IS architectures. Kolain & Wirth (2018) have created an architectural blueprint of a process of personal data handling with regard to GDPR's Privacy by Design principle, which represents key entities and their relations in data handling procedures. Similarly, Brückmann & Gruhn (2010) have "developed an architectural blueprint that supports a consistent model-driven development process of business logic for information systems" (Brückmann & Gruhn, 2010, p. 53).

For this reason, an architectural blueprint shall not be understood as reflecting only information systems architectures. Simultaneously, previous research efforts show that an architectural blueprint does not cover all modeling aspects equally extensively. It rather focuses on one of the aspects: organizational, technical, or strategic, while depicting the necessary components and interfaces, connecting the focus-domain to others.

Thus, an architectural blueprint is understood in this work as a special type of a model that encompasses organizational, strategic, and technical aspects of a developed solution, focusing on one of the application domains. While it does not solely refer to an information systems architecture, it includes processes and entities involved in a particular activity in a certain application domain. To avoid confusion, the following two features of an architectural blueprint will be understood is crucial in this work: 1) universality of application for the delineated application scope (e.g., in this thesis - all types and fields of administrative procedures on different levels in Germany), 2) focused on one of the layers of an entity architecture, but not limited to just one layer. The appropriate focus of the architectural blueprint in this work will be defined in subsequent chapters.

Legal Specification Method. Finally, while the research process of the current design science project has been described in great detail, the author still sees the need to specify, which methods of data collection and processing will be used beyond the literature review, in particular in the section devoted to (3) Design and development. The focus of the solution has been determined to address the legal requirements on the national German and the European Union levels, related to the OOP and the PbD. Thus, similar to Kolain & Wirth (2018), who have also been developing an architectural blueprint and have been working with the PbD compliance, the author has opted for the legal specification method.

Although the legal specification method is often used by practitioners, rather than researchers (e.g., by Federal Information Management redactors, who model FIM Processes building block (Föderales Informationsmanagement, 2017), its definition and precise guidelines can still be found in the literature. Its application can have several

motivations, according to Otto & Anton (2007), which are entrenched in the nature of the legislation. “There are certain characteristics of regulations that make them both useful and difficult to apply to design methodologies. Regulations tend to be very structured and hierarchical documents… Some areas of law undergo constant changes, whereas other areas are relatively stable. In addition, amendments and revisions to the same piece of regulation can lead to internal contradictions… Another important characteristic of regulations is the frequent references to other sections within a given legal text and even to other pieces of law” (Otto & Anton, 2007, p. 6). Although having mostly worked with the regulatory context in the United Stated, which is significantly different from that in the European Union countries, Otto & Anton (2007) have pointed out regulatory features, which have made it difficult for software engineers to model regulatory requirements, relevant also in the European countries.

Based on interviews with practitioners, Otto & Anton (2007) have developed the following guidelines to deal with the legislation in software engineering practice. To begin with, it is vital for practitioners to identify relevant regulations, which is significant to each requirement. The authors suggest using reference literature and cross-references in the regulation itself, which will also be performed in this thesis. Furthermore, Otto & Anton (2007) suggest classifying regulation according to various parameters, appropriate for the design. In this thesis the author will perform the classification based on requirements stipulated, which will be identified in the literature review. Finally, the researchers highlight the importance of prioritizing regulation for better identifying, which requirements override or are of higher legal power than the others. Since this consideration is relevant to the European regulation only to a limited extent, the author will address the prioritization only briefly. While the researchers have suggested further guidelines in extracting requirements from the regulation, the author will not describe them in further detail, as they deal with continuous monitoring of legal changes (Otto & Anton, 2007), which are not relevant for this thesis at this point in time.

As stated by Kolain & Wirth (2018), the legal specification method is a promising tool, which is part of “methodology for translating legal requirements into technical guidelines: architectural blueprints designed using legal requirements. The purpose of these blueprints is to show developers how their solutions might comply with” the regulatory principles. While not finding wide application in research, this method would indeed help to fulfill the purpose of defining compliance with regulatory requirements in eGovernment design.

The compliance operationalization should, however, be combined with the right tool to create an architectural blueprint. This work will be relying on enterprise architecture

concepts and models, using Archimate, which are considered suitable for 1) representing the layered view of an administrative system and 2) translating high-level requirements into operational processes and infrastructures (Jonkers et al., 2006). Enterprise architecture methodology and in particular, Archimate, are also seen as beneficial to the artifact created in this thesis due to its high potential to be utilized as a reference architecture in the future (Tepandi et al., 2019). These reasons form a basis for the tool selection, applied in this work.

In sum, this thesis is following the steps of the Pfeffers et al. (2007) design science cycle to develop an architectural blueprint as an artifact to address the issue of alignment and compliance with the OOP and the PbD in eGovernment projects of the national scale in Germany. To define the prospects of alignment in further detail, the author extracts the requirements to fulfilling the two principles from the literature and classifies the existing regulation according to these sets of requirements. The author utilizes the legal specification method to map the regulatory requirements of the OOP and the PbD and, using the specification of Archimate, creates an architectural blueprint of the German administrative digital services, compliant with the OOP and the PbD.

4 Solution Motivation.

The environment, in which German eGovernment is evolving, is highly complex. Apart from ambitious goals set by the federal government to advance digital administrative services on the federal, state and municipal levels, the eGovernment build-up efforts need to keep up with no less ambitious projects of the European Commission and other EU member states, constantly advancing in this field. Grasping this complexity for this study is essential to motivate the need for an architectural blueprint, paving a way towards compliance with the Once-only and the Privacy by design principles. This section will, therefore, be devoted to outlining existing policy actions in the EU and German national contexts, providing an overview of the existing eGovernment infrastructure components.

4.1 eGovernment Regulation on the EU Level.

To begin with, advancing eGovernment in the EU is part of the European Commission's broader strategy of creating the Digital Single Market. Central to this effort is the EU Digital Single Market strategy, introduced in 2015. The EU Digital Single Market strategy is built on three pillars: 1) ensuring better access to digital products and services, offered across the EU for citizens and businesses located within the borders of the union, 2) developing high-speed, secure infrastructures, providing accurate and unified information and supporting this exchange through digital channels, further innovation and fair competition by introducing proper regulation; 3) ICT research and innovation to assure competitiveness of the economy (European Commission, 2015). eGovernment services play an essential role in bringing this strategy into life, which requires standardization and interoperability of offered solutions. "eGovernment services that are being developed in different Member States should be able to communicate with each other and not develop in isolation" (European Commission, 2015). In this respect, the European Commission undertakes the initiative of defining the standardization plan and prioritizing areas, which are essential in the Digital Single Market context.

Although the development of particular electronic administrative services has not been indicated as a Commission's priority in the strategic document, the European Commission has been working on the issue. It has consequently adopted the eGovernment Action Plan 2016-2020. "The vision is to have public administrations in the union … providing digital services that are borderless and user-friendly. Opening the services between public administrations to work within and across borders is expected to increase efficiency and help the free movement of citizens and businesses" (Rinne, 2019, p. 37). To achieve greater cross-border possibilities and user-friendliness, the eGovernment Action Plan 2016-2020 outlines the following policy actions:

"1) Modernizing public administrations using key digital enablers (for example technical building blocks like CEF DSIs like eID, eSignature, eDelivery, etc.);

2) Enabling mobility of citizens and businesses by cross-border interoperability;

3) Facilitating digital interaction between administrations and citizens/businesses for high-quality public services" (European Commission, 2016a).

In fulfilling its role of the driver of the listed policy actions, the European Commission suggests the following principles, for which it expects high degree of commitment from the member states: 1) Digital by default, suggesting that public administrations should give preference to digital public services in the first place; 2) the Once-only principle; 3) Inclusiveness and accessibility, implying that digital public services should be available to citizens of various levels of technology savviness and access to the internet; 4) Openness and transparency, referring to cooperative and at the same time data protection aware use of citizen data; 5) Cross-border by default, expecting administrations to avoid further fragmentation and strive to provide access to citizens of other EU member states; 6) Interoperability by default, encouraging seamless and silo-free digital service provision in the member states; 7) Trustworthiness and security, highlighting the importance of privacy and IT-security regulations and best practices. One of the actions, suggested by the Commission, to achieve the highlighted goals and to enact these principles is to introduce the EU-wide Single Digital Gateway (SDG). The Single Digital Gateway is "based on existing portals, contact points and networks, expanding, improving and streamlining all information, assistance and problem solving services needed to operate efficiently across borders, and enabling users to complete the most frequently used national procedures fully online" (European Commission, 2016).

In this context, the Single Digital Gateway is thought of as a means to fix the "discrepancies in the availability of online information and procedures. There is a lack of quality in relation to the services and a lack of awareness regarding that information and those assistance and problem-solving services. Cross-border users also experience problems finding and accessing those services" (Council Regulation (EU) 2018/1724, 2018, p. 3). While the Commission has taken previous attempts to address these issues, such as "single points of contact, product contact points and construction products contact points, professional qualifications assistance centers, and consumer centers", these efforts have had a sectoral character. "Under the Services Directive, the points of single contact (PSC) were supposed to be established by the Member States by 2009 and were meant to cut red tape and to modernize national administrations. However, the implementation levels were not convincing" (Scheinert, 2018, p. 3). Single Digital Gateway policy action and regulation (the regulation will be discussed in further detail below) have been

introduced to overcome this situation, serving as a single-entry point to receive information, assistance and fulfill administrative procedures online (Council Regulation (EU) 2018/1724, 2018).

While the Single Digital Gateway is thought of as an EU-level OSG portal for most frequently used digital administrative services, it should by no means be understood as a back-office integration of EU public services, but rather as an interface between citizens or businesses and administrations. Nevertheless, some level of interoperability, as well as integrated information management within member states, is essential. It includes the authentication services for EU citizens and businesses, as well as document exchange between authorities of different levels (Rinne, 2019).

Apart from being dedicated a separate regulation, which will be discussed in the Chapter The Artifact for Aligning the OOP and the PbD Requirements., the creation of the EU-wide Single Digital Gateway is supported through the regulatory framework of the Electronic Identification, Authentication and Trust Services (eIDAS) regulation and closely connected to the regulatory actions in developing the e-Justice Portal and the Business Registers Interconnection System (BRIS). All of them have majorly a cross-border cooperation relevance. The eIDAS regulation addresses the issue of citizens not being able to use "their electronic identification to authenticate themselves in another Member State because the national electronic identification schemes are not recognized in the other Member States" (Cuijpers & Schroers, 2014, p. 30). It establishes the legal requirement for recognition of electronic identification means of cross-border EU-nationals and ensures, therefore, citizen empowerment across the European Union in using digital government services. Being the first concrete implementation of a one-stop government portal, e-Justice Portal serves as an example for future action and cooperation in the light of SDG (Home, n.d.). As far as the BRIS Regulation (EU 2015/884) is concerned - it establishes "standards and the architecture of the EU-wide system of interconnected registries on EU-registered companies" and serves as an exemplary measure to establishing the OOP-critical integrated base registries infrastructure (Council Regulation (EU) 2015/884, 2015).

Finally, the European Commission's effort towards creating the Single Digital Gateway is being underpinned through the corresponding Programs - the CEF Program and the ISA^2 Program. Connecting Europe Facility (CEF) is a funding instrument of the European Commission to facilitate innovation in the areas of transportation, energy, and telecom through "innovative financial support instruments, such as guarantees and project bonds" (Connecting Europe Facility, n.d.). Its main goal is to offer readily available online tools that help to tackle cross-border challenges. Apart from project investment, CEF offers

open-source building blocks for smart government and smart city development, such as eID (identification), eDelivery (electronic data and document exchange among administrations), eSignature (electronic signing of documents for end-to-end digital processes), eInvoicing, eTranslation, eArchiving, as well as Big Data Test Infrastructure and Context Broker, which have been added to the solution portfolio in 2018 (CEF Building Blocks presented at Releasing the Power of Procurement, 2019). In the context of the OOP, in particular eID, eDelivery and eSignature are believed to be the most crucial elements of the data collection and data exchange processes. "The Once Only Principle (OOP) is undergoing a preparatory action within CEF. The various work packages will define if this should be considered as a Building Block or as a service of an existing Building Block" (Once Only Principle reduce the administrative burden for individuals and businesses, n.d.).

The Interoperability Solutions for Public Administrations, Citizens and Businesses successor Program (or ISA^2, running as a successor program of the ISA in 2016-2020) is tasked with the creation of "digital interoperability solutions or components that can be used in public administrations in the EU" (Rinne, 2019). Its goal is, therefore, to create interoperability standards for cross-border EU public services. One of the solutions offered in the context of the SDG-implementation is the European Interoperability Reference Architecture (EIRA). "The EIRA is a four-view reference architecture for delivering interoperable digital public services across borders and sectors. It defines the required capabilities for promoting interoperability as a set of Architecture Building Blocks" (European Interoperability Reference Architecture (EIRA) v3.0.0, 2020, p. 11). The goal of EIRA is to encourage the reuse of already existing interoperability solutions and help public administrations keep costs down when creating eGovernment systems (Rinne, 2019).

All in all, the European Commission has been steering the enabling of cross-border eGovernment solutions by promoting building blocks, such as concepts, documentation and processes, reference architectures, and open-source tools, as well as suitable regulatory framework and data use principles. The EU member states are expected to comply with this policy action and enable its key requirements by 2023. However, the progress towards creating One-stop government portals as a starting point for the cross-border Single Digital Gateway has not been equally progressive in all member states. Moreover, since the member states have very different starting points, as far as the public IT infrastructure is concerned, their commitment to the OSG development might not result in the desired outcomes. Since this thesis is focused on Germany, the following subsection will discover the underlying eGovernment policies and created infrastructure to understand what is already in place as a basis for the One-stop government portal.

4.2 eGovernment Initiatives on the National Level in Germany.

Although several initiatives in the German digital public administrations agenda have been undertaken to boost the country's public e-services offer, most of them had a general character, aimed at increasing the availability of online access to public administrations. Bund Online (2000-2005) has set a goal of bringing 400 services online. It "introduced a central management system for establishing methods and basic components to exchange experiences, including a content-management-system, a virtual post office, an ePayment-Platform, a form-management-system and the portal Bund.de" (Räckers, 2019a).

Recognizing the results of the first eGovernment initiative (Bund Online) and realizing at the same time the level of fragmentation of administrative processes that emerged, the Federal Government has proposed a new strategic initiative in 2003 - Deutschland Online. The policy action was expected to "provide a framework for cooperation between all administration layers" (Siegfried, 2006, p. 122). It has set the following priorities: 1) integrating cross-level administrative services and offering them online, 2) ensuring interoperability and connected online eGovernment service portals; 3) developing common IT-infrastructures to facilitate data exchange; 4) developing common standards for eGovernment services, and 5) exchanging eGovernment solutions among different administrative entities (Siegfried, 2006). Its results have not been highly recognized, and it was followed by another initiative.

The initiative eGovernment 2.0 (2006 - 2010) has brought further fragmentation to IT-investment and operation on the 3 levels of governance (Räckers, 2019a). Having the goals of further extending the eGovernment services supply, aligning efforts with the economy, promoting eID and safe communication infrastructures, the initiative has shifted focus towards the eGovernment build-up on the federal level, but has overlooked the need for cooperation with the states and the municipalities (Räckers, 2019a).

The role of the National eGovernment Strategy (NEGS) was to address the emerged fragmentation. The strategic document is addressing challenges of internet access and service availability, standardization and integration into the EU eGovernment context, providing the basis for legal, organizational, and technical modernization, ensuring investment and developing agile and flexible public administrations (Mkude & Wimmer, 2014). It is intended to achieve "1) secure and barrier-free access to online-service and user-oriented services; 2) efficient and effective administrative services through elimination of bureaucracy and cooperation between all levels of governance; 3) data protection and information security; 4) transparency and citizen participation" within the framework of vertical and horizontal cooperation among public authorities (Ziele der Nationalen E-Government Strategie, n.d.). The context of this strategy is still relevant to

the eGovernment development in Germany, and NEGS is still viewed as a significant policy document.

Following the adoption of NEGS, the federal government has brought the Digital Administration 2020 into life, which is primarily intended to create the necessary environment for the implementation of the E-Government Regulation 2013 (EGovG). The Digital Administration 2020 Policy emphasizes the aspects of information and knowledge management and bridging the gap in eGovernment development, which originates from the federalist structure. It focuses on 1) norm-screening and replacement of norms and procedures that stand on the way of digitalizing administration; 2) ensuring barrier-free setting of e-government by offering building blocks for digital administration solutions; 3) unifying description of processes, services, and unitary forms; 4) integrating existing solutions (such as eID and De-Mail) in administrative processes and services; 5) establishing a form-management system; 6) integrating secure ePayment and payment platform; 7) supporting electronic file management (e-Akte), as well as 8) process optimization of federal administration. In bridging the gap in eGovernment development on the regional and municipal scales, the Digital Administration 2020 foresees supporting activities of IT Planning Council in creating framework conditions for federal cooperation; further standardization and promoting electronic access and eGovernment services; ensuring navigability of eGovernment solutions for users (by means of a single point of contact, or EA 2.0). Thus, building on existing eGovernment infrastructure, the strategy is expected to reshape and coordinate the eGovernment landscape to simplify access for users and to enable further integration with the EU-wide initiatives (PG Digitale Verwaltung, 2014).

All in all, as follows from this brief overview of the German federal government's strategic actions, it is not easy to view the eGovernment development on the national scale in the cross-border by default context of the European Union. Numerous initiatives in single municipalities and states to digitalize administrative services are not enough to easily inscribe Germany into the Single Digital Gateway action of the EU. Moreover, the situation becomes even more complicated when one considers already existing eGovernment solutions that have been constantly promoted.

Although put together, these initiatives do form the basis for the creation of a One-stop government portal and its subsequent integration into the EU Single Digital Gateway, there is still a tremendous amount of work lying ahead. The following subsections will be dedicated to outlining the basic eGovernment projects and infrastructures in Germany, related to the SDG Regulation.

Single Point of Contact. Although this component of the OSG is not offered through a digital interface in Germany, it does exist in the form of a phone number. By calling 115, a citizen could reach a government of any level to receive information about provided services. “The phone call triggers a search for information about services from a database, containing standardized information on frequent requests” (Geschäfts- und Koordinierungsstelle 115, 2019). The contact is available Monday through Friday and could be assessed as successful - 65% of requests are answered in the first call, and in case they cannot be responded to - they are forwarded to the customer service to be responded to within 24 hours. The information is gathered only about most frequent requests.

Since 2009 there have been multiple (both on different levels and in different points in time) efforts dedicated to establishing a digital Single Point of Contact (in germ. Einheitlicher Ansprechpartner) to implement the EU Single Point of Contact Directive (amended through the SDG Regulation). The project has reached quite an advanced stage in several states. In the state of North-Rhine Westphalia, for instance, the portal was centralized in 2016. “However, due to an unsuccessful attempt to integrate legacy IT-infrastructure, the portal could not offer assistance to intended users until today and serves as a navigator tool to find the responsible authority in a very limited spectrum of services. Further integration and electronic service delivery face legal barriers and limited use of eSignature and related infrastructure (eID, De-Mail)” (Holz et al., 2018, p. 18).

The successor initiative EA 2.0, promoted by the IT Planning Council, was targeted at building an EA-network across all levels of administration to implement the One-stop government. It was expected to be built upon the existing contact infrastructure (primarily related to G2B services). As of 2019, the project has been suspended and integrated into the implementation of an integrated portal network (Portalverbund) (Bundesministerium für Wirtschaft und Energie, n.d.).

Secure Communication and User Authentication. The first project, initiated in this area, and brought into life is the De-Mail - secure information exchange infrastructure, used inside the administrative bodies, as well as by businesses and a private individual to carry out secure message and document exchange and serving as e-evidence. Becoming a service provider of De-Mail requires adhering to strict certification rules and guaranteeing end-to-end encryption of electronic communication (De-Mail in der Bundesverwaltung: Empfehlungen des BfDI, 2013). This and other requirements are outlined in the De-Mail Act of 2011. Through the De-Mail Act, “an admission procedure for De-Mail providers was established, with which compliance with these minimum requirements is checked using uniform rules (“accreditation”). All De-Mail providers are

checked according to uniform criteria in a transparent procedure. It is a prerequisite for building trust in the security and quality of De-Mail services" (Häufig Nachgefragt De-Mail, n.d.). These criteria are grouped into categories, dealing with such processes as account opening and management of a De-Mail account; mailbox and shipping; identity verification; directory; document filing; ensuring rights of the data subject; data protection management (De-Mail-Kriterienkatalog für den Datenschutz-Nachweis, n.d.).

The most crucial eGovernment infrastructure, relevant to the creation of the One-stop government and the implementation of OOP, is service accounts. By means of service accounts, citizens "get personalized access to their government portals" (Schallbruch, 2017). Setting up a service account requires identification through the eID function of the new ID card (Krimmer et al., 2017b). In this case, the account is considered to maintain the highest security level and, therefore, "personal information and documents could be saved on the e-government portal" (Schallbruch, 2017, p. 652). The service account can be set up without the mechanism of two-factor identification as well, using regular email or De-Mail. However, the functionality of the portal decreases in this case (Krimmer et al., 2017b). Additionally, the OZG highlights that service accounts would serve as a central authentication solution. Nevertheless, it remains unclear which level of identification would be required in the future (Stocksmeier et al., 2019).

The use of service accounts is inevitably connected with the use of service portals. The overall landscape of service portals in Germany is highly decentralized, as by means of a service portal, each state and municipality offer eGovernment service to citizens and businesses (Schallbruch, 2017). Their primary information and transaction functionality should be complemented by the Administration search (Behördenfinder) and description of services (Diensteverzeichnis), which are vital to ensure the usability of this infrastructure (Riedel, 2019). The connection of these single portals into an integrated portal network is planned for pragmatic reasons: to build up on the existing infrastructure and offer a search and redirection functionality. In itself, such a solution is inferior to an OSG portal, as it requires more considerable effort to convince users of its usability. However, its status as a step towards an OSG portal remains unclear (Nationaler Normenkontrollrat, 2019).

Finally, as far as German eGovernment infrastructure to secure user authentication is concerned, a new ID card has been introduced in 2010, which allows enabling an electronic ID function. As mentioned in relation to service accounts, eID represents an essential part of the service account infrastructure, since it ensures user identification in a secure and trustworthy manner (at least for public administrations). The eID function can be activated, with which electronic signing of legal documents can be performed, and

eGovernment portals can be accessed, using a card reading device (Räckers, 2019b). However, the use of eID's in Germany has been quite limited. For this reason, in autumn of 2013, the IT Planning Council adopted the "Strategy for eID and other trust services in eGovernment (eID Strategy)" and has prepared guidelines on the promotion of eID in states and municipalities. It still preserves its relevance in the site of OZG implementation (eID-Strategie, n.d.).

Interoperability and Standardization. Besides eGovernment projects, aimed at developing single components of the entire eGovernment infrastructure, the Federal Government has been undertaking policy actions, targeting the incompatibilities in digitalization efforts to enable the eGovernment system functionality. The efforts in the area of standardization have been relatively recent and are still undergoing constant changes. Nevertheless, the achieved results are being communicated to lower administrative levels in parallel.

The most prominent project in this area is the Federal Information Management. Since 2013 it aims at "creating a sustainable infrastructure at the technical-editorial and organizational level that includes information on administrative procedures (performance descriptions, form and process information). In cooperation with the LeiKa projects (Service Catalogue of the public administration; uniform directory of administrative services across all administrative levels) and the Federal Editorial Office, a common infrastructure is created within the public administration in order to reduce the editorial effort in describing information on administrative procedures with higher quality" (Föderales Informationsmanagement (FIM), n.d.). After the successful application of the project results in 2014-2015, it was developed into a further supporting infrastructure for the eGovernment development in Germany. "The Federal Information Management (FIM) serves to provide easily understandable information to citizens, uniform data fields for form systems, and standardized process specifications for administrative enforcement" (FIM Föderales Informationsmanagement, n.d.). This effort is, therefore, focused on 3 application areas, which are Services, Data Fields and Processes, which could help to understand, what are the standard procedures, which processes underly administrative services and what kind of information is required for the provision of public e-services (standardized forms). Primarily, FIM strives to achieve the goal of implementing the "one-for-all" principle[1] and decrease the effort of modeling legal language into the technical specifications. Moreover, FIM offers space for citizen participation in designing digital public services - Digitalization Labs for high-priority

[1] The "one-for-all" principle in German eGovernment projects refers to a possibility to develop various solutions from various administrative areas that can be re-used by other administrations without requiring tedious process and IT-development (Föderales Informationsmanagement (FIM) Infomationsveranstaltung, 2019).

services. The need for further data exchange standards and interfaces, as well as register interconnection, can be identified there (Föderales Informationsmanagement (FIM) Infomationsveranstaltung, 2019). In connection to the Once-only principle, special attention should be paid to the FIM-harmonization of data fields, as it allows to standardize application forms, required for citizens to apply for digital public service.

Another significant standardization effort to be highlighted in this context is KoSIT. “The task of KoSIT is to coordinate the development and operation of IT Standards for data exchange in public administration (XÖV – XML in public administrations). KoSIT supports the IT Planning Council in its task to adopt independent and interdisciplinary IT interoperability and IT security standards and to manage cross - federal eGovernment projects. The resulting range of tasks also includes the operation of the standardization agenda and the XÖV framework” (Startseite, n.d.). The standards, created under KoSIT, support the standardization efforts of FIM, in a way the XÖV-Framework includes data exchange standards for FIM-Data Fields (Föderales Informationsmanagement, 2019).

The need to catch-up on standardization and orchestrating architectural management in Germany is very high. It is still unclear that this is necessary and how this could be developed precisely. What is needed is an open discussion on how a standardization regime – embedded in a digital service standard for Germany – can be set up, and a service and integration platform can be introduced on a trial basis. According to the National Norm Controlling Council, such efforts as FIM and KoSIT are building a solid basis for standardizing services. They need to be further intensified in order to be beneficial to key public e-services stakeholders, in the first place, municipal administrations (Nationaler Normenkontrollrat, 2019).

To sum up, it is essential to point out that the eGovernment development efforts and the achieved results in Germany have not been primarily concerned with the EU cross-border perspective. It is easily explained by the fact that the administrative landscape in Germany is various, multi-level, and complex. Nevertheless, the Federal Government expresses its commitment to the EU-level eGovernment initiatives and continues to drive Germany’s integration into the supranational ecosystem by its current initiatives. Some of these initiatives have a regulatory character, such as the Online Access Law, which, when implemented, could serve as a milestone in the development of the One-stop government portal. This and other relevant regulations will be further discussed in the Chapter The Artifact for Aligning the OOP and the PbD Requirements.

While these efforts are essential to fulfill the German government's cross-border commitments, they are also crucial for the next steps of the eGovernment development in Germany. The administrative service provision is viewed as complicated by citizens and

businesses. They are not easy to use both off- and online. Whereas it is impossible to change the administrative structure, the Federal Government is looking for a solution to simplify the use of eGovernment services for citizens and businesses. Easy navigation and clear and consistent service description across municipalities, which is aimed at through the OZG and the standardization frameworks, are, therefore, crucial. The next step would be ensuring trust in digital services, their regard for privacy.

Thus, the problem identified through the review of the current eGovernment infrastructure is that of a structural character, which cannot be solved by changing the administrative structure. Single service account and service portal solutions are introduced in Germany on different levels of governance and often independently from each other, although with a certain degree of standardization. The navigation throughout different administrative levels is difficult for citizens, who are required to invest a lot of time in finding the responsible authority and its digital interface. To maintain transparency and usability of eGovernment solutions, this issue could be addressed by ensuring greater usability and trust, respectively, by the OOP and the PbD principles.

At the same time, implementing the Once-only and the Privacy by design principles is a pronounced commitment of the German Federal Government to the implementation of the SDG regulation, which is not as easy to operationalize in the federal system. Therefore, the main motivation of the architectural blueprint, developed in this thesis, is to highlight the legal requirements, which are to be fulfilled in further eGovernment development. Aligning the Once-only and the Privacy by design principles could, thus, bring the eGovernment in Germany one step closer to integrating it into the cross-border digital services, as well as address the needs of the potential national and EU-users. Additionally, eGovernment initiatives in Germany and the regulatory requirements, currently in place, cannot be ignored in the processes of the artifact development, and need to be reconciled with the EU legislation, related to the OOP and PbD.

Meanwhile, identifying relevant regulation both on the EU and the German national scale is not a matter of searching for keywords “Once-only principle” and “Privacy by design”. Both concepts have their own requirements to be fulfilled in order to be implemented and integrated in information systems and administrative process design. For this reason, the following chapter will review and operationalize the meaning of the two principles, as it exists in current research.

5 Requirements of the OOP and the PbD Principles.

This section deals with the theoretical underpinnings of the One-stop government, the Once-only and Privacy by design principles. The author will outline the existing research contributions on the three concept matters central to this thesis. Databases searched to identify main sources of these contributions are: WebOfScience, IEEE, JSTOR, GoogleScholar, ProQuest and Limo, where out of results produced by searching with key words ("one-stop government", "one-stop shop government", "one-stop shop portal government", "one-stop e-government", "once-only principle", "once-only principle e-government", "once-only e-government", "data re-use in e-government", "privacy by design"), following journals and conferences have been identified:

- IEEE conferences, Government Information Quarterly, Proceedings of the International Conference on e-Learning, e-Business, Enterprise Information Systems and e-Government for the One-stop government;
- the Proceedings of the International Conference on Digital Government Research and Digital Gipfel for the Once-only principle, as well as
- the Proceedings of the 12th International Conference on Availability, Reliability and Security, Computers, Privacy & Data Protection, International Conference on Privacy, Security, Risk and Trust and International Conference on Social Computing for Privacy by design.

The ultimate goal of gathering these contributions, as well as of the section as a whole, is to 1) define precise objectives for the architectural blueprint of the OSG portal in Germany, compliant with the OOP and the PbD principles; 2) provide a guideline to classifying regulatory requirements, which will serve as a basis for this work. As a result of this literature review, a framework, guiding further legal requirements collection and specification, is developed.

For this literature review, there is, however, a vital need to point out, what is understood by the concept "principle" in this work. Principles in the field of eGovernance are often viewed in the strategic context, which underlies eGovernment success: availability, user-centricity, and ease of use, privacy and security, innovativeness, and connectivity. Their primary goal is to complement the eGovernment objectives and to establish criteria to evaluate eGovernment projects (Heeks, 2005). Nevertheless, previous eGovernment research efforts did not explicitly tackle the nature of principles' application in this area of public administration: whether implementing principles should be mandatory and should be integrated into the regulatory landscape.

Within the Public Administration domain, principles are often understood as legally binding fundamental rules that need to be abided by in all types of procedures, connected to the exercise of power, such as constitutional principles of the separation of powers, the rule of law, or federalism. According to Jaeger (2002), constitutional principles are fundamental and have a generic nature, which means they need to be embraced in all kinds of government processes, including the development of eGovernment. These general principles are often entrenched in regulation and require compliance by all participants in the specific jurisdiction (Jaeger, 2002). Such a relationship between the application of principles and their regulatory essence is easily traced in the privacy regulation, in particular in case of the PbD principle, employing which is foreseen by the General Data Protection Regulation and the Federal Data Protection Regulation in Germany.

Often the Once-only principle application is also supported through the regulation. Thus, Belgium has passed a law on the OOP, which obliges public administrations to collect the same citizen data only once (Loi garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité et portant simplification et harmonisation des formulaires électroniques et papier, 2014). The OOP-based digital public services are also part of the Single Digital Gateway regulation, which foresees the cross-border administrative e-services to include once-only data collection. While similar national legislation has not been passed in Germany, the author would like to point out that in this work both OOP and PbD are viewed as fundamentally legal principles, which require compliance with. The further attributes of the OOP and the PbD are further discussed in the corresponding subsections.

To begin with, while Single Digital Gateway, as mentioned previously, is a specific policy action in the European cross-border public e-services, its underlying idea can be found both in public and private sector service design and both inside and outside the borders of the EU. One-stop government is often defined as “a single point of access to electronic services and information offered by different public authorities” (Wimmer, 2002, p. 92). It promises benefits to all players, providing and using digital public services. It is beneficial for citizens and businesses since the OSG reduces navigational efforts and allows requesting services more efficiently. For public bodies, an OSG portal increases the satisfaction of citizens and businesses with services and allows lowering transaction costs and achieving efficiency gains inside the public service provision.

In practice, however, the integration of services from different authorities and from different levels of governance and the consequent creation of a one-stop-shop portal that

serves as an interface to the user is rather a cost-consuming and complicated project. Academia has identified multiple issues connected to the development of a One-stop government portal. To begin with, the researchers (Kohlborn, 2014; Gouscos et al., 2007) have been concerned with assessing the impact and usefulness of such portals, which are not directly under the responsibility of a single authority. Kohlborn (2014) argued that lacking assessment opportunities are primarily connected to "the missing conceptualization of constructs related to quality, such as satisfaction, behavioral intentions, and value" (Kohlborn, 2014, p. 226). Gouscos et al. (2007) claimed to have found an assessment framework for the OSGs. They highlight the importance of such aspects as "effort of familiarization", or portal navigation, "effort of acquisition", or overall effort to request a service, "technical support necessity", "time of acquisition" and the overall "quality of experience" to be central to the assessment of the portal. According to them, the overall value of the portal is expressed in its ease of use, characterized by simplicity, compared to disconnected e-government services (Gouscos et al., 2007).

The same opinion is expressed by the group of researchers, who propose reference architectures, data models, and whole-scale portal prototypes - the interface must be user-friendly in the first place. However, besides offering such a principle, the authors highlight the importance of overall integration of the portal with different technology and application services, as well as throughout various authorities. Glassey (2004) proves the validity of this statement in his research on creating an OSG portal for the Swiss authorities. The researcher conducts a tedious description of all services in the Swiss public administrations (grouped in Information, Communication and Transaction types), their connection with different public authorities. As a result, the researcher categorizes all actors involved in service provision to offer a data model of an OSG-portal (Glassey, 2004). This work on process mapping proves that introducing technology to avoid administrative burden requires an understanding of processes in authorities that underlie service provision, as well as understanding the users. Moreover, having previously created a prototype of an OSG-portal, Glassey (2002) provides an example of how understanding the user may provide the key to simpler architectures even before offering the portal to users (Glassey, 2002).

Furthermore, researchers point out the importance of policy actions, related to standardization, promoting interoperability, and portal integration, as a vital step towards implementing the One-stop government. Describing the eGOV project, Tambouris (2001, p. 363) highlights that promoting open standards "to support interoperability between the national portal and other public authorities that provide content to the portal" is a vital component of any OSG project. It is especially crucial when it comes to complex administrative structures. Tambouris (2001) suggests the GML-XML application as a

possible open standard in this context. Similarly, viewing the implementation of the OSG policies from the perspective of eGovernment stage models as a first step towards implementing a No-stop shop government, Scholta et al., (2019a) highlight the integration of data collection, data storage and data use as critical features of a functional OSG portal.

According to Scholta et al. (2019a), triggering of eGovernment services through data collection can take place through individual forms, attributed to each administrative body or department, through "a single point of contact with citizens (one form, as in the one-stop-shop)", or through no form at all. Data collection through one form in this context requires a single integrated interface for all the authorities of all levels of governance, making it a central feature of the OSG. Meanwhile, data storage can remain "distributed or limited to department-wide integration", although holding high potential for being integrated consequently (Scholta et al., 2019a, p. 12). The main goal of the data collection through a single form is integrating data use, offering administrative services, where a citizen is not expected to submit the same information to multiple agencies multiple times.

Putting the issues of the One-stop government development in the policy context of Germany, Scholta et al. (2019b) point out that One-stop government policies towards eGovernment services that are "more convenient for citizens and businesses" are preceded by the policies "standardized service descriptions" and "interconnected portals", leading at the next stage of administrative integration to No-stop shop policies. At the first stage of achieving more citizen-centered eGovernment services, the state introduces standardized service descriptions, which "harmonize the specification of government services for citizens and businesses" and tackle the issue of identifying responsible authorities in complex administrative systems (Scholta et al., 2019b, p. 3275). This role is currently undertaken by FIM and KoSIT, described in the previous section. At the second stage, the state attempts to address the issue of communicating with authorities in a less complicated manner by establishing "connections between individual portals of government entities" and navigating the user towards the desired service provider (Scholta et al., 2019b). This stage is to be achieved by creating the integrated portal network by 2022, which is a central requirement of the OZG regulation. At this point, a single sign-on option of verifying identity is also offered, which in the context of Germany is expected to be realized through service accounts. As a next step the government aims at establishing a One-stop government portal, which frees the user from navigational efforts, while citizen "information is transferred to the right authority in the back end" (Scholta et al., 2019b, p. 3276).

Finally, previous research has been dealing with the architectural components of a One-stop government portal, aiming to identify essential features of a system that allows for

the “single form” convenience. According to Sedek et al. (2014), in a One-stop government system, consisting of a one-stop eGovernment portal, e-government application providers and e-government service providers, a One-stop eGovernment portal is responsible for providing an interface to the one-stop eGovernment application to users, “user security and registration, application subscription and application hosting” (Sedek et al., 2014, p. 98). In their perspective, such a system overall requires a high level of standardization and integration. Similarly, having developed a more complex structure of an OSG, Hongbo (2013) underscores that a key to achieving user satisfaction in electronic communication with citizens is information sharing and integration, which helps to satisfy the demand for high information security.

While researchers, designing OSG architectures discussed above, have not been relying on the EU Single Digital Gateway guidelines and building blocks, their works have been promoting the desired outcome of this supranational policy action: to achieve a “Multi-clinic” OSG (Hauser, 2017, p. 132). According to this goal, portal integration is not enough to achieve One-stop government services, as greater data collection integration is needed to deliver the desired user satisfaction. Although in complex administrative environments, such as Germany, preliminary steps towards OSG, such as portal integration, are vital, these efforts should not be mistaken for an OSG implementation.

All in all, based on the literature analyzed, it is hard to infer any requirements to reflect the One-stop government portal in the architectural blueprint. The way it can be organized varies significantly, apart from the fact that with a One-stop government-to-user interface, all communication and transactions are carried out by means of this interface. Moreover, the literature highlights the importance of the back-office integration in providing government services via OSG, which requires infrastructure for data sharing and joint data collection. These requirements are, however, better conceptualized in the Once-only principle related research, as discussed below.

5.1 Requirements of the Once-only Principle.

While no concrete policy action has been taken in the national level eGovernment development in Germany towards achieving a One-stop government after portal integration, there are cross-border projects testing the viability of this concept. These projects revolve around the Once-only principle, the basis for which is expected to be integrated with all the EU member states by 2023 (Demiri, 2018).

In academia, as well as in the high-level policy circles, there is no single definition of what the Once-only principle is. Generally, it is understood as an eGovernment principle, suggesting “that citizens and businesses should supply certain standard information only

once to a public administration" (Krimmer et al., 2017a, p. 546). Krimmer et al. (2017a) point out the controversy in the understanding of the OOP in the EU member states, which, on the one hand, suggest solely data collection integration, and, on the other hand, highlight the data storage integration as well. Following from the definition of the OSG and its particular connection to the data collection integration, the OOP in this thesis will be understood as "the collection of data, stipulating that data can be submitted to public administrations only once, while still allowing for multiple repositories" (Krimmer et al., 2017a, p. 547). Moreover, in the German policy context, one could differentiate between the Once-only principle 1.0, which presupposes data collection and sharing within public administrations, and the Once-only principle 2.0, which integrates "significant private sector actors" in this equation (Digitale Verwaltung und öffentliche IT, 2018).

While scientific efforts, defining the OSG are quite scarce, works that operationalized the Once-only principle are even less numerous. The searches for journals and contributions on OSG (in Government Information Quarterly, MIS Quarterly Proceedings of the International Conference on e-Learning, e-Business, Enterprise Information Systems and e-Government) have resulted in 0 mentionings of the Once-only principle. Nevertheless, academic efforts that focus on OOP implementation across the EU agree on precise requirements that enact the Once-only collection of citizen data, serving in many ways as preconditions to the OOP-implementation.

To begin with, the enabling of the Once-only principle is often viewed as following **well-developed and trustworthy data sharing practices** in public administrations. Krimmer et al. (2017a) point out that OOP-based eGovernment services rely on data sharing among public authorities with high respect for data protection in this context. According to Cave et al. (2017), data exchange, which ensures data protection, data quality, administrative collaboration, and re-use of data with underlying architecture and semantic solutions, is the cornerstone of an effective Once-only principle implementation. In more practical terms, the EU suggests the CEF eDelivery building block to be an essential element of the OOP-commitment (Once Only Principle reduce administrative burden for individuals and businesses, n.d.).

Following data sharing among administrative entities, the implementation of the Once-only principle requires a high degree of standardization (Krimmer et al. 2017a). Especially vital this requirement appears to be in the context of highly complex administrative structures. The National Norm Controlling Council of Germany has, in this respect, also recommended achieving greater **standardization of data forms and G2C and G2G interfaces** to enact the OOP-based eGovernment services (Fromm et al., 2015).

Furthermore, another CEF building blocks suggested for the implementation of the OOP are eID and eSignature (Once Only Principle reduce administrative burden for individuals and businesses, n.d.). Indeed, **electronic identification systems** are viewed as an essential component for establishing trust in OOP-enabled eGovernment services, as highlighted by Cave et al. (2017).

Additionally, Cave et al. (2017) point out the need for **integrated base registries** in the context of effective OOP-implementation. As suggested in EIF 2.0, base registries are "reliable sources of basic information on items such as persons, companies, vehicles, licenses, buildings, locations and roads, which are authentic and authoritative and form the cornerstone of public services" (ISA, 2015). Special attention has to be dedicated to the integration of base registries in contexts of high administrative complexity, such as in the case of Germany.

Finally, as already mentioned in the definition of data sharing (Krimmer et al., 2017a, Cave et al., 2017), the OOP-enabled eGovernment services have to comply with the data protection regulation and transfer data to administrative bodies upon agreement of the data subject (Fromm et al., 2015). In this respect, **rights, roles and responsibilities of actors involved should be clearly defined in this context** (Krimmer et al., 2017a; Cave et al., 2017; Digitale Verwaltung und öffentliche IT, 2018) and data sovereignty of subjects has to be guaranteed through the transparency of data sharing and use (Digitale Verwaltung und öffentliche IT, 2018).

All in all, the operational building blocks that enable eGovernment services, based on the Once-only principle, can be summarized into the following list of requirements:

1) Data sharing;

2) Standardized interfaces and data formats;

3) Electronic identification;

4) Integrated base registries:

5) Transparency in assigning roles and responsibilities of parties to the process.

Further requirements mentioned above point out the importance of data protection with regards to the OOP-enabled eGovernment services, which will be discussed in the following subsection, dealing with Privacy by design requirements. Data subject's consent and data sovereignty have not been included in this list, due to the duplication with the PbD requirements.

5.2 Requirements of the Privacy by Design Principle.

Although the principle of Privacy by design has received much attention since the publication of the EU General Data Protection Regulation (Council Regulation (EU) 2016/679, 2016, or the GDPR), the idea of entrenching privacy requirements in the design of information systems is not new. Still, defining it and its components has been troubling researchers for at least one decade.

The Privacy by design principle has been viewed as a solution to tackle a complex issue of data protection compliance through technology design. The GDPR itself defines privacy by design as "nothing more than data protection through technology design" (Council Regulation (EU) 2016/679, 2016). Researchers and practitioners have heavily criticized this understanding of the Privacy by design principle. They highlight that ensuring privacy by technology design allows to guarantee privacy rights only to a limited extent, and safeguarding privacy should, therefore, not be limited to implementing PbD (Koops & Leenes, 2014). Therefore, the academia and the practitioners see its implementation and effects as much more than just technology design. The essence of the idea to design technology, which considers data protection before being implemented, is a complicated task, taking into account the uncertainty about the meanings of regulatory prescriptions.

Moreover, researchers find it troublesome to grasp what level of design and which solution life cycle phases should be taken into consideration while designing data protection compliant eGovernment solutions. Gürses et al. (2011) point out that "data protection compliance should be embedded throughout the entire life cycle of technologies and procedures, from the early design stage to their deployment and use". Angelopoulos et al. (2017) draw additional attention to the fact that privacy protection should be embedded "into the design specifications of technologies, business practices, and physical infrastructures", suggesting modeling tools, which could help "to systematically elicit and document privacy, security and trust requirements". Pagallo (2012) agrees with such approach to understanding privacy by design. The researcher highlights that "organizing data processes and product design" is equally important when embedding data protection in information systems design, since business processes, such as data collection, handling, processing, storage and use, can also present danger to privacy, if carried out falsely (Pagallo, 2012, p. 332).

A similar approach is advocated by Cavoukian (2009, p. 1), who sees privacy by design to be comprised of the "trilogy of 1) IT Systems, 2) accountable business practices, and 3) physical design and networked infrastructure". Gürses et al. (2011) also suggest concrete steps to design information systems and underlying processes that comply with

data protection regulation. Thus, in this work, Privacy by design will be understood as "an approach to protecting privacy by embedding it into the design specifications of technologies, business practices, and physical infrastructures" (Angelopoulos et al., 2017, p. 4).

As far as the operational components of Privacy by design are concerned, Cavoukian (2009) has developed a list of conditions, which according to her, could help to enable electronic services, compliant with data protection regulations. According to Cavoukian (2009), designing data protection means ensuring 1) privacy by default, 2) visibility and transparency of data use, and 3) data subjects' empowerment to controlling the use of their data. More precisely, 1) privacy by default should be understood as a combination of 1.1) embedded purpose specification procedures, through which data subject is informed about the intention to leverage particular data, 1.2) data collection limitation and 1.3) data minimization, which ensures that only data needed to provide a service is being collected, as well as use, 1.4) retention and disclosure limitation, which means that data controlling actions have to serve a specified purpose. As far as visibility and transparency of data use are concerned, Cavoukian highlights assuring the 2.1) accountability of service providers, 2.2) openness of regulatory expectations, and 2.3) compliance and 2.4) redress mechanisms. Finally, empowering data subjects to control the use of their data is, according to the researcher ensured by the following: 3.1) obtaining the explicit consent of data subjects to process their data, 3.2) maintaining accuracy, 3.3) completeness and up-to-date information, as well as 3.4) providing access to individuals to information about the use of their data (Cavoukian, 2009).

Apart from suggesting 12 actionable process and information systems design principles, Cavoukian's work lays the ground for the process of engineering Privacy by design, conceptualized in Gürses et al. (2011). The researchers in this respect highlight that purpose specification and data minimization are crucial to data protection compliant digital services. The data minimization requirement should be enacted by anonymization and pseudonymization. Gürses et al. (2011) highlight, therefore, data minimization as a second step to engineering Privacy by design, undertaken as a result of functional requirements analysis and precise description of system functionality, followed by modeling attackers and assessing risks and threats, as well as by multilateral security requirements analysis and implementation and testing (Gürses et al., 2011).

Although not tailored specifically to enabling data protection compliant eGovernment services in a particular context the requirements, summarized by Cavoukian (2009) and further elaborated by Gürses et al. (2011), have served as a starting point for many analytical works, interpreting the GDPR-established Privacy by design to eGovernment

practitioners in Europe. They have also been discussed in the context of implementing electronic health cards and eID in Germany by Schaar (2010). The former German Data Protection Commissioner highlighted that for the implementation of electronic health card it was essential to 1) guarantee data sovereignty of the insured person, 2) ensure the voluntary basis for the use of an electronic card, 3) establish control of the insured person over the "extent of data", recorded and deleted from the system, 4) establish control of the patient over data access, 5) ensure the right to be informed about operations, performed with personal data and 6) provide an ability to check, which parties have accessed their data (Schaar, 2010). Moreover, according to Schaar (2010) "when taking decisions about the design of a processing system, its acquisition and operation, the following general objectives should be observed: 1) data minimization, 2) controllability of the subject over personal data, 3) transparency of the system operation, 4) data confidentiality and authorized access to data, 5) data quality, 6) possibility of segregation of IT systems, used for different purposes" (Schaar, 2010, p. 273).

In practice, these requirements have also been extended by the requirements of end-to-end compliance (use of system components, which officially commit to complying with data protection regulation), data security requirements and good practice data handling procedures (such as end-to-end encryption) (DSK, 2017). These principles are, however, rather, technology and implementation-specific and, therefore, will not be included in the scope of this thesis.

All in all, based on contributions by Cavoukian and Schaar, one could summarize the following requirements to Privacy by design compliant eGovernment services:

1) Purpose specification;
2) Data minimization in collection and processing;
3) Accountability and confidentiality of data controllers and processors;
4) Controllability of available data by data subject
5) Accuracy and data quality;
6) Access to information about collected and stored data;
7) Consent of the data subject to data processing.

All in all, these seven regulatory requirements are considered to be vital in implementing the Privacy by design principle and ensuring data protection compliant electronic services. They have been conceptualized as building the ground for privacy-aware development of information systems. "Privacy-aware development requires to guarantee as much as possible that data privacy is considered during all the phases of the development process and guaranteed by the resulting systems" (Colombo & Ferrari,

2012, p. 81). Moreover, they include privacy sensitive requirements of data subject's consent and data sovereignty (formulated here as controllability).

To sum up, this section has outlined 12 requirements that an OSG portal needs to fulfill in its process and information systems design in order to fulfill the Once-only and the Privacy by design principles. The integration of these requirements with an OSG portal should be, thus, understood as a primary objective of the architectural blueprint, which guides compliance with these 2 high-level principles. Moreover, as both the definition of the OOP and the PbD show, key challenge to enabling the OOP and PbD compliant administrative services is to design administrative processes that underly these requirements and are essential for IT design. Therefore, the literature review further justifies the focus of this work on the process domain, rather than the technology domain. This finding will also be crucial to artifact development in the following chapter. Finally, it is crucial to underscore, that dealing with PbD and OOP implementation in pursuing One-stop government policies, this thesis focuses mostly on administrative services, provided to citizens, rather than businesses. This additional limitation is crucial to place due to the fact that selecting regulation for some requirements (such as 4) Integrated base registries to fulfill the OOP), the author will deal with different regulatory documents, depending on the potential user group of digital administrative services.

6 The Artifact for Aligning the OOP and the PbD Requirements.

This chapter will proceed with analyzing closer the legal basis for giving way to the implementation of the Once-only principle and its alignment with the Privacy by design principle in Germany. The national legislation is directly addressing neither of the principles, therefore, relevant EU Regulation has been drawn upon to seek the connection with further eGovernment requirements.

As mentioned previously, the requirements, identified through the literature review, will not be used fully in proceeding with the development of an architectural blueprint. This is due to the fact that a part of requirements, fulfilling the implementation of the Once-only principle is primarily focused on privacy protection by data controllers and processors. It especially concerns the requirements such as 6) Consent of the data subject and 7) Data sovereignty of data subjects, which are directly mentioned as part of the fulfillment conditions for the Privacy by Design principle (see 4) Controllability of available data by the data subject and 7) Consent of data subject to data processing).

Indeed, previous research highlights the need for safeguarding privacy in the contexts of data sharing and data reuse by public administrations while providing administrative e-services. For this reason, the PbD principle will be understood as partially overlapping with the Once-only principle, as depicted in **Figure 1**. It also reflects the requirements for fulfilling the OOP and the PbD, as well as the role of the Once-only principle in realizing the implementation of the One-stop government policies.

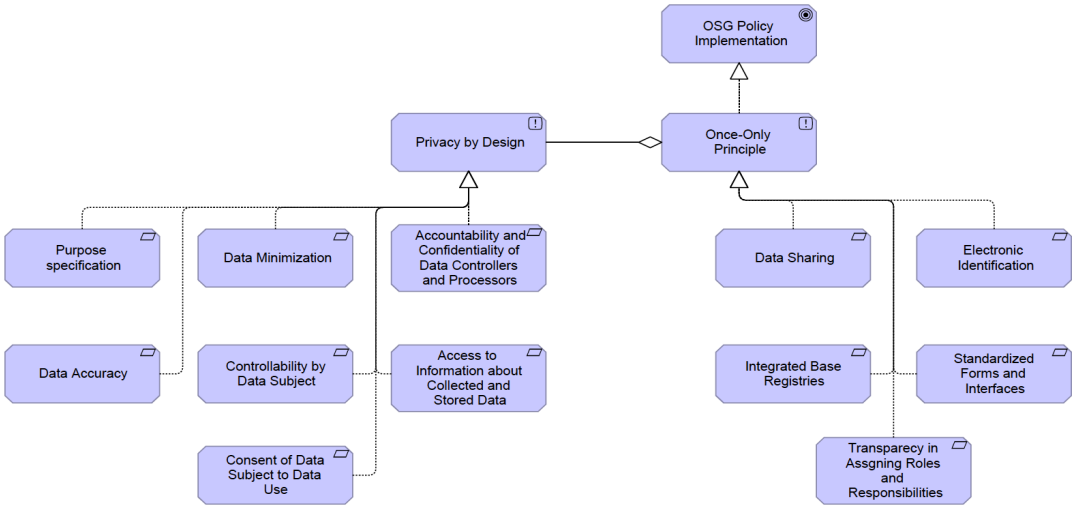


Figure 1. OOP and PbD principles and requirements.

Apart from operationalizing the meaning of the concepts OOP and PbD through the requirements, this classification plays an essential role in identifying the important legislative sources of specifications for data handling processes and systems. The sources

of common law, issued on the federal level in Germany and on the supranational level, have been studied throughout the prism of relevant literature to develop specifications for seven PbD and five OOP requirements.

EU Regulation. To begin with, the German government has expressed its commitment to implementing the Single Digital Gateway regulation of the European Union, adopted in 2018 (The Single Digital Gateway of the European Union, n.d.). According to this regulation, access to the government services in the European Union should be enabled for the EU citizens through the single digital gateway - Your Europe portal.

As stated in the Preamble of the SDG regulation, "this Regulation should support the use of the 'once-only' principle and should fully respect the fundamental right to the protection of personal data, for the purpose of the exchange of evidence between competent authorities in different Member States" (Council Regulation (EU) 2018/1724, 2018, p. 3). It foresees the creation of the cross-border by default and accessible national public e-services, which are interoperable and can be integrated into the pan-European One-stop government portal for essential EU services. The gateway is, thus, expected to set up conditions for providing all necessary information about public e-services, offering key contacts for assistance, and enabling one-stop government transactions via the portal interface on the EU level. Primarily, the goal of enabling the One-stop government portal provision of administrative services is focused around "the 21 requested public administration procedures, organized around certain life events: (1) birth, (2) residence, (3) studying, (4) working, (5) moving, (6) retiring, (7) starting, running and closing a business" (Rinne, 2019, p. 39). In the context of this thesis, the regulatory provisions of the Single Digital Gateway regulation for 1) Data sharing and 3) Electronic identification and 5) Transparency in assigning roles and responsibilities, fulfilling the implementation of the Once-only principle, will be essential.

Being adopted in the form of regulation by the European Union institutions and, therefore, having a high degree of consensus around its prescriptions, the Single Digital Gateway regulation is to be implemented by all member states without exclusions within 2018-2023 (Somssich, 2015). The regulatory prescriptions of the SDG regulation will, for this reason, be treated in this thesis as possessing equivalent regulatory power to the federal-level national legislation.

The same commitment to the implementation is expected to be expressed towards the Electronic Identification, Authentication, and Trust Services (eIDAS) regulation, which brings forward the importance of personal identification services to perform transactions to receive digital public services. With electronic identification being an essential requirement for the implementation of both the One-stop government portal and the

Once-only principle, the success of the implementation of cross-border electronic identification services largely defines the implementation of the SDG regulation (Rinne, 2019).

eIDAS regulation calls upon cross-border enabling of the electronic identification means, which are compatible in all national electronic identification schemes of the national administrative e-services. Moreover, the regulation puts forward the implementation of interoperable electronic trust services, namely electronic signatures, electronic seals, time stamps, electronic delivery services, and website authentication (Council Regulation (EU) 910/2014, 2014). Although the spectrum of electronic trust services, addressed by the regulation is quite broad, this work will focus primarily on 3) Electronic identification, essential for the implementation of the Once-only principle.

German National Regulation. As it comes to translating the prescriptions of the regulatory requirements of the German national legislation, the author points out that the architectural blueprint is not meant to cover or aggregate all possible OOP and PbD requirements specific to selected (in either SDG regulation or OZG) services. Neither does it aim at combining the specifics of each state or municipal administrative proceedings. Such undertakings require considerable effort and resources, as well as cooperative engagement of relevant authorities, which is beyond the scope of this work. For this reason, it is primarily the national sources of common law that will be taken into account for developing the architectural blueprint.

To begin with, the eGovernment implementation efforts have been entrenched in the Basic Law of the Federal Republic of Germany (GG), the German constitution. The Art. 91c of the GG has laid the basis for the strategic action on the national scale, as well as for the creation of the institutional framework, surrounding key administrative bodies and structures behind eGovernment. Apart from creating a legislative framework for the cooperation of actors in the federal administrative structure, it gives way to the standardization on the basis of agreements across the federation levels (Junk, 2009). Thus, this provision is essential for the specification of 2) Standardized forms and interfaces.

Moreover, due to the time-critical character of the SDG and the OOP implementation, several legislative acts, essential in the process of translating regulatory requirements into technical specifications, are being adopted on the federal level. A vivid example is the implementation of the Bureaucracy Alleviation Law III (Bürokratieentlastungsgesetz III), which paves the way towards the creation of 4) Integrated base registries for businesses. Due to the fact that the future of contents of these regulatory acts has not been fully defined and adopted as of February-March 2020, these legislative requirements will not be taken into account.

Furthermore, the most prominent regulation that has to deal with the implementation of the SDG regulation on the national scale, according to the IT Planning Council (The Single Digital Gateway of the European Union, n.d.), is the recently adopted Online Access Law. The Online Access Law is targeted at having 575 services in federal, state and municipal service provision digitalized by 2022. It further creates a regulatory framework for their interconnection in the integrated portal network and promotes the creation of cross-state interoperable electronic identification solutions - service accounts (Onlinezugangsgesetz – OZG, 2017).

According to the Online Access Law, the integrated portal network should serve as a single point of access, which navigates users to the online portal of responsible authority and, therefore, does not aim at creating a single digital gateway. Moreover, the text of the regulation is quite concise and has a mere prescriptive nature, rather than descriptive, like sectoral regulation. Nevertheless, its role is essential in mapping the requirements of 1) Data Sharing and 3) Electronic identification for paving the way to OOP-implementation. It also brings up relevant points, which cover the realization of 7) Consent of data subject to data use requirement of the Privacy by design principle.

Additionally, all eGovernment initiatives in Germany draw upon the legal provisions of the eGovernment Act (E-Government Act - EgovG, 2013), or the Act to Promote Electronic Government. Being a predecessor of the Online Access Law in the specialized field of the digital public services regulation, the Act obliges public administrations to ensure online access to the administrative services. The regulation forces the implementation of the De-Mail infrastructure, as central to the realization of digital public services. Furthermore, the regulation permits the replacement of written forms through electronic ones by means of securing them through technologies, such as Qualified Electronic Signature. This regulation serves as a reference for state eGovernment laws and provides details on the roles and responsibilities of parties to the process. Finally, the regulation instructs responsible authorities on their role in the process of standardization and vests binding power in their decisions (E-Government-Gesetz, n.d.). Therefore, the legal requirements of the eGovernment Act, 2013, serve as a basis for specifying technical services and processes behind 1) Data sharing, 2) Standardized forms and interfaces, and 5) Transparency in assigning roles and responsibilities.

In addition, the following regulations that deal with 3) Electronic identification for realizing the Once-only principle have been identified in this work: the Act on Identity Cards and Electronic Identification, which fixes the use of electronic identification means, and the Act on Electronic ID Card, which is intended to ensure the implementation of the eIDAS regulation. The latter one foresees the use of electronic ID cards by EU-

citizens in German service portals as identification means to receive digital administrative services. Having been adopted quite recently (in June 2019), the regulation still requires more precision on the technical implementation.

Moreover, this work will view the Administrative Procedures Act of 1976 as an additional source for requirements to implement the One-stop government portal in Germany. Although often viewed as a barrier to digitalization in public administrations, the Administrative Procedures Act has been amended several times to integrate the electronic service provision by the public sector (Djeffal, 2018). Thus, the requirement to provide a written form by the citizen to receive a public service was replaced by confirming the validity of an electronic form after the adoption of the Act to Promote Electronic Government (BMI, Referat O2, n.d.). Therefore, this regulatory document serves as a basis for the specification of the OOP requirement 2) Standardized forms and interfaces.

Besides the GG, the EGovG and the Administrative Procedures Act, it is the resolutions of the IT Planning Council regarding the mandatory adoption of federally developed standards that serve as a basis for the specification of 2) Standardized forms and interfaces. In particular, it is the resolutions 2019/15, 2019/14, 2018/40, and 2017/40 that play a key role in the standardization of data exchange interfaces and data forms to collect information from citizens. The binding power of the IT Planning Council resolutions is prescribed by the Act to Promote Electronic Government in Art. 10, stating that "if the IT Planning Council adopts a resolution on supradisciplinary and interdisciplinary IT interoperability or IT security standards, they should be enacted" (E-Government Act - EgovG, 2013).

Finally, two sectoral regulatory documents will be considered while creating the architectural blueprint. The necessity of their use is justified by the absence of a modernized registry landscape and the corresponding regulation (Nationaler Normenkontrollrat, 2017). More precisely, there is no centralized solution for registry maintenance or registry interconnection on the federal level neither for persons nor for businesses. Thus, this thesis will make use of the Federal Act on Civil Status, 2007, and the Federal Act on Registration, as of 2017, which regulate the registry keeping and the use of the base data on persons (Nationaler Normenkontrollrat, 2017).

Data Protection Regulation. Most of the technical specifications for the Privacy by design requirements originate from the EU General Data Protection Regulation (GDPR), 2016, and the Federal Act on Data Protection (BDSG), 2018. The term Privacy by design appears both in the BDSG and the GDPR, where it is defined as "data protection through technology design" (Council Regulation (EU) 2016/679, 2016). Its requirements, defined for this thesis, largely correspond to the principles of data handling in Art. 6 of the GDPR:

1) lawfulness, fairness and transparency; 2) purpose limitation; 3) data minimization: 4) accuracy; 5) storage limitation; 6) integrity and confidentiality; 7) accountability (Council Regulation (EU) 2016/679, 2016).

Nevertheless, since the Privacy by design definition, used in this thesis, comprises technical and organizational measures to ensure the respect for citizens' privacy rights, the principles, defined in the Art. 6 of GDPR, have been regrouped to correspond to the Privacy by design requirements, introduced in the literature review. These adjustments have resulted in the following representation of the GDPR principles of data handling:

1) Purpose specification, corresponding to purpose specification in GDPR;

2) Data minimization in collection and processing, corresponding to data minimization in GDPR;

3) Accountability and confidentiality of data controllers and processors, corresponding to accountability in GDPR;

4) Controllability of available data by data subject, corresponding to storage limitation in GDPR;

5) Accuracy and data quality, corresponding to accuracy in GDPR;

6) Access to information about collected and stored data, corresponding to integrity and confidentiality in GDPR;

7) Consent of the data subject to data processing, corresponding to lawfulness, fairness and transparency in GDPR.

Unlike in the process of specification of legal requirements of the Once-only principle, the Privacy by design requirements have been consistently gathered from the EU General Data Protection Regulation.

"Despite being directly binding for all the EU member states, the GDPR does not render national data protection provision obsolete" (Molnár-Gábor, 2018, p. 619), which has led the German Bundestag to adopt the national Data protection regulation in accordance with GDPR. Thus, the Federal Act on Data Protection is used in this thesis as an additional source for the specification of some of the requirements, including 1) Purpose specification and system segregation (if necessary) to fulfill the desired purpose, 2) Data minimization in collection and processing, 3) Accountability and confidentiality of data controllers and processors, 4) Controllability of available data by the data subject, and 6)

Access to information about collected and stored data, corresponding to integrity and confidentiality in GDPR.

According to Kolain & Wirth (2018), the listing of requirements, along with their definition and prescriptions to implement them in legislation, serves as an overview of the precise steps, meant to fulfill them. While listing each article referring to a single regulatory act is sufficient (as in Kolain & Wirth (2018)), this approach does not suffice, in case of applying the method of legal specification to several legal documents. Complex relationships are created while adopting regulations in national and supranational jurisdictions. Moreover, a single regulatory act often prescribes the implementation guidelines for several requirements, realizing the principle. Thus, the author of this thesis has expanded the approach to legal specification by opting for a table representation. The complete overview of legislative acts and their requirements is represented in Annex 1.

6.1 Fulfilling the Requirements of the Once-only Principle.

Data Sharing. To begin with, the implementation of the OOP presupposes that receiving citizen data once, the authorities, responsible for providing various categories of administrative services, will use this data to provide any service without requesting this data from the citizen again. Thus, the terminology data Controller and data Processor can be applied to this perspective to indicate authorities, which serve as a primary receiver of citizen data and the service provider, who leverages this already provided and processed data. Data Controller and Processor can be perceived as the roles that a responsible authority plays in the process of service provision. A collaboration of the roles Processor and Controller is aimed at fulfilling the Once-only principle (Fulfilling OOP in **Figure 2**), which in their interaction reuse already submitted citizen data (Reusing citizen Data in **Figure 2**).

According to Art. 8 of the Online Access Law, “permanent storage of the identity data and its transmission to and use by the authority responsible for the Administrative Service is permitted. In the case of permanent storage, the user must have the possibility to delete the user account and all stored data independently at any time” (Onlinezugangsgesetz – OZG, 2017). This provision enables the process of the Controller, related to Sharing data, and the process “Request data from controller” in the overall “Providing Service” function of a Processor. Moreover, as prescribed by Art. 5 of the Act to Promote Electronic Government, transmission of citizen data may be done electronically: “With the consent of the data subject involved in the procedure, the competent authority may electronically obtain the necessary evidence from a German public body directly from the issuing public body” (E-Government Act – EgovG, 2013).

More precisely, the process of Providing Service from the Processor perspective includes several steps. Having received a request for a service, the Processor checks, whether the required data has already been submitted earlier, and whether the Processor is simultaneously a Controller. The Processor retrieves base data in order to be able to identify the citizen and requests additional information from another Controller or the User, if necessary. Having examined the data, the Processor can then provide a requested service to the citizen. The same is valid for the Controller, which by Sharing data, checks the Processor request on the subject of Processor's eligibility and Controller's access to the data and forwards it after retrieving.

For Germany, citizen data transmission in providing administrative services is also expected to function in the cross-border context. While the national regulation does not prescribe any information services to be used while Sharing data, Art. 38 of the SDG regulation requires that "the Internal Market Information (IMI) system shall be used for exchanges of information, including of personal data, among the IMI actors" (Council Regulation (EU) 2018/1724, 2018, p. 28), which according to Art. 14 is "established by the Commission in cooperation with the Member States" (Council Regulation (EU) 2018/1724, 2018, p. 20).

For the German national context, it is also essential to take into consideration that the standard XFall should be considered for the information exchange between public authorities and the interoperable data forms respectively. These requirements will be discussed more in detail in the next subsection.

Finally, the application component (currently included in the blueprint as IMI, as part of the Information exchange Function, which should be extended with an application component appropriate to the national data transfers) shall provide an application interface to the Controller. The model of the requirement Data Sharing is depicted in **Figure 2**.

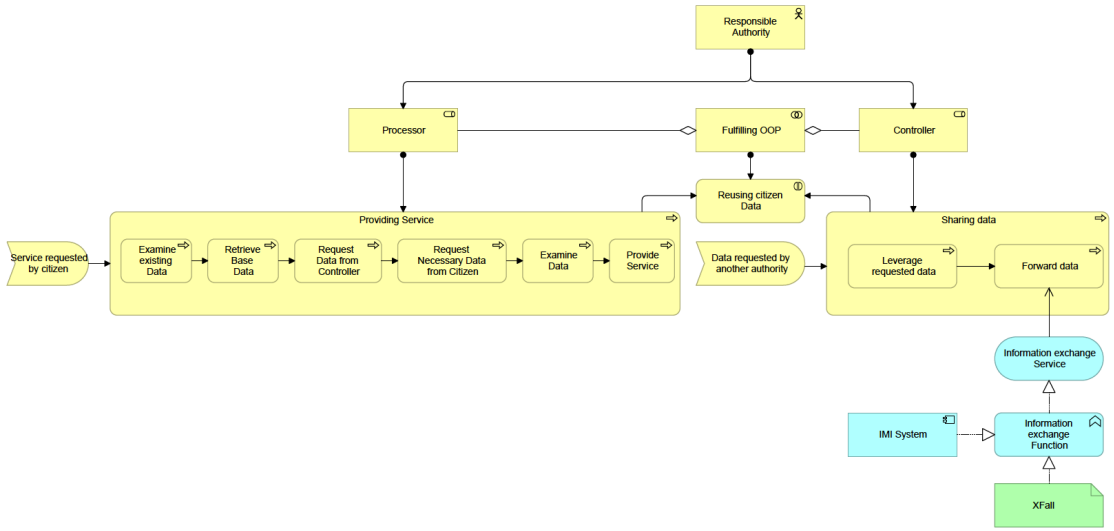


Figure 2. Data sharing.

Standardized Interfaces and Forms. In the federalist context of Germany, standardization plays a crucial role in building the integrated portal network, as well as for the fulfillment of the OSG policies (Scholta et al., 2019b). Therefore, the need for realizing this requirement finds evidence in numerous legislative documents and policy initiatives of the Federal Government. The development of the "one-for-all" standardized forms and interfaces is also part of these initiatives and is fulfilled in the form of cooperation between the administrative levels. According to Art. 91c of the Basic Law of the Federal Republic of Germany, "the federal and the state governments can determine the standards and security requirements necessary for communication between their IT systems. Agreements on the basis of cooperation are required" (Basic Law for the Federal Republic of Germany - GG, 1949).

In doing so, the central role in steering the process is assigned to the IT Planning Council. The defined standards have a binding nature and are expected to be implemented across all federal levels. The Act to Promote Electronic Government thereby prescribes in Art. 10: "If the Planning Council for cooperation on IT matters in the field of public administration between the Federation and the Länder (the IT Planning Council) adopts a resolution on supradisciplinary and interdisciplinary IT interoperability or IT security standards, they should be enacted" (E-Government Act – EgovG, 2013), which is depicted in Annex 2.

In addition to Art. 10, the EGovG provides in the context of standardization a requirement for a transition to electronic forms, submitted to the authorities as a service request, which is outlined in Art. 13: "Where a legal provision stipulates the use of a certain form providing a signature field, this alone shall not be tantamount to requiring written form.

The signature field shall be omitted from a version of the form intended for electronic submission to the authority" (E-Government Act – EgovG, 2013). Further options for the submission of Electronic Forms in the state administrative proceeding are outlined in Art. 3a of the Administrative Procedures Act: "Documents can be submitted in an electronic format, and electronic documents must be signed with a qualified electronic signature, or through an electronic form, accessible by public bodies, or De-Mail" (Verwaltungsverfahrensgesetz - VwVfG, 1976).

Coming back to the role assigned to the IT Planning Council in defining standards, it is the resolutions of the IT Planning Council that enforce standards, defined through complex standardization initiatives, like KoSIT and FIM, addressed in the Section eGovernment Initiatives on the National Level in Germany. More precisely, it means that the standards, defined within FIM and KoSIT underly the resolutions of the IT Planning Council and the standards should, therefore, be included in the blueprint, although not being part of the federal regulation. In the context of standardized forms and interfaces (which include both interfaces provided to citizens and between data controllers and processors), XFall, XProzess, and XDatenfelder standards have special relevance.

XFall has been adopted with the 2017/40 resolution of the IT Planning and sets an interoperability standard "for the exchange of applications between the administrative bodies and user, as well as among administrative bodies" (Entscheidung 2017/40, 2017). Thus, as shown in Figure 2, XFall should be considered in the Sharing data process between authorities, as well as between Users on the one side and Processors and Controllers, communicating by means of the One-Stop Government Portal, on the other (which is depicted in Figure 3).

The resolution 2019/15 of the IT Planning Council adopts XDatenfelder, "the interoperability standard for the exchange of basic information, used in FIM-Datenfelder among public administrations" (Entscheidung 2019/15, 2019). XDatenfelder underlies the standardized forms used in requesting services by citizens from public administrations, which, according to the EGovG, can be submitted electronically. This XML standard lays the basis for the reference forms, realized through the FIM-Datenfelder, which in turn underlies Standardized Forms provided to citizens for submission.

Finally, although the regulatory provision is not providing process or service design prescription, it is still worth mentioning Art. 20 of GDPR. Art. 20 points out the need for standardized data forms in the context of data transportability: "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format

and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided". Thus, offering standardized forms to collect data from citizens could enable public authorities to fulfill the GDPR provisions. The complete model of the requirement 2) Standardized interfaces and forms is presented in **Figure 3**.

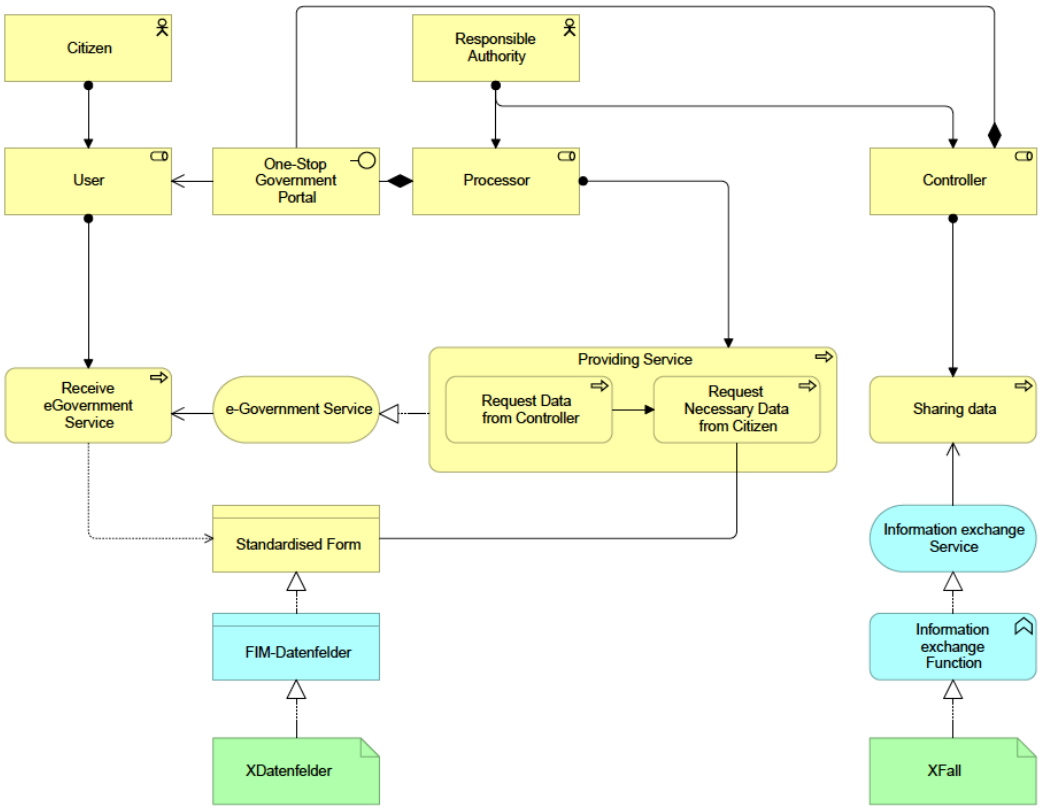


Figure 3. Standardized interfaces and forms.

Electronic Identification. According to Art. 3 of the Online Access Law "The federal government and the states provide user accounts in the integrated portal network, which enable users to identify themselves uniformly to receive the electronic administrative services of the federal government and the states, available in the portal network" (Onlinezugangsgesetz – OZG, 2017). For this reason, the Identify oneself on the Service Portal process is modelled in **Figure 4** as a first step to Receiving eGovernment services by Users.

However, as already revealed in the Section eGovernment Initiatives on the National Level in Germany. of this thesis, the infrastructure underlying user accounts varies depending on the trust levels, defined at the account confirmation stage. At the highest level of security, which takes place through the eID authorization, the User is able to store

documents in his or her service account and share them with the authorities electronically. Such a precondition is important for receiving eGovernment services fully electronically and media break free, which is why this thesis deals with eIDs as a means of identification on service accounts, with their connection to a One-stop government portal. As depicted in **Figure 4**, designated public authorities also undertake the role of Enablers of User Accounts, who are responsible for Establishing User Accounts and, as discussed later, for Adjusting identification requirements to cross-border users' needs.

Electronic identification of users for receiving eGovernment services is specified in Art. 18 of the Act on Identity Cards and Electronic Identification by prescribing that "Electronic identification shall take place via the transmission of data from the Electronic Storage and Processing Medium of the identity card. Data shall be transmitted only if the Service Provider transmits a valid authorization certificate (User Authorization) to the identity cardholder (the User), who then enters his/her PIN code" (Act on Identity Cards and Electronic Identification - PAuswG, 2009). This provision is fully in accordance with Art. 5 of the Act on Electronic ID Card adopted recently (Gesetz über eine Karte für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums mit Funktion zum elektronischen Identitätsnachweis – eIDKG, 2019). **Figure 4** depicts the Electronic Identification Service and the Electronic Storage Service, together with the application functions and components realizing them. It also introduces the role of the Service Provider, along with assigned processes, related to user authentication (User Authorization).

Furthermore, with respect to the electronic identification, Art. 7 of the OZG prescribes that "Public bodies, designated by the federal government and the states respectively, should take care of establishment of user accounts and registration of users. The accounts should be recognized by all authorities". This legislative provision is only concisely represented in the model in **Figure 4**. Nevertheless, it finds further refinement in the Art. 12 of the Act on Electronic ID Card, which states that "When applicants pick up their identity cards, they shall state in writing to the identity card authority whether they intend to use the electronic identification function. If not the ID card authority should deactivate this function" (Gesetz über eine Karte für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums mit Funktion zum elektronischen Identitätsnachweis – eIDKG, 2019). This provision replaces Art. 10 of the Act on Identity Cards and Electronic Identification (PAuswG, 2009), which prescribes the opt-in activation of the electronic identification function with a possibility to change citizen's mind at any time.

Regarding the responsibilities of processing authorities in this respect, the responsible authorities are only allowed to use the data stored on the ID card only for identity

verification purposes. This provision finds justification in Art. 20 of both the Act on Identity Cards and Electronic Identification and the Act on Electronic ID Card, highlighting that "Public sector bodies may use the identity card only to verify identity electronically and not for the automated retrieval or storage of personal data" (Act on Identity Cards and Electronic Identification - PAuswG, 2009; Gesetz über eine Karte für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums mit Funktion zum elektronischen Identitätsnachweis – eIDKG, 2019).

Finally, from the cross-border perspective, according to Art. 13 of the SDG regulation, "Member States shall ensure that … c) cross-border users are able to identify and authenticate themselves, sign or seal documents electronically"… (Council Regulation (EU) 2018/1724, 2018, p. 20). More precisely it means, as stated in Art. 6 of the eIDAS regulation, that "the electronic identification means issued in another Member State shall be recognized in the first Member State for the purposes of cross-border authentication for that service online" (Council Regulation (EU) 910/2014, p. 86). Therefore, the identification of cross-border users is treated in this thesis in the same way as that of the German citizens.

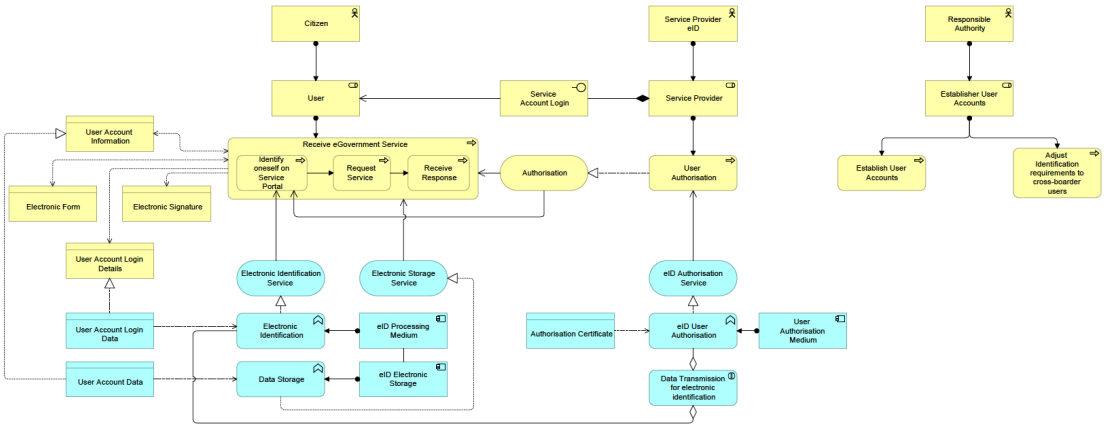


Figure 4. Electronic identification.

Integrated Base Registries. It is essential to clarify upfront that the requirement of integrated base registries is not addressed in the currently adopted German legislation and is only foreseen to be adopted for the business registries in the near future. Furthermore, it is not entirely clear whether existing registries for persons will be used as base registries and if they will, in which way they will be interconnected across administrative levels and with each other. Nevertheless, the author of this thesis has utilized the recommendations of the Norm Controlling Council and included the requirements for maintaining and accessing the population and civil status registries (depicted in the model of Figure 5 generally as Registries) in the process of service provision.

According to Art. 3 of the Federal Act on Registration "to carry out tasks the registration authorities should store personal data in the population registry" (Federal Act on Registration – BMG, 2013). Registration authorities in their role of data Controllers, therefore, Store Base Data upon receiving the citizen consent to base data storage (Request Consent to Base Data Storage). In case of the civil status registry, it is, furthermore, prescribed by Art. 3 of the Federal Act on Civil Status for registry-keeping to be carried out electronically (Personenstandsgesetz – PStG, 2007).

Finally, Art. 38 of the Federal Act on Registration and Art. 55 of the Federal Act on Civil Status foresee the collaboration of the Controller and the Processor in providing electronic public services through data sharing, under the condition that "Technical infrastructure is available to share data and/or provide access to it" (Personenstandsgesetz – PStG, 2007). However, the role of registries in this context is not covered in the regulation. These scarce provisions regarding the role of base registries in the fulfillment of the Once-only principle are depicted in **Figure 5**.

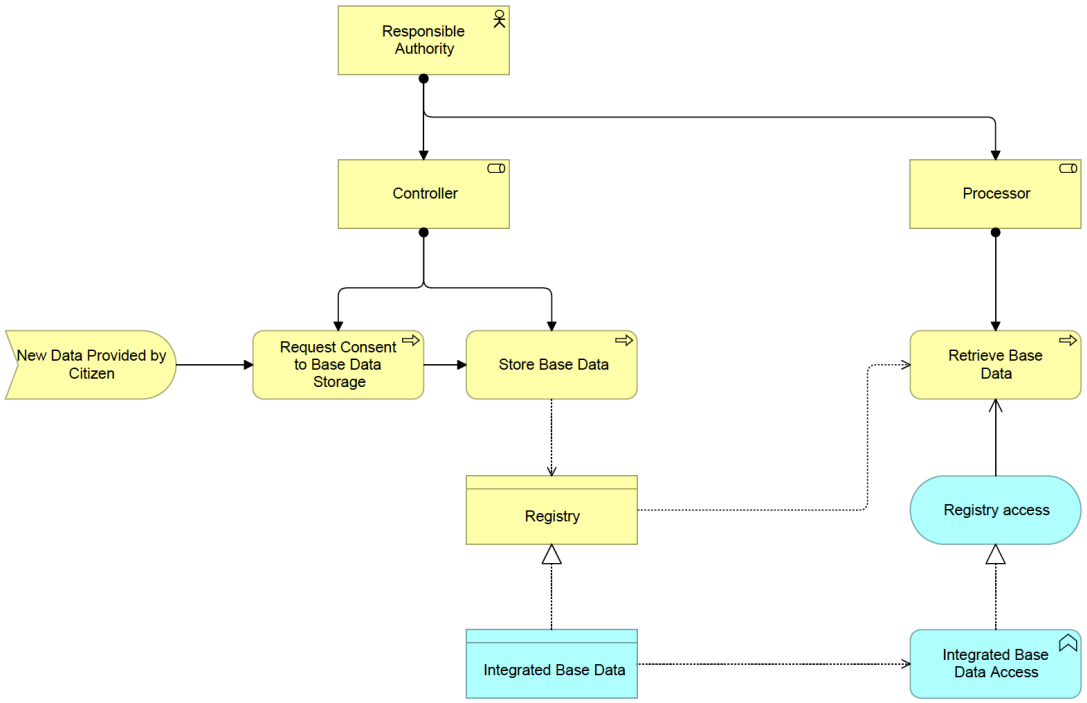


Figure 5. Integrated base registries.

Transparency in Assigning Roles and Responsibilities of Parties to the Process. Finally, when it comes to enabling the Once-only principle, the literature, as well as the legislation, requires that Controllers and Processors provide transparent information on processing data and the role of parties to the process (Provide Information on Activities and responsibilities). This request is entrenched in the Act to Promote Electronic Government, Art. 3: "Every authority shall provide information in generally

comprehensible terms about its activities under public law relating to external parties and provide contact details and forms for citizens" (E-Government Act – EgovG, 2013). In this context, the activities involving external parties include, but are not limited to, data sharing between Processors and Controllers, as well as the authentication services revealed in subsection Electronic Identification as a Prerequisite to Fulfilling the Once-only principle. With respect to several authorities partaking in data processing, Art. 11 of the EGovG stipulates additionally that "Joint procedures are permissible and require transparency in ensuring the legality of collecting, processing and using data. An overview is maintained by data protection officials on both sides" (E-Government Act – EgovG, 2013).

Ensuring transparency through providing publicly accessible information is depicted in **Figure 6**, as one of the processes associated with responsible authority's role as Processors (Provide information on activities and responsibilities). Furthermore, this requirement is underpinned by the EU Single Digital Gateway regulation in Art. 10: "The Member States and the Commission shall ensure that, before users have to identify themselves prior to launching the procedure, they have access to a sufficiently comprehensive, clear and user-friendly explanation of … b) the name of the competent authority responsible for the procedure, including its contact details" (Council Regulation (EU) 2018/1724, 2018, p. 18).

In addition, regulatory provisions attempt to ensure transparency in assigning roles and responsibilities through the authorization of public administration employees (Authorize Oneself) and log data keeping (Organize and save records of the procedure). Thus, Art. 39 of the Federal Act on Registration prescribes that "the body authorized to retrieve data shall take appropriate technical and organizational measures to ensure that data can be retrieved only by authorized persons" (Federal Act on Registration – BMG, 2013). What is more, Art. 40 of the Federal Act on Registration requires authorities to "keep a record of the following: 1. the body authorized to retrieve the data, 2. the data retrieved, 3. the time of retrieval, 4. the file reference of the retrieving authority, if extant, 5. the identifier of the retrieving person. Keep log data for 12 months" (Federal Act on Registration – BMG, 2013). Although the processes performed by the Public Administration Employee (modeled in **Figure 6**) have been collected from the regulation, dealing with a concrete set of services - registration, their relevance is additionally revealed in general regulation on data protection in the subsequent subsections. Nevertheless, it is also crucial for grasping the meaning of transparency in assigning roles and responsibilities and is, therefore, already brought up in this subsection.

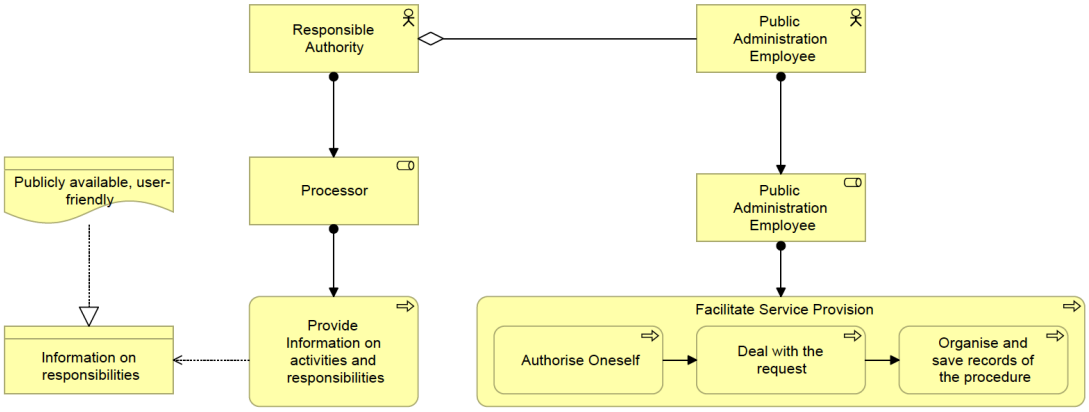


Figure 6. Transparency in assigning roles and responsibilities of parties.

6.2 Fulfilling Privacy by Design Requirements.

Purpose Specification. The requirement of purpose specification is central to GDPR-compliant data handling and requires personal data to be "… 2) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes…" (Council Regulation (EU) 2016/679, 2016). It has also been present in the national data protection regulation in Germany and was included in various sectoral regulations related to electronic data processing (Federal Act on Registration, Federal Act on Civil Status are only a few examples, already mentioned in this thesis). The requirement has been depicted in **Figure 7** with respect to Providing Service processes of data Processors and Sharing data, assigned to Controllers.

According to Art. 23 of the Federal Act on Data Protection "public bodies are allowed to process data for other purposes", in case the processing clearly corresponds to the interests of the data subject (Federal Data Protection Act – BDSG, 2017). In doing so, public bodies are allowed to transfer personal data to other authorities while they clearly state the purpose of their request and comply with this purpose, as stipulated by Art 25. (Federal Data Protection Act – BDSG, 2017). One of the ways to comply with purpose specification is offered by Art. 6 of the EU General Data Protection Regulation: "for further processing, compatibility check must be conducted, which includes checking 1) the link between the original and proposed new purposes, 2) context in which data were collected, 3) nature of data, 4) consequences of processing, 5) existence of safeguards including encryption or pseudonymization" (Council Regulation (EU) 2016/679, 2016). **Figure 7** displays the processes, underlying actions of responsible authorities as

Processors, and as Controllers in ensuring purposeful processing (Define purpose and necessary data, Request data necessary) and sharing of personal data (Check Purpose Compatibility).

Data Minimization. Art. 5 of GDPR stipulates concerning data handling that "personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed", thus, fully integrating the term data minimization in regulating data use (Council Regulation (EU) 2016/679, 2016). Possible measures to ensure minimal use of personal data in the processing are highlighted in Art. 71 of the Federal Act on Data Protection, according to which "the controller, both at the time the means of processing are determined and at the time of the processing itself, shall take appropriate measures to implement data protection principles, such as data minimization, in an effective manner, to ensure compliance with legal requirements and to protect the rights of data subjects. In doing so, the controller shall take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the legally protected interests of the data subject posed by the processing. In particular, personal data shall be processed, and processing systems shall be selected and designed in accordance with the aim of processing as

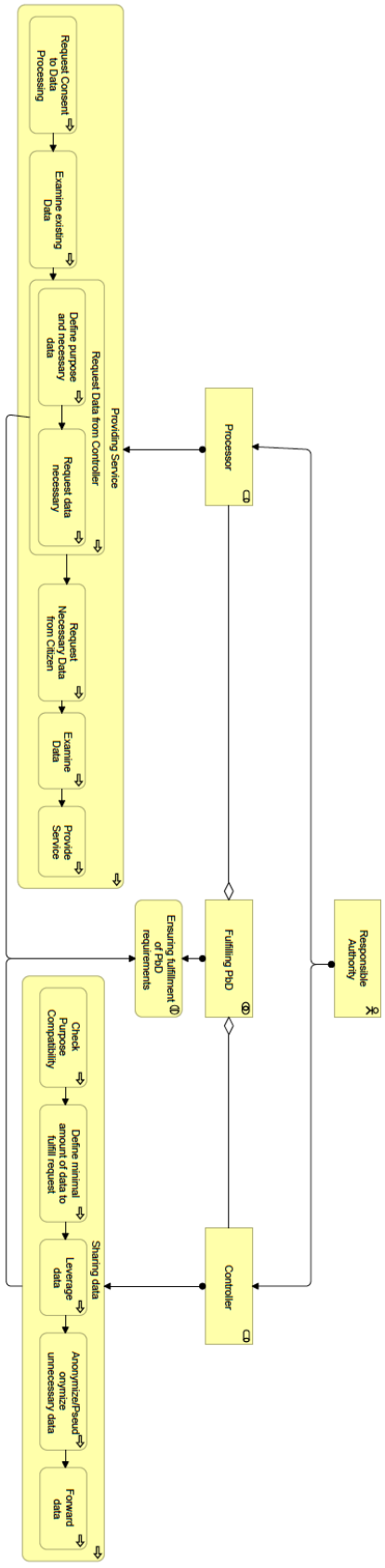


Figure 7. Purpose specification.

few personal data as possible. Personal data shall be rendered anonymous or pseudonymized as early as possible, as far as possible in accordance with the purpose of processing" (Federal Data Protection Act – BDSG, 2017). Although it appears difficult to find an application example for measures of data anonymization and pseudonymization in relation to provided digital public services, these measures have still been implemented in the core data Controller's processes (Define minimal amount of data to fulfill the request, Anonymize/Pseudonymize unnecessary data) and depicted in **Figure 8** (Anonymized/Pseudonymized Data, realizing the File with minimized data).

Art. 25 of GDPR also points out that "the controller shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons" (Council Regulation (EU) 2016/679, 2016), identifying the need for authorized access to personal data from the side of authorities, already mentioned in the subsection Transparency in Assigning Roles and Responsibilities of Parties to the Process in Enabling the OOP.

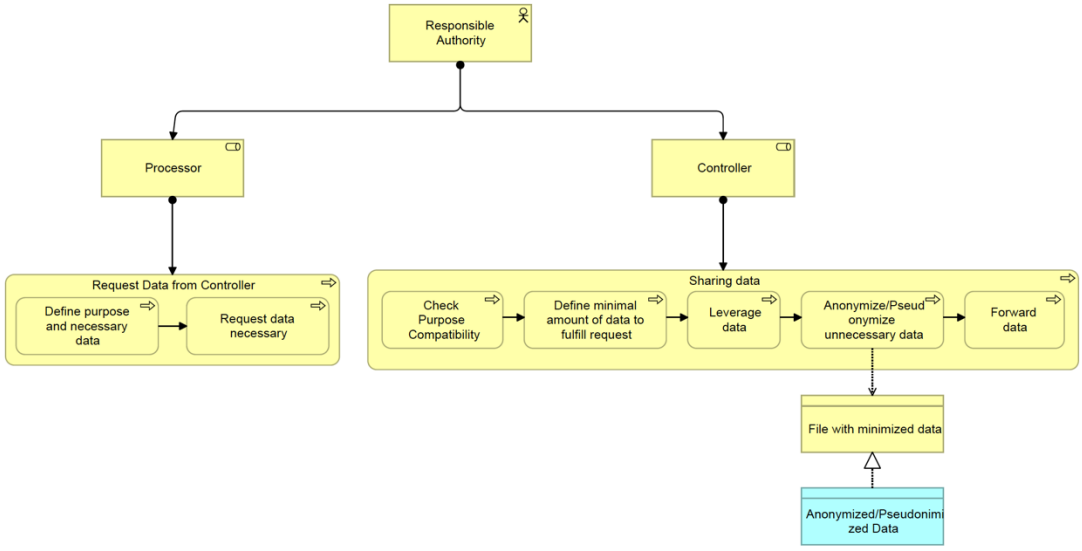


Figure 8. Data minimization.

Accountability and Confidentiality of Data Controllers and Processors. Overall, the GDPR places the responsibility for lawful and fair data processing with the Controller, who should also be able to demonstrate compliance with the provisions stipulated by Art. 5 of the EU General Data Protection Regulation (Council Regulation (EU) 2016/679, 2016). As suggested by Art. 30 of the GDPR, demonstrating compliance could be enabled through the record-keeping of the Controller or Processor (Organize and save records of the procedure, as part of the Public Administration Employee's process of Facilitating Service Provision, depicted in **Figure 9**): "each controller and, where applicable, the controller's representative, as well as each processor, or processors representative, shall

maintain a record of processing activities under its responsibility" (Council Regulation (EU) 2016/679, 2016).

While it is hard to operationalize processes, underlying the exercise of accountability, **Figure 9** reflects the precautions measures outlines in the Federal Act on Data Protection. Art. 64 stipulates that "the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. The controller shall take into account the relevant Technical Guidelines and recommendations from the Federal Office for Information Security: Restriction of Read and Write rights, implementation of electronic signatures and stamps (compatible with crypto concept), documented assignment of rights and roles, processes to ensure data accuracy, process guidelines and risk assessment of functionality, security and intrusion detection" (Federal Data Protection Act – BDSG, 2017). These measures, depicted within the process of Ensuring Data Security (Put in Place Continuous Risk Assessment, Implement Mitigation Measures and Carry Out Continuous Risk Assessment) with the full list of mitigation measures retrievable from the Technical Guidelines from the Federal Office for Information Security (Technical Guidelines FOIS) have been depicted in **Figure 9** as part of the processes, performed by the Controller.

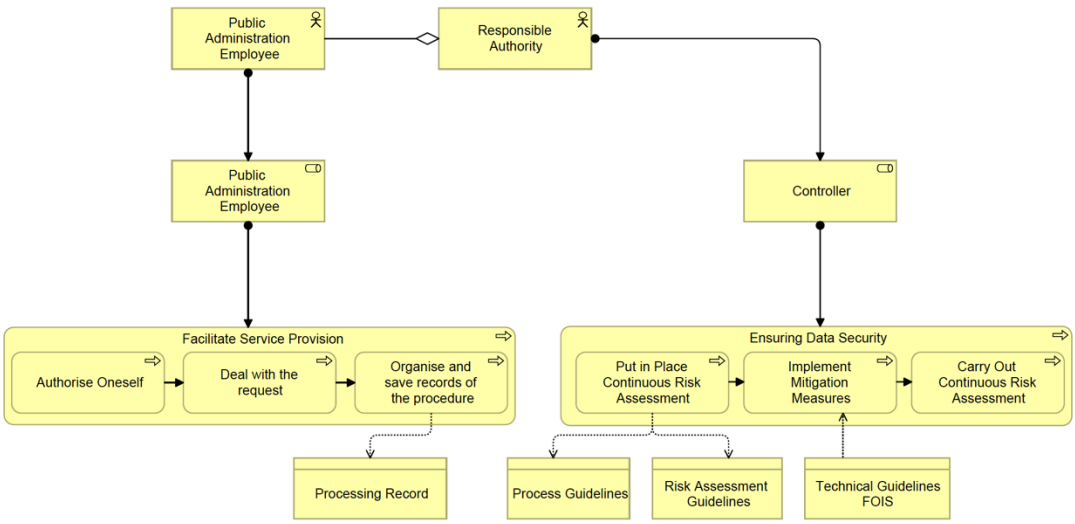


Figure 9. Accountability and confidentiality of data controllers and processors.

Access to Information about Collected and Stored Data. The GDPR stipulates through Art. 13 that "data subjects have the right to know what data are being held that pertain to them. Data controllers are obliged to provide information on: the controller, the purpose of the processing; the categories of data processed; the recipients of the data; the envisaged retention period; the individual's rights of rectification and erasure; the source of the data; and any regulated automated decisions made on the basis of the data" (Council

Regulation (EU) 2016/679, 2016). As suggested in **Figure 10**, this could be integrated into the communication of citizens (Users) and authorities (Controllers) on the OSG portal, with the Controller using Processing Records, produced over time by employees of the responsible authority, handling personal data, to deliver this information. Using the OSG portal would enable smooth transmission of "information enabling the data to be located", excluding the refusal of providing such record by public authority due to an effort of providing this information being "disproportionate to the data subject's interest in the information", as indicated in Art. 34 (Federal Data Protection Act – BDSG, 2017). The Federal Act also prescribes the requirement of enabling users' right to information about personal data processing on Data Protection, excluding the provision of information on the planned use of data (Art. 32), which is also not covered in the model of **Figure 10** (Federal Data Protection Act – BDSG, 2017).

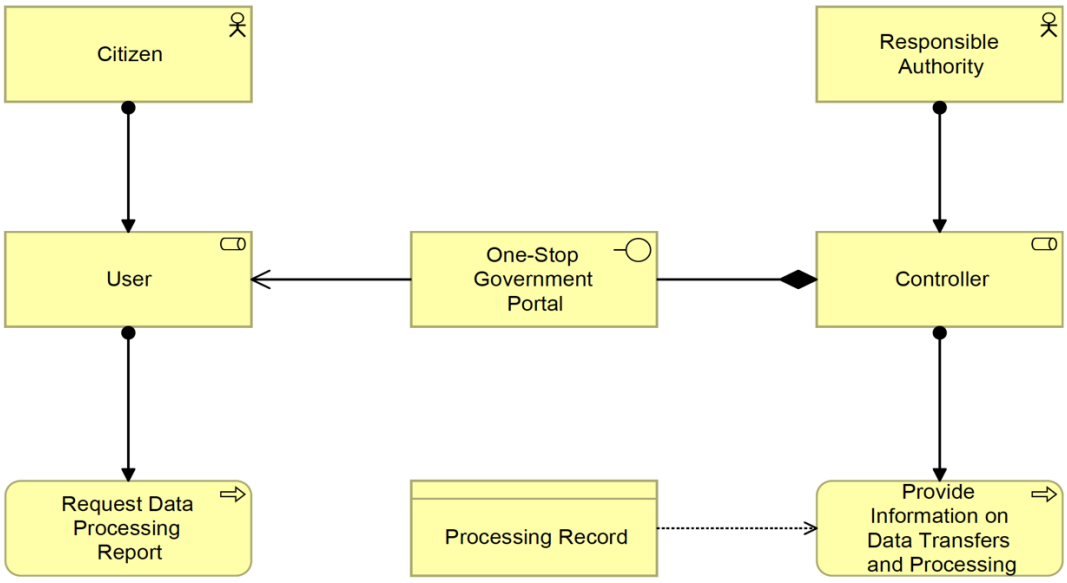


Figure 10. Access to information about collected and stored data.

Accuracy and Data Quality. Although much emphasis in the literature is put on ensuring data accuracy in processing data by public authorities in eGovernment literature, it is disproportionate to the regulatory measures taken to ensure the quality of stored data. Art. 5 of the EU General Data Protection Regulation only mentions the need for safeguarding data accuracy, stating that "data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay" (Council Regulation (EU) 2016/679, 2016). While relying on the regulation, the architectural blueprint could not go beyond these requirements and, with respect to data accuracy, only adds the "Conduct regularly Accuracy Checks", as **Figure 11** reflects.

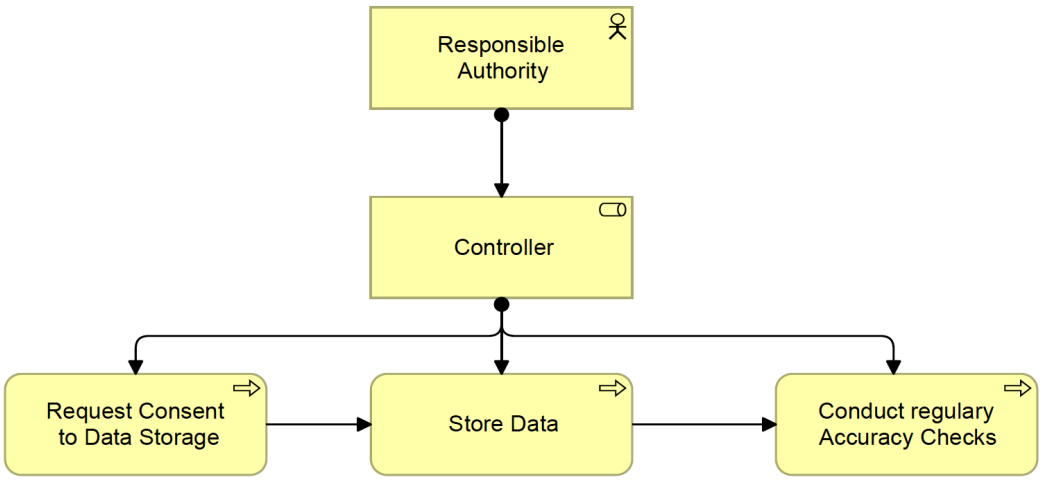


Figure 11. Accuracy and data quality.

Controllability of Available Data by Data Subjects. Although there are no regulatory provisions that deal explicitly with data controllability, the regulation often mentions ensuring the core right of the User to erase, or block, his or her data. Therefore, data controllability will be revealed in this thesis in the context of erasure and blocking stipulations. Such right is also provided for directly by the Online Access Law, the Art. 8 of which prescribes that "in the case of permanent storage, the user must have the possibility to delete the user account and all stored data independently at any time" (Onlinezugangsgesetz – OZG, 2017). In Figure 12, the OZG-requirement regarding the deletion of user accounts has been reflected by the processes Delete Account on the side of the User and Fulfill Account Deletion on the side of Responsible Authority.

The right of the User to have his or her data deleted is, furthermore, protected by the GDPR, which with Art. 17 provides for the data subject's right to "obtain from the controller the erasure of personal data without undue delay" (Council Regulation (EU) 2016/679, 2016). Furthermore, according to the GDPR's Art. 18, "the data subject shall have the right to obtain from the controller restriction of processing where … data is inaccurate, data is not needed for processing, but needed for exercising subject's rights" (Council Regulation (EU) 2016/679, 2016). Any rectification of this right must be communicated by the controller, as stipulated by Art. 19 of the EU General Data Protection Regulation (Council Regulation (EU) 2016/679, 2016). Finally, communication means need to ensure the right of the data subject "to object, on grounds relating to his or her particular situation, at any time to processing of personal data", as prescribed by Art. 20 (Council Regulation (EU) 2016/679, 2016).

Nevertheless, it is pointed out in Art. 35 of the Federal Act on Data Protection that "if in the case of non-automated data processing erasure would be impossible or would involve a disproportionate effort due to the specific mode of storage and if the data subject's interest in erasure can be regarded as minimal, the data subject shall not have the right to erasure and the controller shall not be obligated to erase personal data, restriction shall be applied instead" (Federal Data Protection Act – BDSG, 2017). Therefore, for the purpose of ensuring full compliance with the GDPR provisions is it important that technical means, underlying data controllability rights of citizens, minimize the effort in erasing and disabling processing of personal data. On the level of respective administrative procedures, data controllability by the User (Erase or Block Data) in communication with the Controller (Fulfill Data Erasure or Blocking) over the OSG Portal is depicted in **Figure 12**.

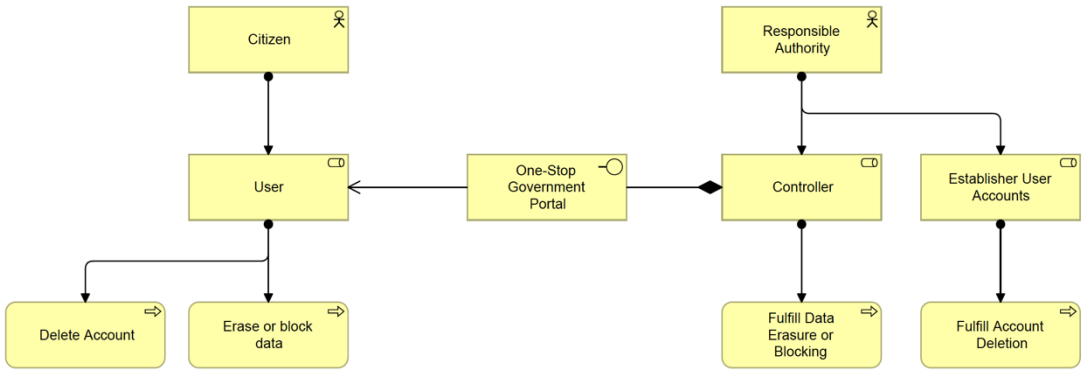


Figure 12. Controllability of available data by data subject.

Consent of Data Subjects to Data Use. Finally, obtaining the consent of the user for data collection, storage and processing is central to both the EU General Data Protection Regulation and the Federal Act on Data Protection. It also underlies all of the processes, enabling the realization of the Once-only Principle. More precisely, Art. 8 of the OZG covers the requirement to obtain citizen's consent to store data (reflected in the model in **Figure 13** for the Request Consent to Base Data Storage process of the Controller): "with the consent of the user, permanent storage of the identity data and its transmission to and use by the authority responsible for the Administrative Service is permitted" (Onlinezugangsgesetz – OZG, 2017), while Art. 5 of the Act to Promote Electronic Government highlights the consent requirement in data sharing: "with the consent of the data subject involved in the procedure, the competent authority may electronically obtain the necessary evidence directly from the issuing public body" (E-Government Act – EgovG, 2013).

Indeed, “all data processing shall be carried out under consent of the data subject. The controller must provide information on: the legal basis for processing the data; the period for which the data shall be retained; the individual’s right to complain to the Information Commissioner’s Office; whether providing the data is required by statute or contract; and the consequences of not providing the data”, which is prescribed by Art. 6 of GDPR and is reflected in the Processor’s task of Request Consent to Data Processing (Council Regulation (EU) 2016/679, 2016). It is vital to ensure that the consent can be revoked by the user, and the Controller must be able to demonstrate a justification for processing at any time, according to Art. 7 of the EU General Data Protection Regulation (Council Regulation (EU) 2016/679, 2016). The communication of consent has also been attached to the use of the OSG portal, as reflected in **Figure 13**.

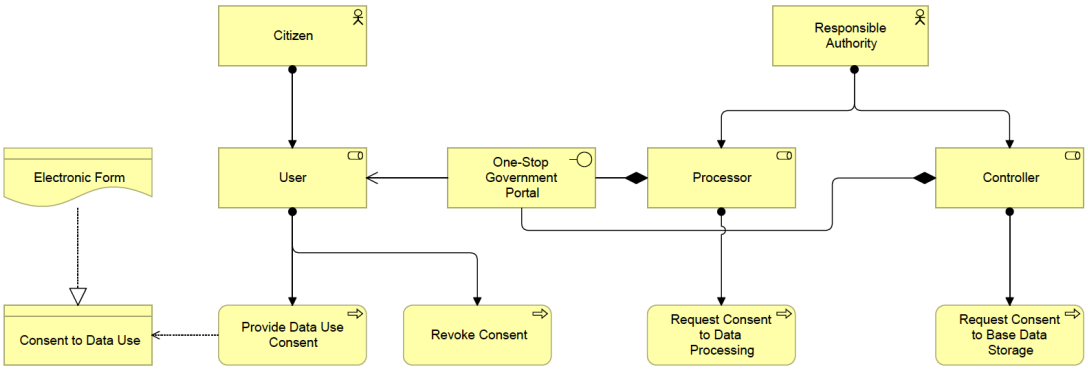


Figure 13. Consent of the data subject.

7 Solution Demonstration.

The created architectural blueprint, focused on the implementation of administrative processes within eGovernment services, provided via a One-stop government portal, and aligning the realization of the OOP and the PbD principles, is intended to serve as a guideline to process and information systems architects. It is designed in a way to serve as a general guideline, which is detached from the state or municipality specific eGovernment services, as well as from the field-specific administrative procedures. Nevertheless, due to the generic nature of the selected regulatory stipulations to create the blueprint, the author assumes its applicability in any specialized procedure to ensure that citizens receive digital government services. This section serves as a demonstration of the created artifact, including scenarios of its application in various field-specific procedures and state-specific jurisdictions.

The key concepts applied in this section correspond to those modeled in the architectural blueprint. The Responsible authorities are attached to the specific administrative bodies and play the roles of the Controllers and the Processors, dealing with the citizen data. Users in the context of this thesis are viewed primarily as citizens, willing to receive digital administrative services. The One-stop government portal, which does not find application in the digital administrative services, keeps the general name of the “One-stop government portal”. It should not be understood as the integrated portal network currently under development under the Online Access Law in Germany.

The key processes, assigned to particular roles, have been defined as follows:

1) *Controller:*
   a. Sharing data (Check purpose compatibility => Define minimal amount of data to fulfill the request => Leverage requested data => Anonymize/Pseudonymize unnecessary data => Forward data),
   b. Request consent to base data storage,
   c. Store base data,
   d. Ensuring data security (Put in place continuous risk assessment => Implement mitigation measures => Carry out continuous risk assessment),
   e. Provide information on data transfers and Processing,
   f. Conduct regular accuracy checks;
2) *Processor*:
   a. Providing Service (Examine existing data => Retrieve base data => Request data from controller => Request data from citizen (Define purpose and necessary data => Request data necessary) => Examine data => Provide service),
   b. Provide information on activities and responsibilities,

c. Request consent to data processing;

3) *Public Administration Employee*:

a. Facilitate Service provision (Deal with the request => Organize and store records of the procedure).

7.1 Scenario 1: Life Event Birth.

The first digital administrative service, demonstrated in this section, is the application for child benefits. The authorities often view this digital administrative service as exemplary in highlighting the user benefits in using digital government in Germany. Its application in Austria frames the target vision for implementing the OOP in German eGovernment (Hunnius, 2017). The selection of the child benefit application service in promoting the benefits of the Once-only principle in Germany is often explained by the high level of bureaucratic burden, associated with receiving child benefits.

To begin with, to obtain the service, the User (parent) uses her or his Service account to authenticate her or himself on the OSG. In order to be able to enable the storage function, the User needs to have an eID function activated on the ID card. The storage medium of eID will allow the application of all supporting documents, issued digitally, to the application file, in case they are needed.

Then the User fills out the application form for the child benefits, filling out the fields “Payment details” and having the personal details filled out automatically from the Service account. The User gives his or her consent to data processing and data transfer by checking the boxes. The User's consent is transferred to all parties involved: the processors and the controllers.

The Institution, responsible for paying the child benefit at the Employment Agency (the Processor) examines the application submitted and the data existing in the citizen file (e.g. application filled out for other children). It defines the minimal amount of data to be requested from other authorities, defining the purpose as “Assessing citizen application to child benefits”. The Processor requests the digital birth certificate and the details on the marriage partner from the Registry office (Controller A) in the place of birth, as well as the tax ID from the responsible tax authority (Controller B), respectively. Based on the data exchanged, the Institution responsible for paying the child benefit at the Employment Agency checks whether further data needs to be requested from the citizen and requests it. Having checked the eligibility of the User, the Institution, responsible for paying the child benefit at the Employment Agency, provides the requested service. The same procedure applies to the yearly request for child benefit, which the parents have to submit to the responsible authority. The activities of the Institution, responsible for paying the

child benefit at the Employment Agency, connected to data sharing and application processing, are published on the website of the authority and are publicly accessible.

Acting as the Controller A, the Registry office has the child details, submitted at the time of requesting the birth certificate and the child residence registration. This data is further recorded as the base data in the base registries (interlinked with e.g. the tax ID of a child, which is generated at time of the residence registration) upon the consent of the parents. The Controller A receives a request from the Institution, responsible for paying the child benefit at the Employment Agency, and checks the purpose compatibility with previously obtained consent of the User. The controller checks the minimal amount of data needed to fulfill the request and forwards this data to the processing authority. This procedure is recorded by the public sector employee in the log file and shared with the User in case the record is requested. The controller should ensure the accuracy of the data.

All authorities involved have a continuous risk assessment procedure in place and implement risk mitigation measures, whenever they apply (e.g. end-to-end encryption in data sharing to prevent the data "becoming available to an indefinite number of persons" (Council Regulation (EU) 2016/679, 2016; Federal Data Protection Act – BDSG, 2017)).

7.2 Scenario 2: Building Permit.

The services included in the field "Building and Living" are considered to be assigned high priority in the implementation of the Online Access Law (Stocksmeier & Hunnius, 2018). Similarly, all administrative services, connected to Building, have received high priority in the OZG implementation in the state of North-Rhine Westphalia (Willkommen zur Informationsveranstaltung zum Onlinezugangsgesetz, 2019). For this reason, the state has been actively developing centralized solutions to enable the digital public services, connected to the thematic area of "Building and Living". One of them is the specialized state-wide portal to apply for a building permit and to request several other related services, which can be integrated into all municipalities' administrative procedures in North-Rhine Westphalia (Willkommen zur Informationsveranstaltung zum Onlinezugangsgesetz, 2019). The second scenario was developed based on knowledge gathered in the development of this portal, relying on the Architectural blueprint.

As in the case with the previous scenario, the User (the owner or the architect) identification and authentication on the One-stop government portal is carried out through the Service account. The User has the eID function activated, which means they can not only identify themselves on the OSG portal but can also store relevant documents, using the storage function of the eID application infrastructure. The storage medium is especially relevant for the architect, who could use the portal to exchange construction

documents with parties to the proceedings, independent of the approval procedure (Digitales Baugenehmigungsverfahren NRW, 2019).

The User fills out the application form and is not expected to transmit the data for a second time to receive similar services, or services requiring the same types of data, or to transfer any data to other authorities. Digital building templates are accepted, administrative services and courts are involved, and decisions are made available digitally. The building application includes the following data as an input: data about the applying person, authorization to present building documents, data about the property, data about the construction plans, applicable exemptions and variations in construction obligations, which can be filled out by the User in less detail, as the data will be requested from other authorities. The consent form is included in the application, and the purpose is presented transparently with respect to data sharing.

The Construction Supervision Authority 1, acting as a Processor, is responsible for providing the service. It examines the existing data, retrieves base data to provide identification to the Controller A, which is sharing data on the person to receive the building permit with the Processor. In requesting data, the Processor should indicate the purpose of data use and list the metadata requested. Upon receiving all requested information inputs from other authorities, the Processor determines whether further information should be requested from the applicant via the OSG portal and proceeds to examining the application and making a decision. The Processor makes information on its activities and state transfers publicly available at all times on its website.

Acting as a Controller A, the Construction Supervision Authority 2, which received the request, conducts a purpose compatibility check, which can be inferred from the Processor request and the User Consent, provided at the time of submission. The Controller A forwards the minimal amount of data necessary to fulfill the request (address and contact details of the entity, contact person to receive the construction permit in case of a legal entity). It also conducts regular accuracy checks of the kept data. The information about the data transfer “Controller A – Processor” is recorded by the employee of the Construction Supervision Authority 2, dealing with the request and can be provided upon request of the User via the OSG portal.

The Processor also requests additional information on the property in question to support the application. This information can be provided by the Surveying and Cadastral Administration, or the Controller B. The Controller B checks data compatibility (against the purpose of request) and selects the minimal amount of data necessary to fulfill the request (address of the property/properties, while data about the owner is not needed and needs to be anonymized) and anonymizes the data about the property, forwarding it to the

Processor. The information about the data transfer “Controller B – Processor” is recorded by the Surveying and Cadastral Administration employee and can be provided upon request of the User.

Finally, as a framework activity of handling this application, all responsible authorities involved have the data security measures in place (Controller 1 and 2, Processor).

All in all, being just two of the 575 services to be launched digitally under the Online Access Law, these two services demonstrate the application of the developed artifact. It is worth highlighting that the demonstration is not meant to be part of the evaluation and serves only to the purpose of exemplifying the blueprint application in the field and state-specific administrative procedures. While these two services are selected out of high priority digital services, according to the implementation plan for the Online Access Law (Digitalisierungsprogramm IT-Plannungsrat, n.d.), they are by no means sufficient to conduct a full-scale evaluation of the digital service delivery on the subject of compliance with the Once-only and the Privacy by design principles.

8 Discussion.

This thesis can be viewed as a significant research contribution both from academic and practical perspectives. On the one hand, this work bridges the gap in understanding the operational meaning of the Once-only and Privacy by design principles by consolidating requirements that are suggested by academia in the area of eGovernment and data protection research. While previous research and practice have been highly influenced by the need to explain the "What" of the OOP and the PbD, by creating the terminology and gathering empirical support to present the meaning of these two principles, this thesis has focused on explaining the "How" of the Once-only and Privacy by design principles.

On the other hand, this research is designed to increase the understanding of the One-stop government portal development opportunities in Germany, compliant with the national and EU-level regulatory requirements of the Once-only and the Privacy by design principles. The developed artifact provides guidance to designing processes and services, which take into consideration data protection imperatives and enable user-friendly digital administrative services, with a citizen providing the same information to responsible authorities only once. It utilizes existing regulation and translates regulatory stipulations into an enterprise architecture language that is understandable by practitioners and information systems researchers. Moreover, it builds on the existing eGovernment infrastructure in Germany and inscribes its developments into a broader context of the European Union policies with respect to eGovernment. Thus, it allows assigning policy priorities to further development and promotion of acceptance of the German eGovernment tools.

Nevertheless, this work has been confronted with several limitations that need to be addressed to complete the contribution to the academic discourse. These limitations are dictated both by the initial research scope, defined by the author for this thesis, as well as by the selected methods to extract the artifact design requirements. This section will, therefore, be dedicated to addressing and discussing these limitations in further detail.

To begin with, in this work, the author has defined the OOP and the PbD as principles of a regulatory nature, fulfilling which, by extracting regulatory requirements is sufficient. Nevertheless, as a search for appropriate regulation to cover the requirements of the OOP shows, the regulation might not sufficient. Therefore, there is a clear need for further exploration and definition of the essence of "principle" in the context of the OOP.

In addition, the alignment of the Once-only and the Privacy by design principles in the German eGovernment context in this work is based on the assumption that a One-stop government portal will be the ultimate national solution to fulfill the requirements of the

EU Single Digital Gateway regulation. This assumption is also supported by the information provided by the IT Planning Council. According to it, carrying out the portal integration policy is motivated by the fact that the integrated portal network could pave the way towards the implementation of the Single Digital Gateway regulation in Germany (Das Single Digital Gateway der Europäischen Union, n.d.). A similar suggestion comes from one of the interview partners of Scholta et al. (2019b), representing the federal government – portal integration should be discussed as an enabler of an OSG portal in Germany. Nevertheless, such suggestions preserve a speculative nature and have not been confirmed by government officials. Moreover, the National Norm Controlling Council (2019) suggests the integrated portal network to be an inferior solution compared to the OSG portal, implying that these two solutions are separate.

Simultaneously, there is a clear official commitment to enabling the Once-only principle (Hunnius, 2017) (and even going beyond the OOP 1.0 and enabling the OOP 2.0 (Digitale Verwaltung und öffentliche IT, 2018). As shown in the literature review of this thesis, the OOP is rather applicable in the context of the One-stop government portal implementation. Precisely this policy development serves as a basis for accepting the OSG introduction assumption. It is true that the Once-only principle is an enabler of the OSG portal development, and the OSG portal development is not a precondition for implementing the OOP. But how can citizens apply for administrative services and share their information “only once”, if the single-entry point – the integrated portal network – redirects them to multiple portals for different administrative processes? Based on this confusion, created by the official discourse, the author concludes that there is a lack of understanding of the Once-only principle, its enablers, and application in the German eGovernment policy-making circles. From the research side, it remains unclear how the implementation of the OOP can be successful outside of the OSG scope and whether it is possible altogether. For this reason, there is a need for a broader OOP discussion in the international research perspective, indicating all possibilities for the integration of the Once-only principle into various national eGovernment contexts.

Having noted the limited understanding of the Once-only principle among the eGovernment policymakers, it is also worth highlighting the broader need for understanding the meaning of the EU policies and regulations in the area of eGovernment concerning German digital administrative services. It includes the electronic identification schemes, which are crucial for the implementation of the Single Digital Gateway regulation, cross-border exchange of information and personal data (such as via Internal Market Information System (IMI), as highlighted in the SDG regulation), and EU-financed projects and produced reusable solutions, such as those, offered by the Connecting Europe Facility program.

Furthermore, this work is based on another assumption: that ensuring compliance with the Once-only and the Privacy by design principles can be understood in terms of compliance with the existing regulation. Indeed, both the application of the OOP and the PbD is prescribed by the EU regulation: the Single Digital Gateway regulation and the General Data Protection Regulation, respectively. However, while the understanding of Privacy by design has been maturing in research and practice for over a decade (since being addressed in Cavoukian (2009)) and precise requirements could be easily identified in the text of the regulation, the understanding of the implementation of the Once-only principle is still evolving, and its regulatory underpinnings are still in the process of formulation. Especially in Germany in case of the 4) Interconnected base registries requirement, where the need for interconnection has been well-understood and the recommendations for enabling the interconnection have been presented to the policy-makers by the National Norm Controlling Council (2017) the enactment of the regulatory basis for this requirement is still in progress. This regulatory gap suggests that the architectural blueprint, created in this design science project, is not complete and cannot be completed using the legal specification method within the scope of this thesis.

Pointing out the missing link in the federal regulation in enabling the OOP, it is also worth mentioning that the concept of registry interconnection has not reached an advanced stage in Germany. According to the study of the National Norm Controlling Council (2017) there are examples of registry modernization policies in Austria and Switzerland, which could set an example for Germany. However, Germany would need to face several political, organizational, and technical challenges to enable the registry modernization (National Norm Controlling Council, 2017).

With respect to regulating the registry landscape, which enables the eGovernment development, based on the Once-only principle, the European Commission suggests several good practices that could guide lawmakers. Firstly, the Commission suggests formalizing the equivalence of electronic and paper-based registries (present in the Federal Act on Civil Status, but more vividly exemplified in the Spanish and Belgian regulation). Secondly, it appears that formalizing cross-sectoral data sharing (as enabled through the regulatory principle in the Netherlands) plays an important role in enabling the OOP from the registry perspective. Thirdly, using technology-neutral non-proprietary standards and specifications is essential for regulating the interconnection of base registries (European Commission, 2016b).

An additional limitation of this work is dictated by the selected scope of the project, which excludes the evaluation of the proposed solution. Simultaneously, carrying out the evaluation is essential to assessing the utility of the proposed architectural blueprint in

the context of the design science research. This thesis has demonstrated the application of the architectural blueprint through two scenarios, which could provide the basis for the evaluation. Firstly, they could serve as a methodological basis for assessing artifact's utility (as suggested in the demonstration, the application of the architectural blueprint should be tested in the state-specific and area-specific administrative services). Secondly, they can serve as a template for conducting interviews and surveys with eGovernment professionals and with the public sector experts and researchers. Future research is required to assess the application of the artifact.

Furthermore, there is a need to place the addressed practical problem of lacking guidance on the OOP and PbD compliance into a broader eGovernment context. The connection between the understanding of Privacy by design in terms of both information systems and process design and privacy protection is just one of the examples. However, whether the PbD of information systems and processes is sufficient to address the privacy concerns of citizens remains unclear in current research. This issue is especially vital in the context of Germany, where privacy concerns are often viewed as the main hurdle to eGovernment use. Similarly, PbD is often viewed as just one part of the data protection policy equation, with remaining sets of requirements being vaguely defined. Therefore, scientific discussion around the role of the PbD in data protection compliant eGovernment services is needed.

Finally, the evaluation should include and be useful in delivering precise suggestions regarding the technology and the application architecture, underlying the OOP and the PbD compliant electronic service provision, which go beyond regulatory requirements. A vivid example of the need to extend the regulatory requirements through practitioners' opinion is given by the scarcity of the data accuracy principles. It is indeed a complicated task to fulfill – to ensure data accuracy while asking citizens to provide the same data only once and preserve citizen privacy by minimizing the amount of information accessed, stored, and shared by the authorities (Priisalu, Ottis, 2017). For this reason, a solution balancing the two principles and the possibilities for practical implementation needs to be developed, which might change the core structure for realizing some of the requirements, depicted in this architectural blueprint, developed based on regulation.

The evaluation could also include some particular technological solutions. The Federal Printing Office and the Finance Ministry of the State of Thuringia (the “Life-Chain” project) have developed a service accounts solution compliant with both OOP and PbD, while being built on blockchain (Sichere Lösung für Bürgerkonten nach dem “Once only”-Prinzip, 2018). Considering this solution could also have an impact on the proposed alignment of the Once-only and the Privacy by design principles. It could suggest changes

to underlying processes and services, as well as justify it. Alternatively, the blueprint itself could serve as a basis for the evaluation of the "Life-Chain" solution in Thuringia at a later stage and help assess whether the distributed-ledger technology adds value to the once-only administrative service provision and preserving citizen privacy.

Similarly, the architectural blueprint developed in this thesis could allow for a comprehensive evaluation of further federal initiatives, such as the Data protection cockpit. The project is expected to fill the gap in the functionality of service portals, allowing for greater transparency of data exchange among public administrations to citizens (Ministry of the Interior, Division V II 2, 2019). However, as shown in this thesis, ensuring respect for user privacy is a highly complex process. The introduction of a Data protection cockpit cannot ensure the fulfillment of purpose specification and data minimization requirements, and the solution itself cannot be regarded as sufficient.

All in all, there is no doubt that this thesis provides a significant contribution to understanding the possibilities for the OOP implementation in Germany. Even with its scope limitations it

1) It explains the connection between the supranational and German national eGovernment initiatives and points out the need to ensure compliance with the EU-level regulation,

2) suggests a list of operational requirements, fulfilling which is crucial for realizing the Once-only and the Privacy by design principles,

3) develops an architectural blueprint, which translates the EU and national legislation in a language of the enterprise architecture, which can lay the basis for further development of reference architectures, assessing existing OOP-solutions in the German eGovernment context and identifying the gaps in the regulatory environment.

9 Conclusion.

To sum up, the research goal of this thesis has been achieved. The author has created an **architectural blueprint of the data collection and data use processes in the federal One-stop government portal in Germany, based on the OZG-driven portal integration, to align and comply with the EU-wide Once-only and Privacy by design principles and regulatory requirements to implementing them.** The architectural blueprint developed in this thesis focuses on the digital public services, offered to citizens, and mainly represents the administrative processes, underlying the OOP- and PbD-based services. By means of the design science research methodology, combined with the legal specification method, the author has created a model, which integrates the strategic (Figure 1), organizational and technical aspects of an OSG portal in Germany, enabling the implementation of the Once-only and the Privacy by design principles.

Following the steps of the Pfeffer's (2007) design science research cycle, the author has in the first place identified the need for the architectural blueprint, which would address the issues of usability (the OOP) and respect for privacy (the PbD) in offering the eGovernment services. In the following step, the development of a solution aligning the two principles has been motivated by the complexity of the administrative structure in Germany and its lack of integration into the EU cross-border digital service provision, in particular – the Single Digital Gateway Regulation.

Furthermore, this thesis has identified the requirements for the Once-only and the Privacy by design principles, such as: 1) Data sharing; 2) Standardized interfaces and data formats; 3) Electronic identification; 4) Integrated base registries; 5) Transparency in assigning roles and responsibilities of parties to the process **for the OOP** and 1) Purpose specification and system segregation (if necessary) to fulfill the desired purpose; 2) Data minimization in collection and processing; 3) Accountability and confidentiality of data controllers and processors; 4) Controllability of available data by data subject; 5) Accuracy and data quality; 6) Access to information about collected and stored data; 7) Consent of data subject to data processing **for the PbD**. These requirements are based on previous research and project work in the EU countries, and have, thus, been assessed as relevant in this context. Moreover, the literature review has helped to identify a close connection between the implementation of the Once-only principle and the One-stop government portal. For this reason, the OSG has been chosen as a primary modelling concept in this thesis – the G2C interface for administrative e-services.

Following the identification of the requirements for the two principles, the thesis has classified the EU and the German national regulation, according to the regulatory provisions (articles) addressing these requirements. Based on classified regulatory

stipulations, the author has created models of each requirement, adopting the regulatory terms for key entities, objects and processes, such as the Responsible Authority, the Processor, the Controller, the Citizen and others. Modelled in the Archimate language, the requirements reflect the connection among participating entities and the supporting application infrastructure and services, which connect the organizational and technological aspects of the digital services. Subsequently, the author demonstrates the use of the architectural blueprint in the field specific administrative processes, overarching different administrative levels (application for child benefits), as well as the state-level field-specific processes (requesting building permit in state of North-Rhine Westphalia), showing how the application submission can be enabled through re-using data and safeguarding privacy through the proposed solution.

Finally, the author has discussed the limitations of the proposed solution, which are primarily concerned with possibilities for various applications of the Once-only principle and the opportunities for developing the One-stop government policy in Germany. Due to the underexplored nature of the Once-only principle application and an obscured vision of the future of the integrated portal network (as an independent solution, or as an intermediary solution on the way to a One-stop government portal) in Germany, it is difficult to predict the applicability of the architectural blueprint. What is, however, certain, is that independently of the OSG, the implementation of the Once-only principle requires a regulatory framework with respect to the integrated base registry landscape. Moreover, stronger focus should be put on guiding or regulating data accuracy assurance, especially in decentralized eGovernment systems, such as in Germany.

As far as research is concerned, more thorough understanding of the underlying "principles" in eGovernment is required to ensure their implementation. While this thesis has taken a regulatory approach to eGovernment principles, further work could show that the implementation of the OOP and the PbD principles is not as dogmatic in nature to propose other implementation guidelines. Additionally, more work is needed, highlighting the operational nature of the Once-only principle, including or surpassing the five requirements, outlined in this work. Finally, more comparative studies are needed in this field, which draw upon the similarities of administrative structures. As advanced as Estonia is in the eGovernment development, it cannot serve as an example for countries with federative administrative structures in all aspects of eGovernment implementation. Such approach is also desired for the evaluation of eGovernment progress in the EU and on the international scale.

References

- Act on Identity Cards and Electronic Identification (Personalausweisgesetz - PAuswG), Federal Law Gazette I, p. 1346. (18.06.2009 last amended 22.12.2011). Retrieved April 10th, 2020 from https://www.gesetze-im-internet.de/englisch_pauswg/englisch_pauswg.pdf
- Act to promote electronic government (E-Government Act - EgovG), Federal Law Gazette. I P. 2749 (25.07.2013). Retrieved April 10th, 2020 from http://www.gesetze-im-internet.de/englisch_egovg/englisch_egovg.pdf
- Akkaya C., & Krcmar H. (2018). Towards the Implementation of the EU-Wide "Once-Only Principle": Perceptions of Citizens in the DACH-Region. In *Parycek P. et al. (eds), Electronic Government*. *EGOV 2018. Lecture Notes in Computer Science, vol 11020.* Springer, Cham. Doi: 10.1007/978-3-319-98690-6_14
- Angelopoulos, K., Diamantopoulou, V., Mouratidis, H., Pavlidis, M., Salnitri, M., Giorgini, P., & Ruiz, J. F. (2017). A Holistic Approach for Privacy Protection in E-Government. *Proceedings of the 12th International Conference on Availability, Reliability and Security - ARES '17*. Doi:10.1145/3098954.3098960
- Basic Law for the Federal Republic of Germany (GG), Federal Law Gazette I p. 404. (08.05.1949, last amended 28.03.2019). Retrieved April 10th, 2020 from https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.pdf
- Baskerville, R., Pries-Heje, J., & Venable, J. (2009). Soft design science methodology. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology - DESRIST '09*. Doi:10.1145/1555619.1555631
- BMI, Referat O2. (n.d.). Minikommentar zum Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften. Retrieved March 10th, 2020 from https://www.verwaltung-innovativ.de/SharedDocs/Publikationen/Artikel/Minikommenta_EGov_Gesetz.pdf?__blob=publicationFile&v=1
- Brückmann T., & Gruhn V. (2010). An Architectural Blueprint for Model Driven Development and Maintenance of Business Logic for Information Systems. In *Babar M.A., Gorton I. (eds), Software Architecture. ECSA 2010. Lecture Notes in Computer Science, vol. 6285.* Springer, Berlin, Heidelberg, pp. 53-69.
- Bundesministerium für Wirtschaft und Energie. (n.d.). *Gestaltungsgrundsätze für den Einheitlichen Ansprechpartner 2.0.* Retrieved March 10th, 2020 from https://www.bmwi.de/Redaktion/DE/Downloads/G/gestaltungsgrundsaetze-fuer-den-einheitlichen-ansprechpartner-2-0.pdf?__blob=publicationFile&v=1
- Cave, J., Botterman, M., Cavallini, S., & Volpe, M. (2017). Once-Only Principle for citizens and businesses: Policy options and their impacts. European Commission,

Publication Office of the European Union, Luxembourg. Doi: 10.2759/393169.

- Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Information and privacy commissioner of Ontario, Canada, pp. 1-5.
- Cavoukian, A. (2011). Privacy by design in law, policy and practice. A white paper for regulators, decision-makers and policy-makers. Doi: 10.1080/13600869.2013.801580
- CEF Building Blocks presented at Releasing the Power of Procurement. (2019). In News, CEF Digital, last updated on 31.07.2019. Retrieved March 1st, 2020 from https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/05/07/CEF+Building+Blocks+presented+at+Releasing+the+Power+of+Procurement
- Cleven, A., Gubler, P., & Hüner, K.M. (2009). Design alternatives for the evaluation of design science research artifacts. In *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology, 19,* pp. 1-8. Doi:10.1145/1555619.1555645
- Colombo, P., & Ferrari, E. (2012). Towards a modeling and analysis framework for privacy-aware systems. In *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*, *IEEE, 2012, September*, pp. 81-90. Doi: 10.1109/SocialCom-PASSAT.2012.12
- Common architecture for the Single Digital Gateway. (2017). In ISA² - Interoperability solutions for public administrations, businesses and citizens, European Commission. Retrieved March 2nd, 2020 from https://ec.europa.eu/isa2/actions/common-architecture-single-digital-gateway_en.
- Computing, A. (2006). An architectural blueprint for autonomic computing. *IBM White Paper*, *31*(2006), pp. 1-6.
- Connecting Europe Facility. (n.d.). In *Innovation and Networks Executive Agency, European Commission.* Retrieved March 1st, 2020 from https://ec.europa.eu/inea/en/connecting-europe-facility
- Council Regulation (EU) 2015/884 of 8 June 2015 establishing technical specifications and procedures required for the system of interconnection of registers established by Directive 2009/101/EC of the European Parliament and of the Council. Official Journal of the European Union, L144, pp. 1-9.
- Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119, pp. 1-88.
- Council Regulation (EU) 2018/1724 of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012. Official

Journal of the European Union, L295, pp. 1-30.

- Council Regulation (EU) 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Official Journal of the European Union, L257, pp. 73-114.
- Cuijpers, C., & Schroers, J. (2014). eIDAS as guideline for the development of a pan European eID framework in FutureID. In *Hühnlein, D. (ed.), GI-Edition Lecture Notes in Informatics, Bonner Köllen Verlag, Bonn*, pp. 23-38
- Das Single Digital Gateway der Europäischen Union. (n.d). In *Portalverbund, OZG-Umsetzung, IT-Plannungsrat*. Retrieved February 20th, 2020 from https://www.it-planungsrat.de/DE/ITPlanungsrat/OZG-Umsetzung/Portalverbund/04_SDG/SDG_node.html
- De-Mail in der Bundesverwaltung: Empfehlungen des BfDI. (2013). In *Datenschutz Datensicherheit – DuD*, 37, pp. 404. Doi: 10.1007/s11623-013-0162-6
- De-Mail-Kriterienkatalog für den Datenschutz-Nachweis. (n.d.). In *Datenschutz, der Bundesbeauftragte für Datenschutz und Informationsfreiheit.* Retrieved March 10th, 2020 from https://www.bfdi.bund.de/DE/Datenschutz/Themen/Brief_Paket/DeMailInfosAnbieterArtikel/KriterienkatalogNachweis.html?cms_templateQueryString=De-Mail&cms_sortOrder=score+desc
- Demiri, L. (2018). Single Digital Gateway Regulation and the Once-only Principle. *6th Meeting of the Network on Public Administration and Governance, Heracleion.* Retrieved February 27th, 2020 from https://ec.europa.eu/esf/transnationality/filedepot_download/1671/2875+&cd=3&hl=ru&ct=clnk&gl=de
- Digitale Verwaltung und öffentliche IT. (2018). Der Staat als Digitalisierungsplattform: Once Only 2.0. Digital Gipfel, Nürnberg, 2018. Retrieved March 13th, 2020 from https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2018/p6-der-staat-als-digitalisierungsplattform.pdf?__blob=publicationFile&v=2
- Digitales Baugenehmigungsverfahren NRW. (2019). Abschlussbericht der 1. Projektphase, Partnerschaften Deutschland, MHKBG NRW. Berlin, 2019. Retrieved April 28th, 2020 from https://www.mhkbg.nrw/sites/default/files/media/document/file/Abschlussbericht_DigitalesBaugenehmigungsverfahren_NRW_1.Projektphase_270619.PDF
- Digitalisierungsprogramm IT-Plannungsrat. (n.d.). In *Leitfaden zum Digitalisierungsprogramm des IT-Planungsrates.* BMI, Referat DGII4, OZG-Leitfaden. Retrieved May 3rd, 2020 from https://leitfaden.ozg-umsetzung.de/pages/viewpage.action?pageId=4621615

- Djeffal, C. (2018). Künstliche Intelligenz in der öffentlichen Verwaltung. Bericht des NEGZ, Nr. 3. Berlin, 2018. Retrieved April 25th, 2020 from https://www.hiig.de/wp-content/uploads/2019/03/NEGZ-Kurzstudie-3-KuenstlIntelligenz-20181113-digital.pdf
- DSK. (2017). Datenschutz und Informationsfreiheit als Elemente einer stabilen Demokratie. In *Datenschutz Und Datensicherheit (DuD), 41(12),* pp. 761-764.
- E-Government-Gesetz. (n.d.). In *E-Government-Gesetz, E-Government, Moderne Verwaltung, Themen*. Bundesministerium des Innern, für Bau und Heimat. Retrieved March 20th, 2020 from https://www.bmi.bund.de/DE/themen/moderne-verwaltung/e-government/e-government-gesetz/e-government-gesetz-node.html
- eID-Strategie. (n.d.). In *Projekte, Maßnahmen und Anwendungen, IT-Planungsrat*. Retrieved March 10th, 2020 from https://www.it-planungsrat.de/DE/Projekte/Steuerungsprojekte/eIDStrategie/eID_strategie.html
- Entscheidung 2017/40 - Anwendung des Interoperabilitätsstandards XFall zur Übertragung von Antragsdaten. (2017). 24. Sitzung des IT-Planungsrats vom 5. Oktober 2017. Retrieved April 10th, 2020 from https://www.it-planungsrat.de/SharedDocs/Entscheidungen/DE/2017/Entscheidung_2017_40.html
- Entscheidung 2018/40 – Portalverbund. (2018). 27. Sitzung des IT-Planungsrats vom 25. Oktober 2018. Retrieved April 10th, 2020 from https://www.it-planungsrat.de/SharedDocs/Sitzungen/DE/2018/Sitzung_27.html?pos=4
- Entscheidung 2019/14 - XÖV-Standard für FIM: XProzess. (2019). 28. Sitzung des IT-Planungsrats vom 12. März 2019. Retrieved April 10th, 2020 from https://www.it-planungsrat.de/SharedDocs/Sitzungen/DE/2019/Sitzung_28.html?pos=14
- Entscheidung 2019/15 - XÖV-Standard für FIM: XDatenfelder. (2019). 28. Sitzung des IT-Planungsrats vom 12. März 2019. Retrieved April 10th, 2020 from https://www.it-planungsrat.de/SharedDocs/Sitzungen/DE/2019/Sitzung_28.html?pos=15
- European Commission. (2015). A Digital Single Market Strategy for Europe. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM/2015/0192 final.
- European Commission. (2016a). *EU eGovernment Action Plan 2016-2020: Accelerating the digital transformation of government.* Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM/2016/0179 final. Retrieved February 10th, 2020 from http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15268
- European Commission. (2016b). Access to Base Registries: Good Practices on

Building Successful interconnections of Base Registries. Luxembourg: Publications Office of the European Union, 2016. Retrieved March 31st, 2020 from https://ec.europa.eu/isa2/sites/isa/files/publications/access-to-base-registries-good-practices-on-building-successful-interconnections-of-base-registries.pdf

- European Commission. (2019). eGovernment Benchmark 2019. https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2019/10/eGovernment-Benchmark-Country-Factsheets.pdf
- European Interoperability Reference Architecture (EIRA) v3.0.0. (2020). Introduction to the European Interoperability Reference Architecture v3.0.0. In EIRA Solution, Joinup. Retrived March 1st, 2020 from https://joinup.ec.europa.eu/solution/eira
- Federal Act on Registration (BMG), Federal Law Gazette I p. 2745. (03.05.2013, last amended 18.07.2017). Retrieved April 10th, 2020 from http://www.gesetze-im-internet.de/englisch_bmg/englisch_bmg.pdf
- Federal Data Protection Act (BDSG), Federal Law Gazette I p. 2097. (30.06.2017 last amended 20.11.2019). Retrieved April 10th, 2020 from https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.pdf
- FIM Föderales Informationsmanagement. (n.d.). In *FIM-Portal*. Retrieved March 12th, 2020 from https://fimportal.de/
- Föderales Informationsmanagement (FIM) Infomationsveranstaltung. (2019). *FITKO, Föderales Informationsmanagement, Frankfurt am Main.* Retrieved March 12th, 2020 from https://fimportal.de/download-dokumente
- Föderales Informationsmanagement (FIM). (n.d.). In *Projekte, Maßnahmen und Anwendungen, IT-Planungsrat*. Retrieved March 12th, 2020 from https://www.it-planungsrat.de/DE/Projekte/Anwendungen/FIM/fim_node.html
- Föderales Informationsmanagement. (2017). FIM Baustein Prozesse, Fachkonzept. *Bundesministerium des Inneren, IT-Plannungsrat, Mecklenburg-Vorpommern. Version 01.00 – Stand 06. November 2017.*
- Frank, U. (2007). Evaluation of Reference Models. In *P. Fettke, P. Loos (Eds.) Reference Modeling for Business Systems Analysis*. IDEA Group, pp. 118-139.
- Fromm, J., Welzel, C., Nentwig, L., & Bieker, L. (2015b). Bürokratieabbau durch Digitalisierung: Kosten und Nutzen von E-Government für Bürger und Verwaltung. Retrieved March 13th, 2020 from http://www.uni-potsdam.de/fileadmin01/projects/ls-kuhlmann/NKR/151118_NKR-Gutachten_E-Gov_in_D_Dokumentation_Langfassung.pdf
- Fromm, J., Welzel, C., Nentwig, L., & Weber, M. (2015a). E-Government in Deutschland: Vom Abstieg zum Aufstieg. Retrieved March 13th, 2020 from http://www.oeffentliche-it.de/documents/10181/14412/E-

Government+in+Deutschland

- Gasmelseid, T. (2006). Multiagent Web based Decision Support Systems for Global Enterprises: An Architectural Blueprint. *Engineering Letters, 13(2), IGI Global, Hershey, PA,* pp. 173-184.
- Geschäfts- und Koordinierungsstelle 115. (2019). Behördennummer 115, Ihr kurzer Draht ins Amt. Bundesministerium des Innern, für Bau und Heimat, Berlin. Retrieved March 5th, 2020 from https://www.115.de/SharedDocs/Publikationen/Service_Publikationen/Infomaterialien/flyer_behoerdennummer.pdf?__blob=publicationFile&v=2
- Gesetz über eine Karte für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums mit Funktion zum elektronischen Identitätsnachweis (eID-Karte-Gesetz - eIDKG), BGBl. I S. 846. (01.11.2019). Retrieved April 10th, 2020 from https://www.buzer.de/eID-Karte-Gesetz.htm
- Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz - OZG), BGBl. I S. 3122, 3138 (14.08.2017). Retrieved April 10th, 2020 from https://www.gesetze-im-internet.de/ozg/OZG.pdf
- Glassey, O. (2002). A One-Stop Government Prototype Based on Use Cases and Scenarios. In *Traunmüller R., Lenk K. (eds), Electronic Government*. EGOV 2002. Lecture Notes in Computer Science, vol. 2456. Springer, Berlin, Heidelberg.
- Glassey, O. (2004). Developing a one-stop government data model. *Government Information Quarterly, 21:2,* pp. 156-169. doi: 10.1016/j.giq.2003.12.012
- Gluhak, A., Hauswirth, M., Krco, S., Stojanovic, N., Bauer, M., Nielsen, R., ... & Corcho, O. (2011). An architectural blueprint for a Real-World Internet. *The Future Internet Assembly, Springer, Berlin, Heidelberg*, pp. 67-80.
- Gouscos, D., Kalikakis, M., Legal, M., & Papadopoulou, S. (2007). A general model of performance and quality for one-stop e-Government service offerings. *Government Information Quarterly, 24:4,* pp. 860-885. Doi: 10.1016/j.giq.2006.07.016
- Gregor, S., & Hevner, A. (2013). Positioning and Presenting Design Science Research for Maximum Impact. *Management Information Systems Quarterly, 37*(2), pp. 337-355.
- Gürses, S., Troncoso, C., & Diaz, C. (2011). Engineering privacy by design. *Computers, Privacy & Data Protection*, *14(3),* pp. 1-27.
- Häufig Nachgefragt De-Mail. (n.d.). In *De-Mail, E-Government, Moderne Verwaltung, Themen*. Bundesministerium des Innern, für Bau und Heimat. Retrieved March 10th, 2020 from https://www.bmi.bund.de/SharedDocs/faqs/DE/themen/it-digitalpolitik/de-mail/de-mail-liste.html
- Hauser, F. (2017). Quality of Public Administration, A Toolbox for Practitioners. *Publications Office of the European Union, Luxembourg,* pp. 132-133. Doi:

10.2767/483489

- Heeks, R. (2006). Implementing and managing eGovernment: An international text. *Sage Publications, London.*
- Hevner, A. (2007). A three cycle view of design science research. *Scandinavian journal of information systems, 19(2),* pp. 87-92.
- Hevner, A., March, S.T. & Park, J. (2004). Design Science in Information Systems Research. *Management Information Systems Quarterly, 28.* pp. 75-105.
- Holz, M., Icks, A., Levering, B., & Kasdorf, A. (2018). Reform der Einheitlichen Ansprechpartner (EA): Anregungen von europäischen Good-PracticeBeispielen, IfM-Materialien, No. 264, Institut für Mittelstandsforschung (IfM) Bonn, Bonn. https://www.econstor.eu/bitstream/10419/175343/1/1013893352.pdf
- Home. (n.d.). In *European e-Justice portal*. Retrieved March 1st, 2020 from https://e-justice.europa.eu/home.do?plang=en&action=home
- Hongbo, L. (2013). Model and architecture of one-stop government system: A solution of systemic interoperability. In *2013 6th International Conference on Information Management, Innovation Management and Industrial Engineering*, *IEEE, Vol. 1,* pp. 75-79.
- Hunnius, S. (2017). Das Once-Only Prinzip Potenziale für Bürger, Unternehmen und Verwaltung. IT Planungsrat, 26.04.2017. Retrieved April 20th, 2020 from https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Fachkongress/5FK2017/26April_II_once-only-prinzip.pdf?__blob=publicationFile&v=3
- ISA. (2015). ISA action 1.2 – State of play and next steps. Base Registries. European Commission. Retrieved March 7th, 2020 from https://ec.europa.eu/isa2/sites/isa/files/presentations/base-registries.pdf
- Jaeger, P. (2002). Constitutional principles and E-government: An opinion about possible effects of Federalism and the separation of powers on E-government policies. *Government Information Quarterly, 19(4),* pp. 357-368.
- Jonkers, H., Lankhorst, M., ter Doest, H., Arbab, F., Bosma, H., & Wieringa, R. (2006). Enterprise architecture: Management tool and blueprint for the organisation. *Information systems frontiers, 8(2),* pp. 63.
- Junk, M. (2009). Neuer Art. 91c GG: Die IT-Nutzung bekommt eine verfassungsrechtliche Grundlage – mit wesentlichen Folgen für die Beschaffung. In *Vergabeblog.de vom 24/05/2009, Nr. 2415.* Retrieved March 20th, 2020 from https://www.vergabeblog.de/2009-05-24/neuer-art-91-c-gg-die-it-nutzung-bekommt-eine-verfassungsrechtliche-grundlage-mit-wesentlichen-folgen-fr-die-beschaffung/
- Kalvet, T., Toots, M., & Krimmer, R. (2018). Contributing to a digital single market

for Europe. *Proceedings of the 19th Annual International Conference on Digital Government Research Governance in the Data Age - Dgo '18*, pp. 1-8. Doi: 10.1145/3209281.3209344

- Kohlborn, T. (2014). Quality assessment of service bundles for governmental one-stop portals: A Literature Review. *Government Information Quarterly, 31:2,* p. 221-228. Doi: 10.1016/j.giq.2013.10.006
- Kolain, M., & Wirth, C. (2018). Privacy by BlockChain Design: A BlockChain-enabled GDPR-compliant Approach for Handling Personal Data. *Reports of the European Society for Socially Embedded Technologies*, *2(6)*. Doi: 10.18420/blockchain2018_03
- Koops, B., & Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. *International Review of Law, Computers & Technology, 28*(2), pp. 159-171. Doi: 10.1080/13600869.2013.801589
- Krimmer, R., Fischer, D., & Schmidt, C. (2017b). Bürgerkonten und das Projekt The Once-Only Principle. *Public Government, Institut für den öffentlichen Sektor e. V. Herbst/Winter 2017*, pp. 12-15.
- Krimmer, R., Kalvet, T., Toots, M., Cepilovs, A., & Tambouris, E. (2017a). Exploring and Demonstrating the Once-Only Principle: A European Perspective. *Proceedings of the 18th Annual International Conference on Digital Government Research, 128275*, pp. 546-551.
- Kuechler, B., & Vaishnavi, V. (2008). On theory development in design science research: anatomy of a research project. *European Journal of Information Systems, 17(5),* pp. 489-504. Doi: 10.1057/ejis.2008.40
- Loi garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité et portant simplification et harmonisation des formulaires électroniques et papier. N-2014203384 P-42601. (04.06.2014). Retrieved April 10th, 2020 from http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2014050506&table%20_name=loi
- Martini, M., & Wenzel, M. (2017). „Once only" versus „only once": Das Prinzip einmaliger Erfassung zwischen Zweckbindungsgrundsatz und Bürgerfreundlichkeit. *Deutsches Verwaltungsblatt, 132(12),* pp. 749-758. Doi:10.1515/dvbl-2017-1206
- Ministry of the Interior, Division V II 2. (2019). Registerübergreifendes Identitätsmanagement als Teil der Registermodernisierung. *Zwischenbericht für die Innenministerkonferenz 4. - 6.12.2019.* Retrieved April 20th, 2020 from https://www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/2019-12-04_06/anlage-zu-top-32.pdf?__blob=publicationFile&v=2

- Mkude C., & Wimmer M. (2014). Strategic Aspects for Successful E-government Systems Design: Insights from a Survey in Germany. In *Janssen M., Scholl H.J., Wimmer M.A., Bannister F. (eds) Electronic Government. EGOV 2014. Lecture Notes in Computer Science, vol 8653. Springer, Berlin, Heidelberg.*
- Molnár-Gábor, F. (2018). Germany: a fair balance between scientific freedom and data subjects' rights? In *Human Genetics, 137(8),* pp. 619-626. Doi:10.1007/s00439-018-1912-1
- Nationaler Normenkontrollrat. (2017). Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren. Berlin, 2017. Retrieved April 10th, 2020 from https://www.normenkontrollrat.bund.de/resource/blob/72494/476004/12c91fffb877685f4771f34b9a5e08fd/2017-10-06-download-nkr-gutachten-2017-data.pdf
- Nationaler Normenkontrollrat. (2019). Monitor Digitale Verwaltung #3. Berlin, 2019. Retrieved March 15th, 2020 from https://www.normenkontrollrat.bund.de/resource/blob/72494/1675854/b0a14cedf388ddb05f2b9b9e3827b32d/2019-09-26-monitor-digitale-verwaltung-3-data.pdf
- Once Only Principle reduce administrative burden for individuals and businesses. (n.d.). In *CEF Digital Connecting Europe*. Retrieved March 1st, 2020 from https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Once+Only+Principle
- Otjacques, B., Hitzelberger, P., & Feltz, F. (2007). Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing. *Journal of Management Information Systems, 23(4),* pp. 29-51.
- Otto, P., & Anton, A. (2007). Addressing Legal Requirements in Requirements Engineering. *15th IEEE International Requirements Engineering Conference (RE 2007)*, Delhi, pp. 5-14.
- Pagallo U. (2012). On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law. In *Gutwirth S., Leenes R., De Hert P., Poullet Y. (eds), European Data Protection: In Good Health? Springer, Dordrecht*, pp. 331-346.
- Peffers, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems, 24(3),* pp. 45-77.
- Personenstandsgesetz (PStG), BGBl. I S. 1626. (19.02.2007, zuletzt geändert 20.11.2019). Retrieved April 10th, 2020 from https://www.gesetze-im-internet.de/pstg/PStG.pdf
- PG Digitale Verwaltung. (2014). Digitale Verwaltung 2020. Bundesministerium des Innern, Berlin. Retrieved March 5th, 2020 from https://www.verwaltung-innovativ.de/SharedDocs/Publikationen/Pressemitteilungen/programmdokument_div.pdf?__blob=publicationFile&v=5

- Pries-Heje, J., Baskerville, R., & Venable, J. (2008). Strategies for Design Science Research Evaluation. *ECIS 2008 Proceedings*, pp. 87. http://aisel.aisnet.org/ecis2008/87
- Priisalu, J., & Ottis, R. (2017). Personal control of privacy and data: Estonian experience. *Health Technology, 7,* pp. 441–451. Doi: 10.1007/s12553-017-0195-1
- Project MonLightGrid. (2019). *The Once and Only Principle implementation in the City of Monheim Am Rhein*. Detecon Consulting (June, 2019).
- Räckers, M. (2019a). eGovernment: Basics – Evolution in Germany. Presentation for ST2019 in the S0H15A Course, Selected Chapter: eGovernment. European Research Center for Information Systems, Münster.
- Räckers, M. (2019b). eGovernment: Examples, Success Factors and Hindrances. Presentation for ST2019 in the S0H15A Course, Selected Chapter: eGovernment. European Research Center for Information Systems, Münster.
- Riedel, J. (2019). Wie kommen wir in Verbindung? In *Handbuch Digitale Verwaltung*.
- Rinne, J. (2019). EU's Single Digital Gateway and its implementation in Finnish eGovernment: A case study. Master's Thesis, Aalto University, pp. 1-106.
- Rüscher, D. (2017). Der Digitale Zugang der Bürger zum Staat durch das Onlinezugangsgesetz. *Deutsches Verwaltungsblatt, 132(24),* pp. 1530-1535. Doi: 10.1515/dvbl-2017-2408.
- Scarduzio, J., Giannini, G., & Geist-Martin, P. (2011). Crafting an Architectural Blueprint: Principles of Design for Ethnographic Research. *Symbolic Interaction, 34(4),* pp. 447-470.
- Schaar, P. (2010). Privacy by Design. *Privacy by Design Issue of Identity in the Information Society 3:2,* pp. 267-274. Doi: 10.1007/s12394-010-0055-x
- Schallbruch, M. (2017). IT-Sicherheitsrecht - Schutz kritischer Infrastrukturen und staatlicher IT-Systeme. *Computer Und Recht, 33(10),* pp. 648-655.
- Scheinert, C. (2018). Single digital gateway. *Briefing: EU Legislation in progress. European Parliamentary Research Service, Brussels,* pp. 1-13.
- Scholta, H., Mertens, W., Kowalkiewicz, M., & Becker, J. (2019a). From one-stop shop to no-stop shop: An e-government stage model. *Government Information Quarterly, 36(1), January 2019,* pp. 11-26.
- Scholta, H., Niemann, M., Halsbenning, S., Räckers, M., & Becker, J. (2019b). Fast and Federal—Policies for Next-Generation Federalism in Germany. *Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS 2019),* pp. 3273-3282. Doi: 10.24251/HICSS.2019.395
- Sedek, K. A., Omar, M. A., & Sulaiman, S. (2014). A hybrid architecture for one-stop e-government portal integration and interoperability. *2014 8th. Malaysian Software*

Engineering Conference (MySEC), *IEEE,* pp. 96-101.

- Sichere Lösung für Bürgerkonten nach dem „Once only"-Prinzip. (2018). In Bundesdruckerei. Retrieved February 27th, 2020 from https://www.bundesdruckerei.de/de/Newsroom/Pressemitteilungen/Sichere-Loesung-fuer-Buergerkonten-nach-dem-Once-Only-Prinzip
- Siegfried, T. (2006). E-government in Germany. In *Nixon, P., Koutrakou, V. N. (eds), E-Government in Europe: Re-Booting the State, Taylor and Francis,* pp. 90-102.
- Somssich, R. (2015). Cohabitation of EU Regulations and National Laws in the Field of Conflict of Laws. *ELTE Law Journal, 2015(2).* https://eltelawjournal.hu/cohabitation-eu-regulations-national-laws-field-conflict-laws/
- Startseite. (n.d.). In *Koordinierungsstelle für IT-Standards (KoSIT)*. Retrieved March 12th, 2020 from https://www.xoev.de/
- Stocksmeier, D., & Hunnius, S. (2018). OZG-Umsetzungskatalog. Digitale Verwaltungleistungen im Sinne des Onlinezugangsgesetzes. 1. Auflage, Version 0.98; Berlin, April 2018. Retrieved April 20th, 2020 from https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/26_Sitzung/TOP2_Anlage_OZGUmsetzungskatalog.pdf?__blob=publicationFile&v=4
- Stocksmeier, D., Wimmer, M., Führer, M., & Essmeyer, K. (2019). Once-Only in Deutschland und Europa: Eine Roadmap grenzüberschreitender Vernetzung im Bereich Steuern. *Digitalisierung von Staat und Verwaltung Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2019.*
- Tambouris, E. (2001). An integrated platform for realising online one-stop government: the eGOV project. In *12th International Workshop on Database and Expert Systems Applications*, *Munich,* pp. 359-363.
- Verwaltungsverfahrensgesetz (VwVfG), BGBl. I S. 102. (25.05.1976, zuletzt geändert 21.06.2019). Retrieved April 10th, 2020 from https://www.gesetze-im-internet.de/vwvfg/VwVfG.pdf
- Willkommen zur Informationsveranstaltung zum Onlinezugangsgesetz. (2019). Dachverband der Kommunalen IT-Dienstleister (KDN). Bonn, 2019. Retrieved April 28th, 2020 from https://www.kdn.de/fileadmin/user_upload/2019-10-18-OZG-Infoveranstaltung-Bonn.pdf
- Wimmer, M. (2002). A European perspective towards online one-stop government: The eGOV project. *Electronic Commerce Research and Applications, 1(1),* pp. 92-103.
- Ziele der Nationalen E-Government Strategie. (n.d.). In *Nationale E-Government Strategie, IT-Plannungsrat*. Retrieved March 5th, 2020 from https://www.it-planungsrat.de/DE/ITPlanungsrat/NEGS/Ziele/Ziele_node.html

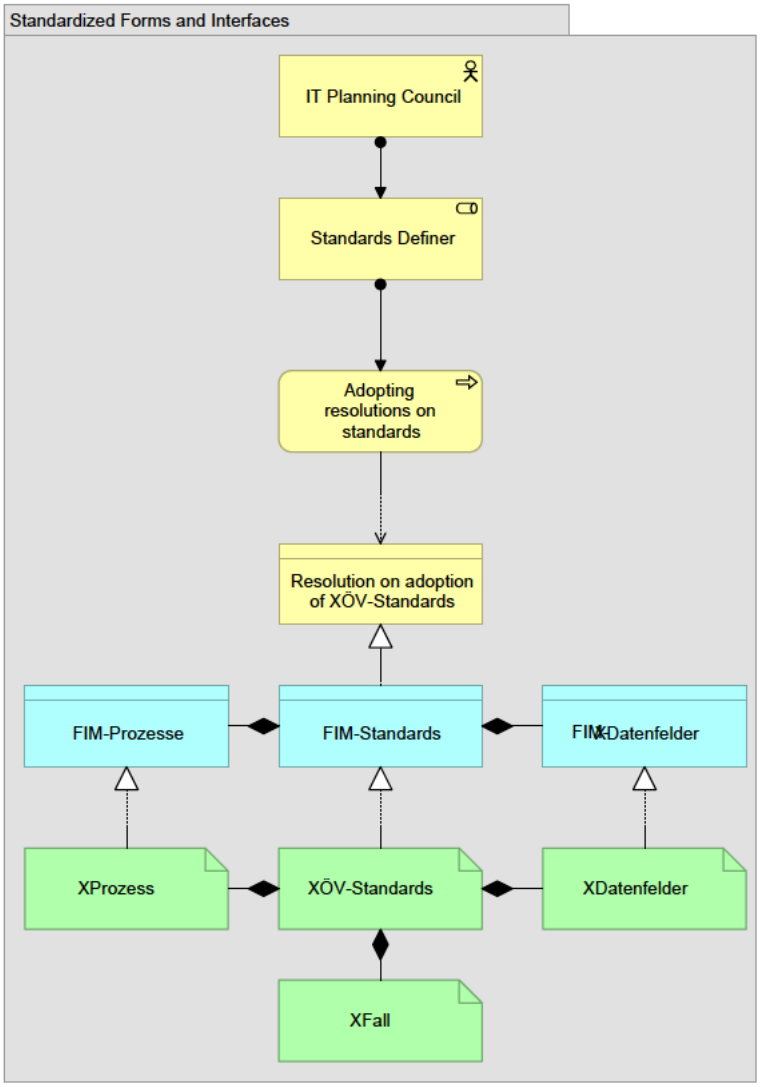
Appendix

A Annex 1. Overview Legislative Acts and Requirements.

	Data Sharing	*Standardized Forms and interfaces*	*e-ID*	*Integrated Base Registries*	*Transparency in Assigning Roles*	*Purpose Specification*	*Data Minimization*	*Accountability*	*Access to Information*	*Data Accuracy*	*Controllability*	*Consent*
SDG Regulation	Art. 14 Art. 38		Art. 13		Art. 10							
eIDAS Regulation			Art. 6									
GDPR		Art. 20				Art. 6	Art. 5 Art. 25	Art. 5 Art. 30	Art. 13	Art. 5	Art. 17 Art. 18 Art. 19 Art. 20	Art. 6 Art. 7
GG		Art. 91c										
OZG	Art. 8	Art. 3 Art. 7										Art. 8
EGovG	Art. 5	Art. 10 Art. 13			Art. 3 Sec. 11							Art. 5
BDSG					Art. 39 Art. 40	Art. 23 Art. 25	Art. 71	rt. 64 Art. 70	Art. 32 Art 34	Art. 32 Art 34	Art. 35	
Feederal Act on Registration	Art. 33 Art. 34 Art. 38 Art. 39 Art. 40 Art. 49			Art. 3 Art. 5								
Federal Act on Civil Status				Art. 3 Art. 55 Art. 56								

	Data Sharing	*Standardized Forms and interfaces*	*e-ID*	*Integrated Base Registries*	*Transparency in Assigning Roles*	*Purpose Specification*	*Data Minimization*	*Accountability*	*Access to Information*	*Data Accuracy*	*Controllability*	*Consent*
PAuswG			Art. 10 Art. 18 Art. 20									
eID-K-G			Art. 5 Art. 12 Art. 13 Art. 15 Art. 17 Art. 18	Art. 23								
VwVfG												
IT PC Resolutions		2019/15 2019/14 2018/40 2017/40										

B Annex 2. Decision Making for Standardization, Art. 10 of the EGovG.



Declaration of Authorship

I hereby declare that, to the best of my knowledge and belief, this Master Thesis titled "Architectural Blueprint of a One-stop government in Germany, aligning the implementation of the Once-only and the Privacy by design principles" is my own work. I confirm that each significant contribution to and quotation in this thesis that originates from the work or works of others is indicated by proper use of citation and references.

Cologne, 30 May 2020

Evgeniia Rudenko

Consent Form

for the use of plagiarism detection software to check my thesis

Name: Rudenko
Given Name: Evgeniia
Student number: 465583
Course of Study: Public Sector Innovation and eGovernance
Address: Schlossplatz 2, 48149 Münster
Title of the thesis: Architectural Blueprint of a One-stop government in Germany, aligning the implementation of the Once-only and the Privacy by design principles

What is plagiarism? Plagiarism is defined as submitting someone else's work or ideas as your own without a complete indication of the source. It is hereby irrelevant whether the work of others is copied word by word without acknowledgment of the source, text structures (e.g. line of argumentation or outline) are borrowed or texts are translated from a foreign language.

Use of plagiarism detection software. The examination office uses plagiarism software to check each submitted bachelor and master thesis for plagiarism. For that purpose the thesis is electronically forwarded to a software service provider where the software checks for potential matches between the submitted work and work from other sources. For future comparisons with other theses, your thesis will be permanently stored in a database. Only the School of Business and Economics of the University of Münster is allowed to access your stored thesis. The student agrees that his or her thesis may be stored and reproduced only for the purpose of plagiarism assessment. The first examiner of the thesis will be advised on the outcome of the plagiarism assessment.

Sanctions. Each case of plagiarism constitutes an attempt to deceive in terms of the examination regulations and will lead to the thesis being graded as "failed". This will be communicated to the examination office where your case will be documented. In the event of a serious case of deception the examinee can be generally excluded from any further examination. This can lead to the exmatriculation of the student. Even after completion of the examination procedure and graduation from university, plagiarism can result in a withdrawal of the awarded academic degree.

I confirm that I have read and understood the information in this document. I agree to the outlined procedure for plagiarism assessment and potential sanctioning.

Cologne, May 30th, 2020

Evgeniia Rudenko