Data protection in smart cities

Vandercruysse, Laurens

Publication date:
2022

Document Version:
Final published version

VRIJE UNIVERSITEIT BRUSSEL

SPECTRE

Dissertation submitted to obtain the degree of Doctor of Philosophy, Ph.D. in Business Economics

DATA PROTECTION IN SMART CITIES

AN ECONOMIC AND MANAGERIAL ANALYSIS

LAURENS VANDERCRUYSSE

2021-2022

Supervisors: Prof. dr. Michaël Dooms & Prof. dr. Caroline Buts
Social Sciences & Solvay Business School

Preface

This dissertation was prepared under the supervision of Professor dr. Caroline Buts and Professor dr. Michaël Dooms at the Vrije Universiteit Brussel (VUB). Sincere gratitude goes out to both, it has been a pleasure working together these past years.

Funding for the PhD was provided by the Research Foundation Flanders (FWO) through the Smart city Privacy: Enhancing Collaborative Transparency in the Regulatory Ecosystem (SPECTRE) project. Thank you to the FWO as well as the entire SPECTRE team, and especially Jonas Breuer and Athena Christofi, for the excellent collaboration. Also, I would like to thank all the experts that participated in the research.

Further, appreciation likewise goes to PhD evaluation committee members: Professor dr. Renata Paola Dameri, Professor dr. Jo Pierson, Professor dr. Peggy Valcke, and Professor dr. Leo Van Hove, for their excellent comments.

Many thanks go to Kenneth Goossens, Bruno Moeremans, Davide Rigoni, Fanny Soyeur, Nanouk Verhulst and the other colleagues at VUB for making it a pleasure to go to work. Gratitude to my parents for their support, thanks to my brothers as well. Finally, a special thank you to Paulien Van Schoor; my wife, my mentor, and my spell checker.

Abstract

Public administrations at all levels of government are confronted with challenges related to growing urban populations and shifting citizen preferences. Especially at the local level this tension is acute, because these challenges are coupled with an expanding number of responsibilities in a context of budget austerity.

To increase budget efficiency, local authorities are increasingly implementing smart city services (SCSs). These SCSs employ information technology to render public service provision more efficient as well as more effective. A smart city, which can be considered the compound of all SCSs in a particular urban setting, is thus developing.

Of course, administering these SCSs often entails the collection and processing of large personal datasets, this holds for managing a smart city a fortiori. The general data protection regulation (GDPR), which was introduced to safeguard the fundamental right to data protection in the rapidly evolving digital economy, is a crucial legal instrument in this context.

Adding to a body of academic literature shaped by technologists and legal scholars, this dissertation studies the topic of data protection in smart cities from an economic and managerial perspective. The collection of articles constituting the various chapters of this dissertation comprises traditional scientific research as well as more practical work, following both quantitative and qualitative methodologies.

The primary focus of the dissertation is on the economic as well as managerial aspects of the data protection impact assessment (DPIA) and on the impact of GDPR on competition in the SCS market.

Key takeaways include: i) improving data protection literacy of the SCS stakeholder community is an important success factor for sustainable smart city development, ii) the DPIA can only be a lever for smart city data protection when implemented through a stakeholder-inclusive approach, and iii) GDPR likely requires pro-competitive flanking measures to be truly effective.

Abbreviations

Short form	Full form
A29WP	Article 29 Working Party
AHP	Analytical Hierarchy Process
BE	Belgium
CCPA	California Consumer Privacy Act
CISO	Chief information security officer
CPV	Common Procurement Vocabulary
DGA	Data Governance Act
DMA	Digital Markets Act
DPA	Data protection authority
DPbDD	Data protection by design and by default
DPD	1995 Data Protection Directive
DPIA	Data protection impact assessment
DPO	Data protection officer
DSA	Digital Services Act
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EU	European Union
EC	European Commission
GDPR	General data protection regulation
IoT	Internet of Things
IT	Information technology
NL	The Netherlands
OECD	Organization for Economic Cooperation and Development
PCP	Pre-commercial procurement
PIA	Privacy impact assessment
R&D	Research and development
SC	Smart city
SCS	Smart city service
SCSP	Smart city service provider
TFEU	Treaty on the Functioning of the European Union
VC	Venture capital

Table of contents

Chapter 1. Introduction

Confronting societal challenges as climate change and expanding urban populations, local authorities are increasingly rendering public services more technologically advanced. Such a smart city transition necessarily also entails data collection efforts entering the physical public sphere. Since local authorities often lack the financial resources as well as the manpower and expertise to move toward a purely public sector driven smart city paradigm (Desdemoustier & Crutzen, 2017; Smart City Institute, 2018), private service providers play a central role in the digitalization and 'datafication' of the public sphere. Both the growth of collected data volumes as such, and the intensified involvement of private actors in public (data) governance, constitute potential dangers for the fundamental right to data protection in smart cities.

Through the various chapters, which are standalone studies as well, this dissertation provides an economic and managerial analysis of data protection in the context of smart cities. Venturing into a research field traditionally dominated by technologists and legal scholars, the aim of this work is to pinpoint typical economic and managerial issues that might have been previously overlooked. Furthermore, the dissertation conveys potential alleviating measures and solutions to identified problems.

This introduction comprises three sections: a presentation of key concepts, an examination of the research field, and an overview of the remainder of the dissertation.

1. Key concepts

It is crucial to introduce a few key concepts that will feature prominently throughout the dissertation. It concerns the concepts of smart city, and the general data protection regulation (GDPR).

1.1. Smart city[1]

The first academic research concerning smart cities dates to the 1990's (Anthopoulos, 2015). Inceptive development of the literature is inherently tied to the advent of new technologies. As a consequence, early definitions strongly stress the technological component of smart cities (Talari et al., 2017). It is important to note that technology is to be interpreted quite broadly. Of course, it includes information technology (IT), but for example technology aimed at reducing environmental impacts as well (Dameri, 2012). Over time, research has also pointed to rising education levels of citizens as a prime element of a smart city (Kummitha & Crutzen, 2017). In essence, the state of the human resources available in the city would drive its smartness. Relatedly, others have stressed that the development state of a smart city can be gauged by the influence of the public in urban governance (Meijer & Bolívar, 2016), i.e.

[1] This section lends from Vandercruysse, Buts & Dooms (2020) and Vandercruysse, Buts & Dooms (2021).

participative decision-making as a fundament of smart city transition. Moreover, the variety of smart city models is a further testament to the confusion surrounding the concept. Some authors model smart cities along various dimensions of smartness (Giffinger et al., 2007), e.g. smart economy, smart mobility, while others consider any attempt at generalization futile and swear by a case-by-case approach (Karvonen et al., 2018).

An exhaustive overview of the various facets, and facet variations, of the smart cities concept is beyond the scope of this dissertation – it is a research field in and of itself. Nonetheless, the understanding that there is a lack of a uniform definition is crucial. Scholarly consensus is present on the fact that "*the*" smart city does not exist.

To somewhat step away from the semantic discussion on the elusive smart city, it is opted to take a more granular approach. This dissertation will consistently view smart cities through its modular building blocks, i.e. the individual smart city services.

In terms of smart city facets, service-centricity necessarily entails making abstraction of certain overarching elements, e.g. smart city vision, politics, etc. However, in exchange it offers the possibility to go more in depth, and to essentially stay close to current smart city development practice which often lacks these elements (see e.g. Dameri & Rosenthal-Sabroux (2014) and Khan et al. (2020)).

In terms of smart city modeling, the focus on the smart city service keeps a middle ground between grouping widely differing smart city services under a thematic umbrella and abiding by a pure case-by-case analysis. On the one hand, data protection implications are arguably more likely to vary between various types of services than between service themes. It can be argued that a camera on a public square and a camera fitted onto a traffic light are more alike, than an end-to-end solution for medical patient files and a visitor counter both in a hospital. On the other hand, similar services hardly all necessitate a sui generis data protection approach. Setting up an identical camera-based security system in city A and city B will likely have similar data protection implications for both environments.

The approach of taking the mentioned level of analysis thus provides several advantages: it simplifies the analysis vis-à-vis an all-encompassing smart city view, it allows for a more thorough understanding of fundamental problems at the base level, and it permits clear differentiation between various types of services with regard to their data protection features.

Furthermore, the more granular view allows us some leeway in defining the pertinent smart city services. To optimize the relevance for data protection, this dissertation zooms in on services having data capabilities. This scope is in line with previous research stating that IT and data (collection) form cornerstones of smart city development (Braun et al., 2018).

For the purposes of the research, we define a smart city service as: "*a service that provides a solution for a societal problem based on technology but with interaction with the physical world where data collection and use are central and involves several stakeholders, both public and private*" (Neirotti et al., 2014; Walravens & Ballon, 2013; as in Vandercruysse, Buts & Dooms, 2020, p. 6). This definition comprises three major elements.

First, the service is to aid in solving a societal problem. This excludes services that do not have a public interest dimension, for example most smart home equipment, and ensures a level of involvement of local authorities. The city is tasked with protecting the public interest of their inhabitants, so they have an obvious stake in services furthering the attainment of that task. Furthermore, the local authority is reserved the sole right to exercise many public duties (Kersting & Vetter, 2013).

Second, the service entails both a technological and a physical component. Purely digital services thus fall outside the scope. While online services surely contribute to smart city development in a broad sense, links to the physical city infrastructure and presence in the public space ensure a more permanent and public character. The presence of physical components in the public domain makes these types of services more inescapable and thus in many ways more intrusive (Ni Loideain, 2018). While one can choose not to sign up to a social media platform because of privacy considerations, opting not to leave the house because of privacy concerns over the presence of a city-wide CCTV-network can hardly be conceived as a real choice.

Third, the service is data-intensive. As mentioned, there is a consensus that the "*smartness*" of a service or a city is in part produced by the collection and usage of large amounts of personal data (Al Nuaimi et al., 2015; Regulation (EU) 2016/679 (GDPR), 2016). Because most local authorities lack the resources and technological competences to develop these services in-house (Desdemoustier & Crutzen, 2017; Smart City Institute, 2018), involvement of private stakeholders necessarily ensues.

To clarify what services meet the above definition of a smart city service, and which services do not, we offer several examples in Table 1.

Service example	**Smart city service**
Online portal for passport or change of domicile requests	No, lack of physical component
Domestic garbage collection based on smart containers	Yes
Online booking service for municipal tennis court	No, lack of physical component
Camera-based solution to monitor littering	Yes
Automatic attribution of welfare cheque based on income-level	No, lack of physical component
Crowd monitoring system via Wi-Fi tracking	Yes

Table 1. Examples to clarify smart city service definition. Source: own creation.

1.2. GDPR

The right to personal data protection is enshrined in Article 8 of the Charter of Fundamental Rights in the European Union (EU) (Charter of Fundamental Rights of the European Union, 2012). Paragraph 2 notes that:

> "*Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified*" (Charter of Fundamental Rights of the European Union, 2012).

References to fairness, purpose specification, legitimate processing, and data access, make clear that the concept of data protection goes beyond mere data security. In some ways, the concept is broader than privacy as well.

Its inclusion in the Charter of Fundamental Rights, and the Treaty on the Functioning of the European Union (TFEU), accords data protection an important role in the EU's legal order (Bygrave, 2017). Fundamental rights are seen as core markers of human freedom and as such deserve strong protection. However, not all fundamental rights are absolute (European Commission, n.d.a), and in cases where these interfere with each other a balance has to be stricken.

In an attempt to update legislation and to render EU member states' data protection levels more uniform, the European Commission proposed a review of the 1995 Data Protection Directive in 2012 (European Data Protection Supervisor, 2019). Concretely, it was proposed that the Directive be replaced by a Regulation, i.e. the GDPR, which was to hold uniformly across the EU and over sector lines (European Commission, 2019).

The GDPR is the most encompassing legal instrument concerning data protection in the EU. The Regulation was introduced in May 2016 and entered into applicability on the 25. May 2018 (European Commission, 2020a). Seven key principles are: lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and, accountability (Regulation (EU) 2016/679 (GDPR), 2016). The latter principle primarily targets data controllers (Urquhart, Lodge & Crabtree, 2019), i.e. the entities determining the purposes of the data processing and the means with which to achieve them.

From an economic and managerial point of view, the accountability principle is of central importance. Not only does the translation of the principle into specific obligations produce additional costs, e.g. integrating privacy-by-design and privacy-by-default, hiring a data protection officer (DPO), or doing a

data protection impact assessment (DPIA), the non-compliance with these obligations can lead to fines up to €10 million or 2% of global annual turnover (Regulation (EU) 2016/679 (GDPR), 2016).

This dissertation focuses on GDPR-related data protection costs in general and their impact on competition, but also zooms in on the DPIA as cost center and managerial problem.

1.2.1.DPIA

As mentioned, the most notable example of a new accountability measure is the DPIA-obligation as put forth by GDPR Article 35 (Regulation (EU) 2016/679 (GDPR), 2016). Citing paragraph 7, conducting a DPIA requires:

> "*A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
> *An assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
> *An assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1;*
> *And the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned*" (Regulation (EU) 2016/679 (GDPR), 2016).

The DPIA puts data controllers in charge of assessing the data protection effects of their own (desired) "*high risk*" data processing activities (Article 29 Working party, 2017; Bu-Pasha, 2020). As a consequence, these actors are responsible for determining its necessity and proportionality as well as its balancing with regard to other various interests. The exercise has to be completed before the data processing is implemented, and the process of doing the DPIA should be well-documented in order to allow for inspection by the data protection authorities (DPAs) (Article 29 Working party, 2017).

According to the European Commission's own regulatory impact assessment in 2012, the cost for a single DPIA can range from €14 000 to €149 000 (European Commission, 2012). It is evident that a novel cost of that magnitude could have substantial economic side-effects on the micro and macro level.

To the best of our knowledge, the research on the economic and managerial aspects of the DPIA contained in this dissertation is among the earliest in the field.

2. Research field

The central theme of this dissertation, i.e. smart city data protection, is rarely connected to the broader disciplines of economics and management. With an eye on substantiating this claim by way of some concrete numbers, a series of queries were run on the Web of Science-database by Clarivate.[2]

Focusing on the smart cities theme, it is immediately clear from Figure 1 that the number of publications has been growing largely consistently over the past ten years. Expanding private sector pilot projects, e.g. Sidewalks Labs Toronto (Cecco, 2020), and growing public sector awareness and data literacy might partly explain the trend.

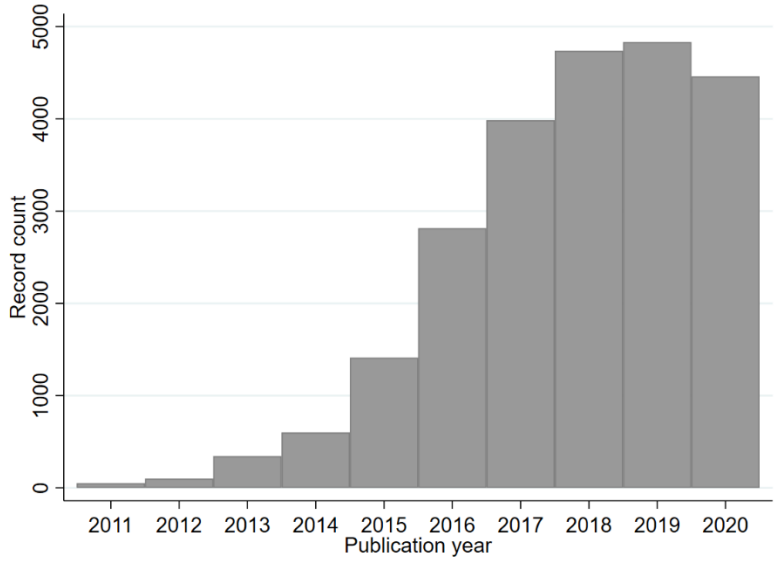

Figure 1. Web of Science-query results for "Smart city" or "Smart cities" per publication year. Source: own creation based on Clarivate (2021).

Nonetheless, a look at the research fields that these publications cover, as displayed in Table 2, shows that the smart cities literature is very much dominated by technologists. Only about three percent of publications can to some extent be considered to fall in the domain of business economics.

Research field	Number of publications	As a % of 23 402
Computer Science	12 213	52,2%
Engineering	9 980	42,6%
Telecommunications	4 618	19,7%
Science Technology Other Topics	2 002	8,6%
Urban Studies	1 514	6,5%

Table 2. Web of Science-query results for "Smart city" or "Smart cities" per research field (performed on 6. January 2022, publications can belong to multiple research fields). Source: own creation based on Clarivate (2021).

[2] All queries were also run in the Law Journal Library by HeinOnline (HeinOnline, 2022). Trends for the various queries in record counts per year are similar (available upon request to the author). As the aim of this section is to indicate the seeming lack of economics and management literature in the research field, rather than perform an exhaustive analysis, it was opted not to include this here.

Pivoting to data protection, the trend of the annual publications graph is similar. The number of publications constantly sits at a relatively high level, but academic interest rises considerably over time as Figure 2 demonstrates.

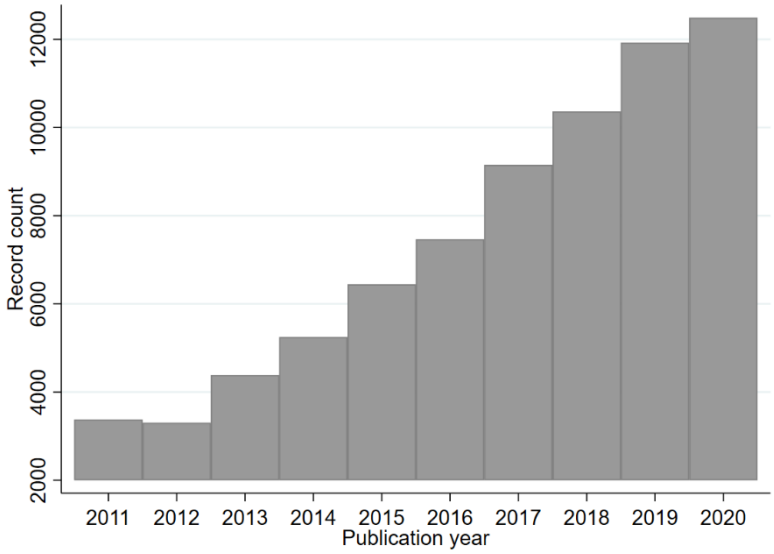

Figure 2. Web of Science-query results for "Data protection" or "Privacy" per publication year. Source: own creation based on Clarivate (2021).

In contrast to the topic of smart cities, data protection is relatively well covered in the business economics literature. This can be seen in Table 3. Important papers include work on privacy protection by social networks (Bonneau & Preibusch, 2010), contextual, welfare and, informational aspects of privacy (Acquisti, Taylor & Wagman, 2016), and on mapping general competitive effects of the introduction of the GDPR (Gal & Aviv, 2020).

Research field	**Number of publications**	**As a % of 99 053**
Computer Science	58 314	58,9%
Engineering	25 272	25,5%
Telecommunications	17 630	17,8%
Government Law	4 688	4,7%
Business Economics	3 685	3,7%

Table 3. Web of Science-query results for "Data protection" or "Privacy" per research field (performed on 6. January 2022, publications can belong to multiple research fields). Source: own creation based on Clarivate (2021).

However, when combining the two central topics of this dissertation in a single query, it becomes evident that the related research is still in its infancy. While Figure 3 shows a clear upward trend, the absolute number of publications is rather limited along the period.

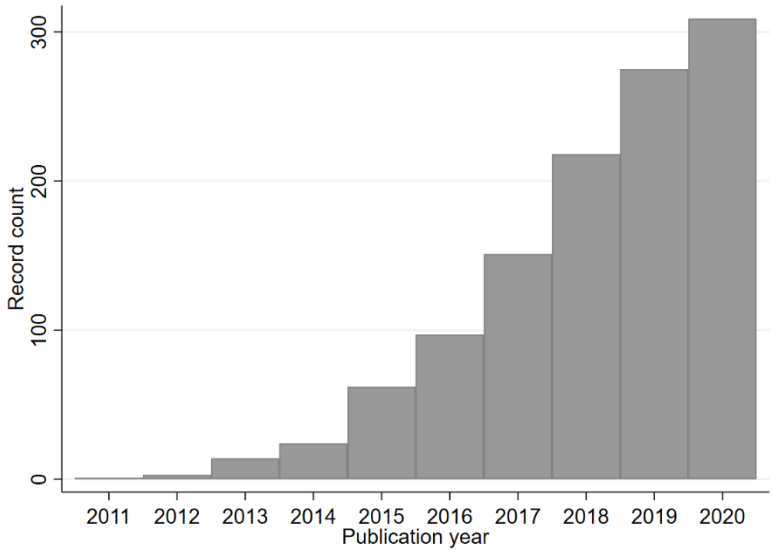

Figure 3. Web of Science-query results for ("Data protection" or "Privacy") AND ("Smart city" or "Smart cities") per publication year. Source: own creation based on Clarivate (2021).

In addition, Table 4 again shows a strong dominance of technologists in the discussion. When it comes to business economics, only 22 publications (less than two percent) over the full period can be resorted under that particular heading.

Research field	Number of publications	As a % of 1 155
Computer Science	804	69,6%
Engineering	481	41,6%
Telecommunications	359	31,1%
Science Technology Other Topics	78	6,8%
Energy Fuels	43	3,7%

Table 4. Web of Science-query results for ("Data protection" or "Privacy") AND ("Smart city" or "Smart cities") per research field (performed on 6. January 2022, publications can belong to multiple research fields). Source: own creation based on Clarivate (2021).

In summary, important forward strides have been made with respect to the economic and managerial aspects of data protection, but an application of relevant insights to the context of smart cities is markedly missing. Smart cities, both in general and in particular with regard to data protection, remains the domain of technology experts. Consequently, considerable blind spots with regard to the economics and management will likely remain. This dissertation provides foundations to fill substantial research gaps in this area.

3. Overview of the dissertation[3]

The dissertation comprises 9 chapters. This first chapter contains the general introduction. Chapters 2 through 5 focus on the economic and managerial aspects of the DPIA instrument in particular. Chapters 6 through 8 concentrate on the impact of the GDPR's introduction on competition in the smart city

[3] This section is largely based on the abstracts of the various chapters that are included in this dissertation.

services (SCS) market. Chapter 9 concludes. Substantive chapters can also be divided based on primary target audiences: Chapter 2, Chapter 4, and Chapter 7 constitute traditional scientific contributions, while the remaining chapters are mostly aimed at practitioners and policy makers. It is important to note that all substantive chapters represent standalone studies, these constitute individual research articles. Table 5 provides a schematic overview of the described structure.

Data Protection in Smart Cities: An Economic and Managerial Analysis		**Main target audience**	
Chapter 1. Introduction		Science	Practice & policy
Managerial aspects of the DPIA	Chapter 2. A typology of smart city services: The case of DPIA	X	
	Chapter 3. Data control in smart city services: Pitfalls and how to resolve them		X
	Chapter 4. The DPIA: Clashing stakeholder interests in smart cities?	X	
	Chapter 5. Beyond data controllership: Merits of a generic DPIA by hardware/ technology suppliers		X
GDPR & competition for SCSs	Chapter 6. Public procurement as a safeguard for competition: The case of smart city services		X
	Chapter 7. Public procurement of smart city services: An exploration of data protection related ex-ante transaction costs	X	
	Chapter 8. Data Protection in smart cities: Pre-commercial procurement as a silver bullet?		X
Chapter 9. Conclusion			

Table 5. Schematic overview dissertation's structure. Source: own creation.

What follows is a concise outline of the contents of the various chapters.

Chapter 1 introduces the research topic, its key concepts, position in the extant literature, and outlines the structure of the dissertation.

Chapter 2 zooms in on the data protection impact assessment-process, one of the specific regulatory requirements in terms of data protection for smart city services characterized by "high risk." In short, the DPIA is an assessment of the data protection implications of a certain data processing to be performed by the data controller before its implementation. This chapter identifies various dimensions, and layers, of data protection complexity to derive a typology of smart city services based on DPIA-costs. It does so through an exploratory case-study of the Flemish smart city.

Chapter 3 investigates the inherent complexities of data controllership in smart city services. Particular characteristics of these services, i.e. data-intensity and complex partnerships, challenge the differentiation between (joint) data controllers and data processors. However, data controllership is

central in allocating data protection accountability, a.o. the responsibility to conduct a DPIA. Building on nine expert interviews with Flemish data protection officers, we pinpoint four possible scenarios. Next, we identify potentially problematic scenarios and subsequently propose a set of measures to handle underlying stakeholder tensions.

Chapter 4 looks at the DPIA through the lense of issue-focused stakeholder management (Roloff, 2008). From a technological perspective, a smart city is often considered as the pinnacle of urban efficiency. From a business perspective, there is a straightforward financial incentive to subscribe to that narrative. However, from a societal perspective, there is a clear friction with several values and norms, e.g. data protection. This chapter focuses on the DPIA in the context of smart city services, and identifies and evaluates the various stakeholder interests that feature during this particular data protection interaction. Empirical data is gathered through sixteen data protection expert interviews and a survey-based analytical hierarchy process method application.

Chapter 5 discusses the position of hardware and technology suppliers in the data protection impact assessment-process. While various stakeholders should be involved, either as required by the GDPR or as suggested by guidance of the Article 29 Working Party, developers of hardware and technological solutions are seemingly overlooked. We examine drivers for their deeper engagement and outline potential benefits thereof.

Chapter 6 centers on the European Union's Digital Strategy. By way of this Strategy, the European Commission aims to tackle precisely pressing competition issues specific to markets of data-intensive services. One of these issues is the substantial and durable competitive advantage that emerges from having exclusive access to large sets of data. The Digital Markets Act proposal, a prime pillar of the Strategy, allows for the identification of gatekeepers. These gatekeepers would then be subject to additional obligations, for example enabling wider data access. This chapter focuses on the market for smart city services and explores the adoption of a more proactive approach through public procurement. The empirical underpinning is provided by 19 semi-structured expert interviews.

Chapter 7 departs from the observation that local authorities often lack both the financial resources as well as the manpower and expertise to develop their own smart city services. It follows that formal public procurement procedures will play a central role in smart city development. This chapter examines private sector borne ex-ante transaction costs related to data protection. These costs can best be described as data protection expenses that are incurred by bidders in the process of compiling a bid for a certain tender, e.g. staff costs emerging from compiling a rudimentary data protection analysis of a data processing system. Through an econometric examination comprising 72 individual

SCS tender bids, we establish the determinants of data protection related ex-ante transaction costs as well as determine their competitive relevance.

Chapter 8 focuses on a common lacuna in classic public procurement procedures, namely a lack of leeway for negotiation between public and private partners. Smart city services are being adopted at a rapidly increasing pace to further the public interest. However, the implementation of such services also presents a potential danger to the fundamental right to data protection. Furthermore, local authorities' requirements with respect to transparency, democratic oversight, and clear accountability tend to transcend those of private actors. These peculiar requirements complicate utilizing traditional public procurement procedures of off-the-shelf products and services. Based on a case-study, this chapter analyzes the potential of pre-commercial procurement, i.e. a particular public procurement procedure supported by the European Union in order to enable public sector innovation, to substantively comply with GDPR.

Chapter 9 provides overarching conclusions, derives a series of recommendations, and proposes avenues for further research.

Chapter 2. A typology of smart city services: The case of DPIA[4,5]

Abstract

The implementation of the General Data Protection Regulation within the European Union intensifies regulatory requirements in terms of data protection for smart city services. In particular, the mandatory data protection impact assessment (DPIA)-process constitutes a complex managerial challenge. To reduce the complexity, this study develops a typology of Flemish smart city services based on DPIA-costs.

Our explorative case study, based on face-to-face interviews and a workshop, shows that DPIA-costs vary along the complexities of i) the urban environment in which a smart city service is provided, and ii) the smart city service itself. The research further demonstrates that these complexities represent multilayered concepts. The complexity of the urban environment consists of three layers: i) city size, ii) diversity of urban stakeholders, and iii) total of smart city services in the urban region. Similarly, the complexity of the smart city service is composed of five layers: i) number of different data streams, ii) clarity of data controllership, iii) amount of use-cases, iv) privacy invasiveness, and v) visibility of the smart city service. While most layers of the respective complexities unequivocally matter in the eyes of the experts, others are more contested, such as the size of the city and the visibility of the smart city service.

This cost-based framework is of value to city administrations and smart city service providers as it allows them to make the DPIA-process more efficient by shortening the learning curve and improving decision-making by clustering services based on data protection needs. In particular, stakeholders that have little expertise in-house, and that are looking for an easy-to-understand, rational framework can benefit from these results. Furthermore, based on both the literature review and the obtained results, our systematic data protection impact-cost-approach is generalizable beyond the EU-borders.

[4] This chapter is published as an article in Cities, we thank two anonymous reviewers and editor Professor dr. Johan Woltjer for their useful feedback on previous versions. Please cite as: "Vandercruysse, L., Buts, C., & Dooms, M. (2020). A typology of Smart City services: The case of Data Protection Impact Assessment. *Cities*, *104*, 102731."

[5] **Author contributions** - **Laurens Vandercruysse**: Conceptualization, Methodology, Formal Analysis, Visualization, Writing - Original Draft; **Caroline Buts**: Conceptualization, Validation, Writing - Review & Editing, Supervision; **Michaël Dooms**: Conceptualization, Validation, Writing - Review & Editing, Supervision.

1. Introduction

While the definitions of 'smart city' and 'smart city service' vary, most scholars agree that information technology is a key aspect of both concepts (Caragliu, Del Bo, & Nijkamp, 2011; Chourabi et al., 2012; Dameri, 2012). From a narrow angle, a smart city can be defined as being on the nexus of three technological advances, namely: the internet of things (IoT), cloud computing, and big data (Edwards, 2016). What binds these elements is their inherent relation to the collection and processing of large amounts of data. As such, smart city services constitute important targets of the General Data Protection Regulation (GDPR) that became applicable in the European Union (EU) on 25. May 2018. Its implementation severely intensified regulatory requirements in terms of data protection for smart city services. In particular, the mandatory data protection impact assessment (DPIA)-process constitutes a new challenge for those data processing activities characterized by "*high risks related to the rights and freedoms of individuals*" (Regulation (EU) 2016/679 (GDPR), 2016). Furthermore, as the European legislator explicitly requires a DPIA to be performed for services that conduct either "*systematic monitoring of public areas on a large scale*" or "*processing of sensitive data on a large scale*" (European Commission, 2018b), a wide range of smart city services will most probably fall within the envisioned scope of the DPIA-obligation.

While the GDPR gave new impetus to research focused on the intersection of smart cities and data protection, discussions on the subject transcend the case of the EU. Around the globe policy makers, with varying success, are developing novel data protection legislation to curtail unbridled data gathering and to safeguard the fundamental rights and privacy of individuals (e.g. the California Consumer Privacy Act (CCPA), the PRC Cybersecurity Law and the PRC E-Commerce Law in China, and India's proposed Data Protection Bill (DLA Piper, 2019)). With the continued development of novel data processing tools and the projected growth of urban populations (Chourabi et al., 2012), data protection is set to become an even more important urban policy issue. The tradeoff between gains of the data economy and data protection remains a contentious tension (Lenard & Rubin, 2010). Undoubtedly, the perceived complexity and uncertainty surrounding the cost impact of rendering smart city services data protection-friendly play a role. How do data protection impacts of smart city services, and the ensuing costs to make that service compliant with data protection legislation, vary? To answer that question, we study the specific case of the DPIA, a systematic impact-cost-approach that is arguably generalizable far beyond EU-borders.

Though a comprehensive data protection typology for smart city services is currently lacking from the literature, there is a clear need for a generic framework supporting the uptake of data protection legislation worldwide. This study develops a generic typology of smart city services based on DPIA-costs. It builds on case-based evidence from one of Belgium's three main regions, Flanders. Flemish

smart cities are interesting cases to study for several reasons. First, the few studies that are available on the topic of Flemish smart cities confirm that city administrations lack necessary expertise to follow-through on implementing smart city services (Desdemoustier & Crutzen, 2017; Smart City Institute, 2018). On the global level, such a lack of expertise is also likely to be widespread, especially in regions where data protection considerations and privacy-awareness are just coming to the fore. In that sense, the case of Flanders can be widely instructive once other regions around the world are moving ahead with these considerations. The potential of the GDPR to serve as a model for international data protection efforts adds to this argument (Albrecht, 2016; Scott, 2014). Second, the DPIA-practice in the EU (including a subregion such as Flanders) has to the best of our knowledge not yet been examined and thus potentially offers enlightening insights. Hence, the development of measures to reduce the perceived complexity of the landscape of smart city services in the specific case of Flanders constitutes a valuable exercise, with potential for analytical generalization.

Sound data protection is a key enabler of smart city services, which contributes to more sustainable cities. More broadly, concrete urban policy recommendations can be derived concerning safeguarding social cohesion and fostering sustained economic growth in the urban environment.

This chapter is structured as follows. Section one reviews the extant literature on smart city service classifications, and privacy- and data protection impact assessments in smart cities. Subsequently, section two further elaborates the research question. Section three contains the explorative qualitative methodology to construct a typology of smart city services. Next, section four explicates our empirical results. Section five discusses wider implications. Finally, section six provides conclusions and recommendations, including avenues for further research.

2. Literature review

2.1. Modeling ‘the smart city’ and typologies of smart city services

The ‘smart city’ as a field of research has developed quickly since the end of the 1990’s when the concept was first introduced (Anthopoulos, 2015). A widespread adoption of the term triggered ambiguity regarding its meaning. There is disagreement in the scientific literature about when or how a city becomes ‘smart’. First, a strand of literature focuses mostly on the pure technological aspects underpinning urban development and processes (Talari et al., 2017), i.e. a smart city as the pinnacle of urban technological prowess. Second, ‘smart’ is used to signify the education-level of the urban population, i.e. smart people flocking together in urban areas resulting in cities becoming smart (Kummitha & Crutzen, 2017). Finally, smart is also used to indicate a high level of collaborative governance in the city, i.e. a wide variety of stakeholders becoming involved in urban steering and sustainable development (Meijer & Bolívar, 2016). It is clear that ‘the smart city’ entails more than the

mere technological aspect; this reductionist view has been subject to a lot of criticism. The human-centric view adds an important dimension, but is not encompassing, nor can the governance perspective cover the entire concept. We argue that data, as the main underlying resource, is the missing link between the three perspectives. Data is gathered through (smart) technology, generated by (smart) people, and used to more efficiently, effectively and inclusively (smartly) govern the city. Data is what makes the city smart and data protection makes that 'smartness' sustainable. Therefore, an attempt to model smart cities should account for the data protection perspective, as a key element of stakeholder trust.

Furthermore, academic literature often groups smart city services per service domain, sometimes referred to as smart city dimensions. Giffinger et al. (2007) suggest differentiating between six smart city dimensions, namely: smart economy, smart environment, smart governance, smart living, smart mobility, and smart people. Arguably, this dimensionality can be used to classify smart city services. Moreover, Fernandez-Anez et al. (2018) distinguish five types of smart city services: economy, environment, living and services, mobility and infrastructures, and people. Alternatively, Chourabi et al. (2012) map eight success factors for initiatives in smart cities ranging from management and organization of the service through the natural environment in which a service is to be instituted. While not originally conceived to the end of classifying services, these success factors lend themselves to scoring and thus classification. The main problem with these classifications is that they tend to discount the variety of individual service characteristics and reduce this service variety to differences in service domain. We argue that practical use can be optimized by taking a more granular look at smart cities and studying the individual building blocks, i.e. individual services and the inherent data protection issues, more closely.

Taking a more micro-level view, Lee and Lee (2014) propose a classification of smart city services on the basis of four characteristics: type of technology, objective, autonomy in using the service, and the level of service interactivity. While we support the level of analysis and the human-centric perspective, we stress the importance of data (protection) considerations. We therefore argue that a more encompassing, systematic approach imposes itself.

Finally, a different stream of research argues that individual smart city cases are so idiosyncratic that only case-by-case smart city models can be expected to deliver a useful result (Karvonen et al., 2018; Kitchin et al., 2018). This approach clearly reduces the practical use and generalization potential of any model. As we value the insight that 'the smart city' does not exist and that urban differences matter, we allow for urban heterogeneity in our typology but nonetheless still offer a considerable level of generalizability. In that sense, our contribution is original.

2.2. The GDPR and the DPIA

The GDPR is the premier legislation dealing with personal data protection in the EU. Upon its entering into applicability as a regulation, the GDPR became immediately, uniformly and universally binding in the 28 member states (European Commission, 2019). Directive 95/46/EC, of which the GDPR is at least an extensive update, became obsolete mostly because of the high-speed technological progress of the last decades and the resulting development of the data economy (European Data Protection Supervisor, 2019). In addition to boosting transparency and strengthening the rights of citizens vis-à-vis data controlling companies, a major aim of the GDPR is to increase the accountability of companies that control personal data (Tikkinen-Piri, Rohunen, & Markkula, 2018). A DPIA constitutes an example of such an accountability mechanism, which leaves organizations determining the purposes and means of a data processing, i.e. data controllers, in charge of assessing the ensuing data protection risks (Regulation (EU) 2016/679 (GDPR), 2016). With responsibility comes accountability, as incompletely fulfilling the DPIA-obligation can result in fines up to €10 million or 2% of global annual turnover (Regulation (EU) 2016/679 (GDPR), 2016). Additionally, the 2012 regulatory impact assessment performed by the European Commission estimated DPIA-costs, including salaries, to vary between €14 000 and €149 000 (European Commission, 2012). The financial investment in the DPIA-process by public and private data controllers will thus be considerable.

2.3. (D)PIA in the context of smart city services

While the DPIA-requirement for certain types of data processing activities has only been introduced in the EU in May 2018, certain Anglo-Saxon jurisdictions have had privacy impact assessments (PIAs) as part of their data protection policies since the 1990's (Binns, 2017; Wright, 2012). Even though the concepts PIA and DPIA are not synonyms, a considerable overlap exists both in terms of purpose as well as procedures (van Dijk, Gellert, & Rommetveit, 2016). Both the PIA- and the DPIA-processes ensure that thorough reflection on data collection, processing and protection takes place before data processing activities are introduced (Bieker et al., 2016; Wright & Raab, 2012). One of their main aims is to safeguard legally required levels of respectively privacy and data protection, but both are defined as actions that go beyond mere compliance (Bieker et al., 2016; Wright & Raab, 2012). Also as regards their prescribed processes they are considerably similar: i) both entail a mapping and examination of envisioned data flows and resulting risks for the rights of data subjects, ii) both define measures to protect these data subject rights in light of the uncovered risks, and iii) both require to conduct a review of the assessment at least when the processing activity changes (Bieker et al., 2016; Oetzel & Spiekermann, 2014; Wright, 2013).

It is important to understand the particularities of a DPIA. Article 35 of the GDPR describes when a DPIA is required, i.e. when the foreseen data processing activities pose elevated risks to individuals'

rights and freedoms (Regulation (EU) 2016/679 (GDPR), 2016). Furthermore, section seven of the same Article describes the minimum requirements for the completion of a DPIA. Such an effort has to at least include:

1. "*A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
2. *An assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
3. *An assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1;*
4. *And the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned*" (Regulation (EU) 2016/679 (GDPR), 2016).

Because of their nature, a considerable variety of smart city services is subject to a DPIA. A single and specific definition of 'smart city service' is not available. However, we can generally define it as a service that provides a solution for a societal demand based on technology that interacts with the physical world, where data collection and data use are central and several stakeholders, both public and private, are involved (Neirotti, De Marco, Cagliano, Mangano, & Scorrano, 2014; Walravens & Ballon, 2013). While it is clear that a wide range of smart city services is required to undertake a DPIA, it is equally clear that not all smart city service DPIAs will consume the same amount of resources (Bartoli et al., 2011; Fagnant & Kockelman, 2015). Indeed, conceptions of 'smart city' vary widely and smart city services are to be interpreted within their urban context (Karvonen, Cugurullo, & Caprotti, 2018; Kitchin, Coletta, Evans, & Heaphy, 2018). This context-dependency is likely to also impact the DPIA. The positive correlation between city size in terms of population and the magnitude of the data protection risk constitutes an example. More intuitively, mapping data flows will also be more time-consuming when more diverse data flows need to be included. These observations are the starting point for the creation of a typology of smart city services.

2.4. Complexity is key

Wright (2012) states that complexity is important in differentiating between DPIAs, as the scale and the scope of such an assessment should correlate positively with the corresponding attributes of the envisioned service. In the literature, two dimensions of complexity are discovered, i.e. the complexity of the urban environment in which a smart city service is provided and the complexity of the smart city service itself. Along these complexities, DPIA-efforts, and the ensuing costs, vary.

As urban centers around the world have grown in terms of urbanized area as in terms of population, smart city services addressing societal needs have been developed (Marrone & Hammerle, 2018; Martinez-Balleste, Perez-martinez, & Solanas, 2013). As a result of this concentrated growth of urban centers, size differences with more rural cities have increased. Cities are complex systems that turn more complex with increasing size (Fernández-Güell, Collado-Lara, Guzmán-Araña, & Fernández-Añez, 2016), which consequently affects the DPIA. Furthermore, growing cities may also induce smart city service providers (SCSPs) to supply certain products and services, which they would not in more rural areas due to economies of scale (Martinez-Balleste et al., 2013; Neirotti et al., 2014). This combination of demand and supply side factors thus provides a fertile breeding ground for the sustained growth of large smart cities, while smaller cities might have to cope with their own specific issues (Bell & Jayne, 2009). Some of the confusion with regard to the concept 'smart city' originates from considering it as a homogenous notion (Kong & Woods, 2018; Shelton, Zook, & Wiig, 2015). However, smart city services are to be understood within their context, i.e. the urban environment in which they are introduced (Kitchin et al., 2018). In short, the differential growth and resulting size are thus of importance for the DPIA-process.

Technological advances enable more service-oriented applications tailored to the population. Smart city services therefore increasingly vary in their complexity and data-intensiveness (van Zoonen, 2016). The difference between a city-wide waste monitoring system and a meal service that uses drones to deliver food orders constitutes an example. The data required to supply the former is limited to waste and domiciles, where both have to be transferred to a centralized server. However, to effectively deliver the latter the service provider needs: e.g. location data of the drones, location data of the client, data on the order, restaurant and menu, and payment data. Additionally, these data streams have to be sent to different interacting devices at various times. Subsequently, the nature of the service influences the amount of effort needed to perform a compliant and relevant DPIA (Wright, 2012).

3. Research objectives and question

As demonstrated, a variety of smart city models have been suggested but an encompassing approach focused on the service level is lacking. In an era of rapid technological evolution and a progressive insight by policymakers and citizens worldwide into ensuing data protection issues, a typology for services based on data protection impacts and costs imposes itself. In concertation with field experts, we develop a data protection impact-cost-typology for smart city services. Building on the DPIA-process as introduced by the GDPR, we establish determinants for the data protection impact of services and the subsequent costs to make the services compliant to data protection law. The DPIA serves mostly to develop a coherent and systematic framework for evaluating data protection impacts and costs. Such a framework could bring a more structured approach to ex-ante management of data

protection and at the same time make the impact assessment processes, more broadly, more cost-effective. More narrowly, a novelty in the EU, the DPIA constitutes a considerable financial challenge for public and private organizations operating within the EU (European Commission, 2012). While the investment to perform a satisfying DPIA can be substantial, it pales in comparison to the fines when not complying with the DPIA-requirement (Regulation (EU) 2016/679 (GDPR), 2016). This chapter develops a typology of smart city services based on DPIA-needs in terms of resources.

The geographical scope is constrained to the Flanders region in Belgium. Flanders is one of three regions in Belgium with proper authorities and consists of 308 municipalities in five provinces (Screen Flanders, n.d.). Comprising an area of 13,522 km^2 and almost six million people, it has a dense urbanization (Leinfelder & Allaert, 2010; Flemish Institute for Biotechnology, n.d.). The region can be characterized as a metropolitan area with multiple centers (Boussauw et al., 2018). As of January 2019, five cities have over 100,000 inhabitants, Antwerp being the largest with a population just exceeding 500,000 (Statbel, 2019). The region is interesting as a case study because of its potential for generalization, specifically to other polycentric, highly urbanized areas, an urbanization type that is becoming more important worldwide (Eurostat, 2016; Liu & Liu, 2018). Additionally, previous research showed a clear demand from local administrations for tools reducing perceived complexity (Desdemoustier & Crutzen, 2017; Smart City Institute, 2018). Conceivably this is the case for most regions internationally, especially areas where data protection and privacy legislation are still in their infancy stages. The potential for novel insights is further maximized as the DPIA-practice in this region has not yet been studied.

We visualize our main proposition in Figure 4:

Proposition - P. As the complexity of the urban environment in which a smart city service is offered and the complexity of the smart city service itself increase, so do the costs of performing a DPIA on that smart city service, ceteris paribus.

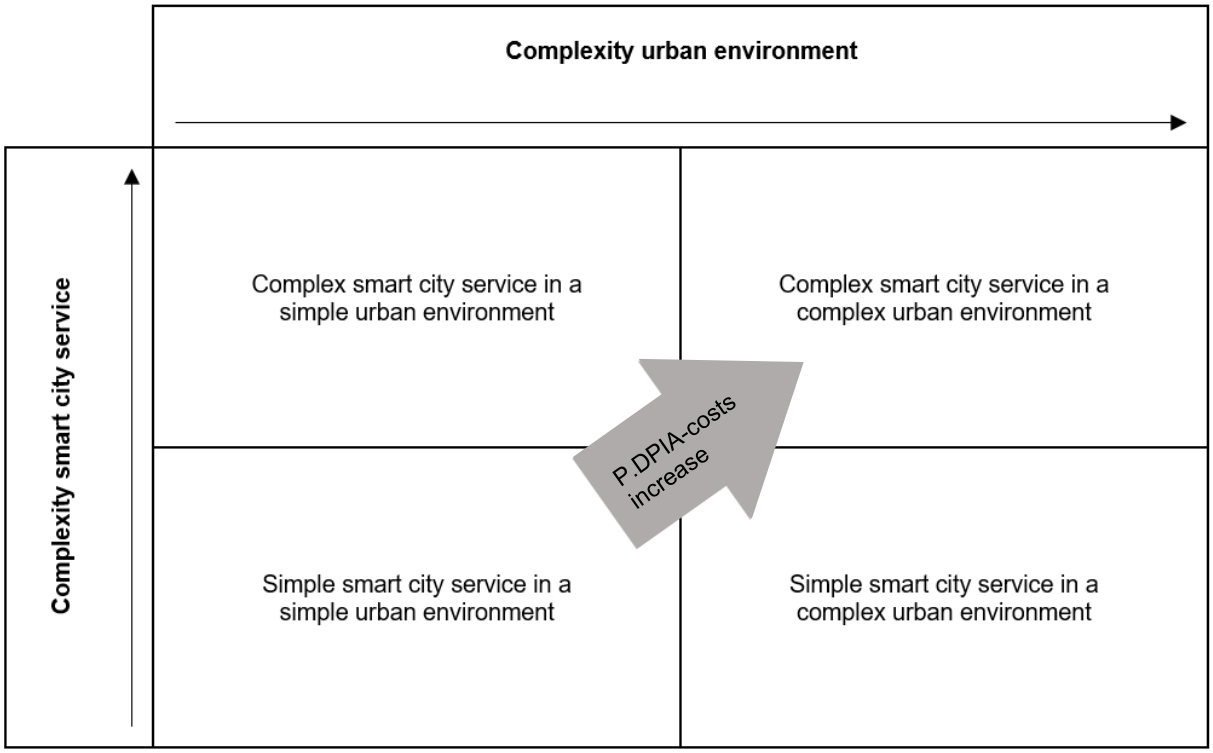

Figure 4. Main proposition. Source: own creation based on the dimensions discerned from the literature review.

4. Methodology

In an initial phase, we presented the test matrix based on the two dimensions identified during the literature review, i.e. the complexity of the urban environment in which a smart city service is provided and the complexity of the smart city service itself, to a diverse group of smart city stakeholders. For this purpose, we organized a workshop where stakeholders could provide input on the theory-based framework. Additionally, DPOs of city administrations and SCSPs were interviewed to further refine the conceptions of complexity and their cost implications for DPIAs. The interview results were illustrated with a selection of authentic early-stage Flemish smart city services.

4.1. Workshop

First, an interactive workshop was organized. Twenty-two prominent smart city actors were invited. These actors were selected based on their experience with and interest in DPIAs on smart city services. The focus was on more senior profiles. The attendance rate was at 50%, with attendees representing various interests: multiple Flemish city administrations, a regulator, a smart city testbed, the private sector, and civil society. A pseudonymized overview of the workshop participants can be found in Table 6.

Organization	Function
Civil society	Media coach
Flemish city	Application specialist data management
Flemish city	Coordinator information security
Flemish city	Coordinator smart city projects
Flemish city	Legal advisor
Industry umbrella organization	Top executive
IT company	DPO
IT company	Strategic buyer
Regulator	Legal advisor
Smart city incubator	Member advisory group
Smart city incubator	Top executive

Table 6. List of workshop attendees' profiles. Source: own creation based on the stakeholder workshop.

We opted for a workshop set-up, as a form of participatory research, to gather a wide range of views of smart city actors. This bottom-up approach then serves as a starting point for follow-up in-depth interviews (Cornwall & Jewkes, 1995). Participatory research accommodates for illuminating discussions between actors in the field and leaves them in charge of pinpointing critical common issues (Brown, 1985). As they are arguably very well placed to identify potentially interesting areas of study, this constitutes one of the strengths of this method (MacDonald, 2012). Moderators were asked not to contribute any content to prevent their influence on the data (Kerr, Farrukh, Phaal, & Probert, 2013). Additionally, the variety of actors guarantees the quality and representativeness of the obtained results (Kerr et al., 2013). As described below, the chosen set-up leaves room for consensus-building and analysis by the workshop participants but at the same time ensures that all actors are heard and that their potentially diverging opinions are documented (Phaal, Kerr, Ilevabre, Farrukh, Routley, & Athanassopoulou, 2016). This modus operandi directly remedies one of the main drawbacks of the workshop method, i.e. that one or a few actors dominate the debate by virtue of their personality or their role in the smart city realm (Cornwall & Jewkes, 1995). Workshops perform particularly well in new areas of research where information is scarce (Ørngreen & Levinsen, 2017).

The workshop was subsequently designed following the principles outlined above. First, the eleven participants were allocated to four smaller groups each moderated by a member of the academic research team. Each actor was asked to individually write down reflections regarding the question: how do urban complexity and complexity of smart city services influence data protection costs? This starting point allows participants to draw from their own experience without interference by others. Subsequently, each group was asked to discuss the results and to make a summary table. Moderators limited their interventions to the minimum, and encouraged all participants to share their thoughts. Next, discussion results were presented by the spokesperson of each group, feeding into a plenary debate. The moderators took notes of the main takeaways. These discussions among participants enabled us to confront specific views at an early stage.

4.2. Interviews

While stakeholder input through a workshop was invaluable for the conception of the relevant dimensions of complexity, it is equally important to validate the matrix by means of individual in-depth interviews with DPIA-experts. Interviews are preferred because of the relatively new nature of the DPIA and the need for flexibility in exploratory research (Fossey, Harvey, McDermott, & Davidson, 2002; Lowe, 2005). We opt for semi-structured interviews to guarantee a certain comparability between the qualitative data (Bogner, Littig, & Menz, 2009).

Nine semi-structured face-to-face expert interviews were conducted between 7. March 2019 and 24. April 2019. We interviewed four DPOs of Flemish cities and five DPOs of private SCSPs. The interviews vary between 40 and 80 minutes and were recorded and subsequently transcribed verbatim. Participants received their transcriptions and could correct errors. To safeguard the anonymity of the respondents, we use pseudonyms. Interviewees were questioned in Dutch about their organization, DPIAs in general, their methodologies for conducting such assessments, costs related to DPIAs and factors that influence the cost level. Their respective experience levels with the DPIA-process are displayed below in Table 7.

Interviewee	**DPIA-experience**
City DPO 1	DPIA completed
City DPO 2	Preparation stage
City DPO 3	DPIA completed
City DPO 4	DPIA completed
SCSP DPO 1	DPIA completed
SCSP DPO 2	Preparation stage
SCSP DPO 3	DPIA completed
SCSP DPO 4	DPIA completed
SCSP DPO 5	Preparation stage

Table 7. DPIA experience level of the questioned DPOs. Source: own creation based on the interviews.

The data protection officer (DPO) plays a key role in the DPIA-process. The GDPR requires the appointment of a DPO for data controllers and data processors, barring limited exceptions, in cases where the data controller or processor is a public actor, i.e. also cities, or where core activities of data controller or data processor involve data processing that entails "*regular and systematic monitoring*" of a large amount of data subjects, or where data controller or data processor process large quantities of "*special categories of data*" (Regulation (EU) 2016/679 (GDPR), 2016). It can be inferred that a considerable variety of smart city actors will be obliged to appoint a DPO. Following their function description, a DPO works on all operations within the organization that involve personal data protection, can provide advice regarding the implementation of the DPIA, and monitors its implementation (Regulation (EU) 2016/679 (GDPR), 2016). Given this strong involvement, the DPO constitutes an appropriate interview subject.

To optimize comparability, we exclusively focus on DPOs. While this approach might overlook data protection considerations at other levels of the organization, this disadvantage is outweighed by the methodological soundness of diligent comparisons. Both public sector and private sector DPOs were approached. Thirty-four DPO-offices of Flemish cities were contacted regarding experience in conducting DPIAs and willingness to participate in an interview. Cities were selected based on population size, which was used as a proxy for data protection expertise within the city administration. We received five positive responses. The main reason for the small final sample is that experience with the DPIA is very scarce and concentrated within the relatively large city administrations. As a consequence, the most knowledgeable local experts were questioned. An exhaustive database of SCSPs does not exist. However, two organizations, i.e. Smart Cities Vlaanderen and Agoria, offer the possibility to self-identifying SCSPs to join their online communities and increase their visibility (Reynaert, 2018; Smart Cities Vlaanderen, n.d.). The 'Smart Cities Vlaanderen' community encompasses 127 companies active in 'Smart Government'-projects (Smart Cities Vlaanderen, n.d.). We contacted the 123 firms of which contact details were published on the website and asked: i) whether they had already conducted a DPIA, and, ii) whether their DPO would be willing to accept an interview. The response rate was at 24% although only four could respond affirmatively to both questions, this again underlining the scarcity of knowledge on the DPIA. The community of Agoria, the umbrella organization of Belgian technology companies (Agoria, n.d.), consists of 94 companies active in the smart city market (Reynaert, 2018). As there is an overlap of 17 companies with the Smart Cities Vlaanderen community, only the remaining 77 firms were sent the same request. The response rate was at 26% of which only one company responded positively to both questions. In total nine interviews, four with public sector DPOs and five with private sector DPOs, were conducted.

Interviewees were explicitly asked to reflect on the relevance of the various dimensions of complexity for the costs of DPIAs in the context of the Flemish smart city. Open coding was organized by dimension of complexity, the code tree can be found in Figure A.1 in Appendix 1.

4.3. Smart city cases

To illustrate the practical value of the matrix, interview results were combined with an evaluation of early-stage Flemish smart city services in terms of their complexities. Currently, a database of Flemish smart city services does not exist. However, considering the aims of this chapter, it is important, on the one hand, to include a wide variety of services, and, on the other hand, to focus on recent services. To satisfy these two criteria, to maximize comparability between cases and to minimize methodological and conceptual confusion, we study twenty-one smart city services that received funding through the most recent 'City of things'-call of Vlaio, the Flemish agency for innovation and entrepreneurship (Flemish Agency for Innovation and Entrepreneurship, 2018). Methodologically, this

modus operandi has several merits. First, as the definition of a smart city service is contested, using services from only one project call at least implies consistent application of the definition to all. Nonetheless services were still tested against the following smart city service definition: a smart city service is a service that provides a solution for a social problem based on technology but with interaction with the physical world where data collection and use are central and involves several stakeholders, both public and private (Neirotti et al., 2014; Walravens & Ballon, 2013). Second, the 2018-call of Vlaio maximizes contemporary relevance through leaving out outdated initiatives, as well as services that were not confronted with GDPR-requirements.

The main applicant of each service was approached via electronic mail to provide their request form for the 2018 Vlaio 'City of Things' project call. We expect that the request form includes information on the respective dimensions (Flemish Agency for Innovation and Entrepreneurship, 2018). It is important to note that these request forms outline the smart city services as the service applicants envision them before any real feasibility study has taken place. While this reduces the practical usefulness, the classification of this type of early-stage services is still interesting and valuable. The response rate of 48% (10/21) allows for a meaningful analysis (Baruch, 1999; Mellahi & Harris, 2015). Three services were excluded because they were purely digital in nature and did not contain a connection with the physical world as our definition of smart city service requires. Services included in the analysis can be found in Table 8.

#	**Short service description**
1	Neighbors support – low-threshold system to realize neighborhood-oriented care
2	Museum of Things for People – IoT set-up to follow visitors and create interest profiles
3	Municipal sensor network for air quality measurements
4	Sharing parking information with all types of application developers
5	Connected public lighting on bicycle paths
6	Mobility management with automatic number plate recognition (ANPR)-cameras
7	Using ANPR cameras for non-police purposes

Table 8. Included services Vlaio-call. Source: own creation based on Flemish Agency for Innovation and Entrepreneurship (2018).

5. Results

5.1. Workshop

Smart city stakeholders largely agreed that data protection costs increase as the two dimensions, urban environment and smart city service, become more complex. This can be deduced from the group discussions as well as from the takeaways of the plenary debate: as the actors explicitly separated the discussions following the two dimensions, they grant a substantial role to each of them. However, stakeholders differ in their opinions regarding complexities. With respect to the complexity of the urban environment, the debate showed that most stakeholders believed that the diversity of

stakeholder interests is most significant but other factors, e.g. scale, were also referenced. Concerning the smart city service, the workshop showed mostly, but not exclusively, complexity stemming from the number of data streams a particular service requires and from the amount of use-cases (Plenary debate takeaways, personal communication, 12/12/2018). It is clear that urban environment complexity and smart city service complexity are layered. Both dimensions and the layers identified during the course of the workshop are displayed in Table 9, for each individual layer also the key impact on the DPIA is summarized and a link to the academic literature is given.

Dimension	**Layer**	**Key impact DPIA**	**Reference**
Complexity urban environment	Size of city	More users, larger area to protect	Braun, Fung, Iqbal, & Shah (2018)
	Diversity of urban stakeholders	Managing data protection	Bresciani, Ferraris, & Del Giudice (2018)
	Total of smart city services	Connecting and combining data	Fung et al. (2012)
Complexity smart city service	Number of different data streams	Mapping (changing) data streams and their risks	Edwards (2016)
	Clarity of data controllership	Data roles and data responsibilities	Finch & Tene (2018)
	Amount of use-cases	More uses and corresponding risks	Puiu et al. (2016)
	Invasiveness	More sensitive data requires better protection	Acquisti, Taylor, & Wagman (2016)
	Visibility	External services are under more scrutiny	Bouranta, Chitiris, & Paravantis (2009)

Table 9. Refined dimensions with layers. Source: own creation based on the stakeholder workshop.

We now study and explain the different layers of the two main dimensions as depicted in Table 9. For each consecutive layer, the principal workshop comment warranting further investigation is presented and followed by a literature-based review. The three layers of the complexity of the urban environment are tackled first, after which the five layers of the complexity of the smart city service are discussed. The quotes in this section are translated from Dutch and, when necessary, slightly adjusted to improve legibility.

First, we explore the layer city size. This layer was referred to explicitly by a workshop participant:

> *"Offering a smart city service in a small city entails lower costs because of the smaller scale"* (Participant 2 of group 2, personal communication, 12/12/2018).

With increased size comes increased complexity (van Zoonen, 2016). The more inhabitants a city has, the more city resources (in absolute terms) are required to provide a service. Hence, there is a positive correlation between the magnitude of the city population and the cost of a city service. The same holds for the size of the urbanized area, e.g. conducting police controls for five blocks is less costly than

organizing the same for fifty-five blocks. The fact that data is central in any smart city service, adds another dimension to this complexity in terms of human and geographical size of urban areas (Khan, Pervez, & Abbasi, 2017). More potential users of a smart city service bring forth an equivalent increase in the amount of devices at risk, just as a larger surface area to cover entails more Internet of Things (IoT)-components and thus again more devices at risks (Braun, Fung, Iqbal, & Shah, 2018). Also, a larger user base means that in case a data breach takes place, it potentially affects more people; this factor has to be considered explicitly when developing risk-mitigating measures (Wright, 2013).

Second, the amount of different stakeholders involved is of importance. This layer featured prominently in the workshop discussions:

> *"The number of parties is important. Negotiations with individual actors are hard, not to mention negotiating with different and changing actors as in smart cities"* (Participant 2 of group 4, personal communication, 12/12/2018).

Smart cities are prototypes of multi-stakeholder systems (Lim, Kim, & Maglio, 2018; Ruhlandt, 2018); the increasing size and diversity of today's cities create an environment where the stakeholder landscape is constantly growing and changing (Fernández-Güell et al., 2016). Management of complex city systems thus becomes considerably more difficult (Lim et al., 2018). With regard to data protection in general, this difficulty is amplified as having a heterogeneous stakeholder landscape, with different resources and interests, makes developing a coherent data management policy much more challenging (Bresciani, Ferraris, & Del Giudice, 2018).

Next, the total amount of smart city services offered is relevant. One smart city actor stressed this during the workshop:

> *"The fact that there are a number of active projects in smart cities means that the nature of the collected data varies. This then has an effect on data protection complexity"* (Participant 3 of group 4, personal communication, 12/12/2018).

Smart cities revolve around data and interconnectivity (Khan et al., 2017). Securing data from one service in an urban environment might be a complicated endeavor, protecting data from all the interacting smart city services in the city is even more demanding (Edwards, 2016; Ni Loideain, 2018). In terms of data protection, major issues arise from introducing additional smart city services in a smart urban environment. For example, connecting and combining services means connecting and combining various data sources. While these data streams might have limited value individually, a combination could become very valuable (Fung et al., 2012). The more data is combined about a single

person, the more easily that person can be re-identified. Easier identifiability directly affects risks (Fung et al., 2012).

The first layer of the smart city service complexity is the sum of different data streams. During the workshop the layer was addressed as follows:

> *"The city possesses different data streams, sometimes even combinations thereof. As a result the impact assessment becomes more complex"* (Participant 3 of group 4, personal communication, 12/12/2018).

As a DPIA requires a systematic description of all envisaged data processing (Wright, 2013), the more data flows are collected to provide a certain service, the more labor-intensive such an exercise becomes. Additionally, smart city services typically have data flows that might change substantially over time (Edwards, 2016). The DPIA subsequently has to be reviewed each time the risks of the data processing activities change (Bieker et al., 2016; van Dijk et al., 2016), again increasing the costs of performing that assessment.

Clarity of data controllership is key when conducting DPIAs, as stated during the workshop:

> *"The complexity of a project is related to data governance. Figuring out the ownership [sic] of data can take a long time"* (Participant 3 of group 4, personal communication, 12/12/2018).

City administrators might not have the funds or expertise to independently develop smart city services. While in the Flemish context city administrations are the most important instigators of new initiatives of this kind (Desdemoustier & Crutzen, 2017), they have to partner up with private companies to be able to follow-through on services, which could create confusion as to who controls, and thus is responsible for, the data (Finch & Tene, 2018). The resulting intricate data controllership structures also affect data management in general, and the DPIA-process in particular (Finch & Tene, 2018). Mapping interorganizational data streams and having to negotiate with different stakeholders, who have diverse data requirements and interests, is harder than doing the same for a single company; taking effective measures to enforce interorganizational agreements might be even harder (Braun et al., 2018; Wright, 2013). Data governance is again complicated when cloud service providers are involved in data storage, stemming from unclarity surrounding data responsibility (Braun et al., 2018).

Third, the amount of use-cases is important. During the workshop this was illustrated by an experienced participant:

> *"Other actors would like to start using existing sensors for other purposes, this increases the cost of performing the DPIA"* (Participant 2 of group 3, personal communication, 12/12/2018).

A dataset collected through certain services can be used for different purposes. Once the IoT-infrastructure is in place, formatting the data for secondary use can require relatively little effort (Puiu et al., 2016). Evidently, using a dataset for multiple purposes implies more data streams, which entails additional potential risks, subsequently a more extensive DPIA-effort will be required (Ni Loideain, 2018).

Furthermore, the nature of the data collected to provide a service influences the data protection needs. Smart city actors were adamant about the significance of this layer:

> *"Intrusiveness affects costs"* (Participant 2 of group 1, personal communication, 12/12/2018).

Different types of data require, even purely legally speaking, a different level of security and protection (Acquisti, Taylor, & Wagman, 2016). While individual appreciations of what constitutes sensitive personal information differ (van Zoonen, 2016), the GDPR explicitly defines special categories of personal information requiring more protection by virtue of their nature in Article 9:

> "*Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited*" (Regulation (EU) 2016/679 (GDPR), 2016).

The default for these special types of personal data is a prohibition to process, which constitutes a higher level of data protection than of other types of personal data. Article 83 of the GDPR renders the distinction even more explicit by making the size of administrative fines contingent on the type of processing, and on the data affected by a data breach (Regulation (EU) 2016/679 (GDPR), 2016). Conducting a DPIA on an activity which processes special types of personal information will thus be more intensive.

The workshop also pointed to a useful distinction based on visibility, for example when performing DPIAs on external versus internal services:

> *"The more visible a smart city service is, the more effort will go into its DPIA"* (Participant 2 of group 2, personal communication, 12/12/2018).

Whether a service is targeted internally, i.e. towards people within the organization, or externally, i.e. towards third parties, has an impact in other business contexts, for instance in terms of service quality (Bouranta, Chitiris, & Paravantis, 2009). The same argument could be used to argue that visibility would influence the DPIA-exercise. While external customers are free to change suppliers and can do so

relatively easily, internal customers cannot (Johnston, 2008). In the context of the DPIA, efforts put into performing the assessment can be expected to be influenced positively when its subject is an external and visible service, as the risk of losing the customer is higher.

5.2. Interviews and smart city cases

A visual overview of the interview results by layer of complexity is provided in Table 10. Interviewees who had already completed a full DPIA at the time of the interview are indicated in dark grey. A '+' signifies the layer was relevant in the Flemish context according to the interviewee, whereas a '-' signifies it was not, a '+/-' indicates the interviewee tangentially validated the relevance of the layer and 'n.i.' means the interviewee did not comment on the layer. Examples of how signs were attributed are presented in Table 11. The discussion of the interviews follows the structure of the visual overview. Quotes provided in this section were translated from Dutch and, when necessary, slightly adjusted to improve legibility.

Dimension	Layer \ Interviewee	City DPO 1	City DPO 2	City DPO 3	City DPO 4	SCSP DPO 1	SCSP DPO 2	SCSP DPO 3	SCSP DPO 4	SCSP DPO 5	Overall
Complexity urban environment	Size of city	n.i.	+/-	+	+	+	-	+	-	-	+/-
	Diversity of urban stakeholders	n.i.	n.i.	+	+	+/-	+	n.i.	+	+	+
	Total of smart city services offered	n.i.	n.i.	+	+	+	n.i.	+	+	+/-	+
Complexity smart city service	Number of different data streams	+	n.i.	+	+	+	n.i.	+	+	+	+
	Clarity of data controllership	+	-	+	+	+	n.i.	+	+	+/-	+
	Amount of use-cases	+	+/-	+	+	+	n.i.	+	+	+	+
	Invasiveness	+	+	+	+	+	n.i.	+/-	+	+	+
	Visibility	n.i.	-	+	-	-	n.i.	+	+	n.i.	+/-

Legend interview results	+ = relevant	- = not relevant	+/- = somewhat relevant	n.i. = no information provided

Table 10. Visual overview of the interview results. Source: own creation based on the interviews.

Interviewee	Quote	Score
City DPO 3	*"What makes a difference is the number of people, because there is of course a difference between following a class of twenty students or following 86,000 residents. That is a different risk*" (personal communication, 16/04/2019)	+
SCSP DPO 4	*"No, I don't think that's relevant, that does not matter"* (personal communication, 18/03/2019)	-
City DPO 2	*"The larger size of your city allows you to implement a little more policy. So that adds processing activities that have not been done elsewhere"* (personal communication, 21/03/2019)	+/-
City DPO 1	No relevant quote available	n.i.

Table 11. Examples of scoring the city size layer in Table 10. Source: own creation based on the interviews.

Differentiating in city size following the number of residents or the size of the city area is important. One DPO resolutely affirmed the importance of the former, while doubting that the latter had a substantial effect:

> "*What makes a difference is the number of people, because there is of course a difference between following a class of twenty students or following 86,000 residents. That is a different risk …*
>
> *… to cover a larger geographic area you would need more IoT-components, but I think the problems in those potential weak spots will be the same for all individual components*" (City DPO 3, personal communication, 16/04/2019).

A colleague from another city had exactly the opposite reaction. This DPO underlined the importance of the geographical territory covered by a smart city service. The DPO argued that managing and securing the infrastructure component is of specific significance (City DPO 4, personal communication, 23/04/2019). The disparity of opinions illustrates that the impact of the city size depends on the specific situation.

City DPO 2 stressed city size as a proxy for power. It was stated that a larger city usually disposes of more resources and has more room to implement policy in general, which could lead to performing entirely new processing activities (personal communication, 21/03/2019).

Private sector DPOs were divided on the importance of the factor, nonetheless two out of five DPOs explicitly acknowledged its significance. SCSP DPO 3 mentioned the impact of city size on the amplitude of the ensuing risks (personal communication, 27/03/2019), while SCSP DPO 1 stressed the effect on the feasibility of mitigating and resolving risks:

> "*Of course a larger scale means that resolving data protection risks is more difficult. It is mainly about feasibility"* (SCSP DPO 1, personal communication, 22/03/2019).

The case in Box 1 illustrates the influence that city size has on risk and it subsequent effects on the DPIA. Both elements of city size are considered as relevant.

Case illustration: A practical example of the relevance of the factor can be found when contrasting the service that aims to use ANPR-cameras for non-police purposes to the service that targets to install a municipal sensor network for air quality measurements. While the former service is steered by five relatively larger cities in Flanders (Service 7, personal communication, 18/02/2019), the latter is led by a municipality in the province of Vlaams-Brabant (Service 3, personal communication, 12/02/2019). The ANPR-service would require a more extensive DPIA in comparison to the air quality service because more people could potentially be affected by a data breach. In addition, covering a wider geographic area requires more IoT-components. Both introduce additional potential risks, ceteris paribus.

Box 1. Case illustration size of city. Source: own creation based on the smart city cases.

Two DPOs resolutely affirmed the significance of the diversity of urban stakeholders involved (City DPO 4, personal communication, 23/04/2019; SCSP DPO 2, personal communication, 07/03/2019). A city DPO mentioned agreement on risk estimates as a potential issue, but also pointed to the need for a collective legal basis for processing as a potential problem. This seems especially relevant when there is a collaboration between public and private partners:

> *"Yes, the larger the number of stakeholders is, the harder it is going to be to get your risk estimates and your agreements. And with respect to different stakeholder types, you have to keep in mind that if you intend to collaborate with private or non-governmental services, you will have separate challenges for the legal basis of processing*" (City DPO 4, personal communication, 23/04/2019).

However, from the interviews it became clear that the scope of stakeholders' views to be reconciled is more important than the bare amount of stakeholders involved. One DPO of an SCSP explicitly put it like this:

> "*I think it matters in particular to what extent the wishes of those stakeholders differ, that is much more important than the number of stakeholders per se*" (SCSP DPO 1, personal communication, 22/03/2019).

Box 2 contrasts two smart city services that affect different stakeholder groups. The case underlines the relevance of this factor.

Case illustration: The difference between the amount of stakeholders involved in the Vlaio-call service on connected public lighting on bicycle paths and the neighbors care support system offers a useful insight. The smart lighting service identified four groups of relevant stakeholders: young people, cyclists, the two cities that are involved in the service, and developers of technological solutions (Service 5, personal communication, 06/02/2019). The care service identified twenty-three separate stakeholder groups to be involved (Service 1, personal communication, 21/02/2019). Performing a DPIA and reconciling twenty-three potentially different views, will be more difficult than agreeing on a suitable DPIA with only four stakeholder groups, all the rest being equal.

Box 2. Case illustration diversity of urban stakeholders. Source: own creation based on the smart city cases.

DPOs acknowledged the additional risk dimension that comes from introducing a service in a smart environment:

> "*Processor agreements are one-to-one contractual relationships. Of course, in smart city contexts it will be mostly platforms, networks of technologies, that are going to share data, that will of course become a complex matter*" (SCSP DPO 1, personal communication, 22/03/2019).

In particular, the risk of re-identification and the increased potential for harm was brought forward. The more data about users is collected and combined directly affects the effort needed to mitigate and resolve the ensuing risks (SCSP DPO 3, personal communication, 27/03/2019; City DPO 4, personal communication, 23/04/2019).

A private sector DPO pointed to an additional issue, namely the correctness of the data (SCSP DPO 4, personal communication, 18/03/2019). SCSP DPO 4 stated that verifying the correctness and originality of data would be the main issue in an advanced smart city context:

> *"The originality of the data is actually the biggest problem, especially if you have a lot of different devices or Smart services"* (personal communication, 18/03/2019).

As correct data is indispensable to all stages of the DPIA, this also impacts the complexity of conducting such an assessment.

A new smart city service as part of an existing smart city framework or strategy within the urban region demands a more intensive DPIA than a standalone smart city service. The case in Box 3 illustrates that this distinction is valuable in practice.

Case illustration: An example of such a specific difference can be found between the neighbors support – low-threshold system to realize neighborhood-oriented care, that is embedded in a regional smart care strategy (Service 1, personal communication, 21/02/2019), and the municipal sensor network for air quality measurements, that is currently a standalone service (Service 3, personal communication, 12/02/2019). Risks that stem from the connection or combination of databases are higher for the care system, all the rest constant.

Box 3. Case illustration total of smart city services offered. Source: own creation based on the smart city cases.

DPOs indicated that the number of different data streams that a service requires, constitutes an important factor (City DPO 1, personal communication, 14/03/2019; SCSP DPO 1, personal communication, 22/03/2019). A DPO put it succinctly as:

> "*Yes. The more flows, the more risks*" (City DPO 3, personal communication, 16/04/2019).

The amount of different data streams is indeed a key aspect of the complexity of a DPIA. Several DPOs confidently affirmed its importance. Two of the interviewees even stated that it was the main differentiating factor (SCSP DPO 4, personal communication, 18/03/2019; SCSP DPO 5, personal communication, 10/04/2019). The DPO most adamant about the significance of the factor mentioned:

> *"I think the main factor influencing the DPIA-cost is the amount of exchanged data flows"* (SCSP DPO 5, personal communication, 10/04/2019).

Smart city services can differ substantially in terms of the amount of data streams they require. The case in Box 4 illustrates the influence on the DPIA.

Case illustration: The amount of data streams needed to provide a service can vary substantially. An enlightening example is provided by the divergence in the amount of data streams in the parking information service and opening it for all types of application developers on the one hand and the service on connected public lighting on bicycle paths on the other hand. The former would entail twenty-eight distinct data streams (Service 4, personal communication, 19/02/2019), while the latter would only require four (Service 5, personal communication, 06/02/2019). A DPIA on twenty-eight data streams would be more complicated than one on four, ceteris paribus.

Box 4. Case illustration number of different data streams. Source: own creation based on the smart city cases.

Multiple DPOs stressed the significance of the clarity of data controllership (City DPO 1, personal communication, 14/03/2019; SCSP DPO 5, personal communication, 10/04/2019). However, a colleague from a large city was less convinced and mentioned that also processors can be obliged to

do a DPIA in particular cases (City DPO 2, personal communication, 21/03/2019). Nevertheless, it is important to note that this does not exclude that tracking data flows, and assessing and mitigating risks, becomes more complex when external service providers are used. All types of external handling of data: storage, processing, etc., can be of importance as SCSP DPO 4 underlined:

> "*The origin of the data source is key. The less you are in charge, the more complex your system becomes, the more complex it all becomes, because you have to go back to the source to be able to do the DPIA*" (personal communication, 18/03/2019).

Private sector DPOs try to avoid taking the role of data controller, because of the ensuing responsibilities, but instead opt for the role of data processor (SCSP DPO 1, personal communication, 22/03/2019; SCSP DPO 5, personal communication, 10/04/2019). A private sector DPO concluded:

> "*We actually try not to take up a controller role"* (SCSP DPO 1, personal communication, 22/03/2019).

One city DPO affirmed that this avoidance tactic is used in practice:

> "*People also want to get rid of that responsibility of being data controller. They prefer to be processors, and that is sometimes very difficult*" (City DPO 3, personal communication, 16/04/2019).

When key actors avoid their data responsibility, completing a DPIA becomes more complex. Information exchange between parties is crucial.

Box 5 demonstrates in this respect, the set-up of the smart city service and its boundaries are important.

Case illustration: Regarding data controllership, we find illustrative contrasts in two cases involving the use of ANPR-cameras. The service on mobility management plans to render data available to, inter alia, application developers (Service 6, personal communication, 19/02/2019). Thereby it creates data streams that travel beyond the borders of the organization, and even beyond the public sector, making the mapping of the streams and the assessment and mitigation of risks more challenging (Service 6, personal communication, 19/02/2019). Alternatively, the service using ANPR cameras for non-police purposes will not make the data available to private players (Service 7, personal communication, 18/02/2019).

Box 5. Case illustration clarity of data controllership. Source: own creation based on the smart city cases.

Empirical evidence also confirms that adding uses to smart city service data, renders the DPIA more costly (City DPO 1, personal communication, 14/03/2019; City DPO 3, personal communication, 16/04/2019; SCSP DPO 5, personal communication, 10/04/2019). SCSP DPO 3 illustrated this with the case of using images of event cameras to track terrorists:

> "*Today we do data processing at events, for me that makes sense. The day people want to use the same data to track who places bombs in the city, the use becomes completely different. For my DPIA that has a terrible impact*" (personal communication, 27/03/2019).

One DPO of an SCSP voiced a particular view on the issue:

> *"We try to look at the roadmap. There is a certain functionality that we propose at the launch. But if we already have ideas about other future functionalities, we try to actually take that into account when performing the initial DPIA"* (SCSP DPO 1, personal communication, 22/03/2019).

This signifies that the mere possibility of multiple, concurrent use-cases in the future will impact DPIA-costs as potential upcoming uses on the roadmap will already be accounted for in the initial DPIA (SCSP DPO 1, personal communication, 22/03/2019).

Additionally, it is important to be aware of the limits of incorporating use cases in a single DPIA. City DPO 4 stressed this issue when mentioning that once a particular use cannot be classified under the original purpose, a completely new DPIA has to be conducted (City DPO 4, personal communication, 23/04/2019).

Box 6 outlines how the amount of use-cases per smart city service can vary in practice and how this variation affects DPIA-costs.

Case illustration: The number of data uses impacts the difficulty of completing a DPIA. Data collected in the service regarding public lighting on bicycle paths will be used to check the amount of cyclists that ride their bike, at various moments during the day (Service 5, personal communication, 06/02/2019). This is the only foreseen use for the data. In contrast, the service to share parking information with all types of application developers anticipates a wide range of uses, from such as using the data to optimize bussing routes, to notifying first responders more quickly in case of incidents during parking (Service 4, personal communication, 19/02/2019). A DPIA on a service, which collects data with a larger amount of use-cases, will require more resources than one on a service which has only one use-case, ceteris paribus.

Box 6. Case illustration amount of use-cases. Source: own creation based on the smart city cases.

DPOs unanimously confirmed that the DPIA-obligation becomes more costly when the privacy invasiveness of a smart city service increases. A city DPO illustrated the importance of the factor with the following case:

> *"For a certain service we opted for ultrawideband with tags, but smart cameras were another option. I think the resulting DPIA would look very differently, so yes that will certainly have an influence*" (City DPO 2, personal communication, 21/03/2019).

Depending on their conception, smart city services can be more or less privacy invasive. Box 7 portrays a case where a more privacy invasive set-up was contemplated in an early stage, and highlights the evident implications for the subsequent DPIA.

Case illustration: The Museum of Things for People, which is an IoT set-up to follow visitors and create interest profiles, constitutes a clarifying example for the factor invasiveness (Service 2, personal communication, 20/02/2019). In a first phase, different technologies were considered to provide this particular service: from Bluetooth tracking to installing camera's throughout the museum (Service 2, personal communication, 20/02/2019). It is clear that DPIAs for the various set-ups would be quite different. The less invasive Bluetooth option would not record faces, nor would it track eye-movements. The more invasive smart cameras option would record faces and track eye-movements. More invasive services present higher risks and thus require more costly DPIAs, all the rest constant.

Box 7. Case illustration invasiveness. Source: own creation based on the smart city cases.

Various DPOs were convinced of the relevance of the visibility divide, namely because of the higher complexity of data flows for external services and the additional public risks that come from hosting external services (SCSP DPO 3, personal communication, 27/03/2019; SCSP DPO 4, personal communication, 18/03/2019). Interaction with third parties is very important:

> "*Yes. You are going to be much more critical towards services for third parties"* (SCSP DPO 3, personal communication, 27/03/2019).

However, some others DPOs did not think the factor plays a role, or normatively disapprove of differentiating on this basis (City DPO 2, personal communication, 21/03/2019; SCSP DPO 1, personal communication, 22/03/2019). City DPO 4 put it rather strongly:

> "*That makes no difference to me. Personal data is personal data*" (City DPO 4, personal communication, 23/04/2019).

One DPO countered the normative argument by saying:

"*In principle that should not matter, but in reality it does matter*" (City DPO 3, personal communication, 16/04/2019).

While opinions on the relevance of visibility for DPIA-costs differ, in practice some services are clearly more visible than others. Box 8 demonstrates the potential significance of service visibility.

Case illustration: It is clear that services do vary according to the visibility factor. The municipal sensor network for air quality measurements is a service that would be mostly used internally, possibly with one-way external reporting (Service 3, personal communication, 12/02/2019). Overall, this would constitute a relatively low visibility service. However, the neighbors support care system would mostly be used externally, e.g. patients, neighbors, care-givers (Service 1, personal communication, 21/02/2019). This means a broader visibility overall. As a result, external services would require more extensive DPIAs, ceteris paribus.

Box 8. Case illustration visibility. Source: own creation based on the smart city cases.

5.3. Overview

The interviews show that city environment complexity and smart city service complexity seem to be positively associated to DPIA-costs on Flemish smart city services. DPOs of public administrations were more adamant about the relevance of the city environment dimension than their colleagues working at SCSPs. A possible explanation for this disparity could be that some private smart city players opt for a cookie-cutter approach when rolling out services in different loci. Nonetheless, our overall results clearly indicate that 'the smart city' indeed does not exist (Karvonen et al., 2018; Kitchin et al., 2018), and that data protection efforts are to vary according to local needs and characteristics.

However, both public and private sector DPOs agree on the relevance of the smart city service complexity. We demonstrate that, in accordance with the theorizing of van Zoonen (2016) and Wright (2012), there is no one-size-fits-all in data protection for smart city services. Inherent service characteristics play an important role in determining the amount of required resources. While our analysis limits itself to the DPIA, the argument arguably holds beyond this practice. In the smart city realm, smart city services are an instructive level of analysis as it allows for a fine-grained differentiation between smart city modules. Just as 'the smart city' does not exist, nor does 'the smart city service'.

The empirical evidence collected from the workshop and the interviews showed that the following factors influence the cost of performing a DPIA on a smart city Service, ceteris paribus:

i) the diversity of the urban stakeholders involved in a smart city service,

ii) the total of smart city services in the urban region,

iii) the number of different data streams a smart city service requires,

iv) clarity of data controllership,

v) the amount of use-cases, and

vi) the privacy invasiveness of the service.

Two other factors are somewhat more contested, namely i) the size of the city in which a smart city service is offered and ii) the visibility of the smart city service. Some DPOs were convinced of the relevance of city size as an impact factor on DPIA-costs because of the additional IoT-components that are required to scale up a smart city service (City DPO 3, personal communication, 16/04/2019; City DPO 4, personal communication, 23/04/2019). Others were more concerned with generalization and pointed to the similarity of the risks of introducing additional identical IoT-components. In their opinion, the impact on the DPIA could be minimal (SCSP DPO 4, personal communication, 18/03/2019; SCSP DPO 5, personal communication, 10/04/2019). Differentiating DPIA-efforts based on visibility of the smart city service does indeed happen in practice according to multiple DPOs (City DPO 3, personal communication, 16/04/2019; SCSP DPO 3, personal communication, 27/03/2019), even though some of their colleagues normatively disapprove of that practice (City DPO 2, personal communication, 21/03/2019; SCSP DPO 1, personal communication, 22/03/2019).

Building on these factors, we develop a typology of smart city services. Urban differences as well as service related specificities form the backbone of our cost-based model. While our focus has been on DPIA-costs, it can be argued that these go hand in hand with privacy risks. As such, the model is also applicable in a broader context.

The final typology of smart city services based on DPIA-costs can be found below in Figure 5.

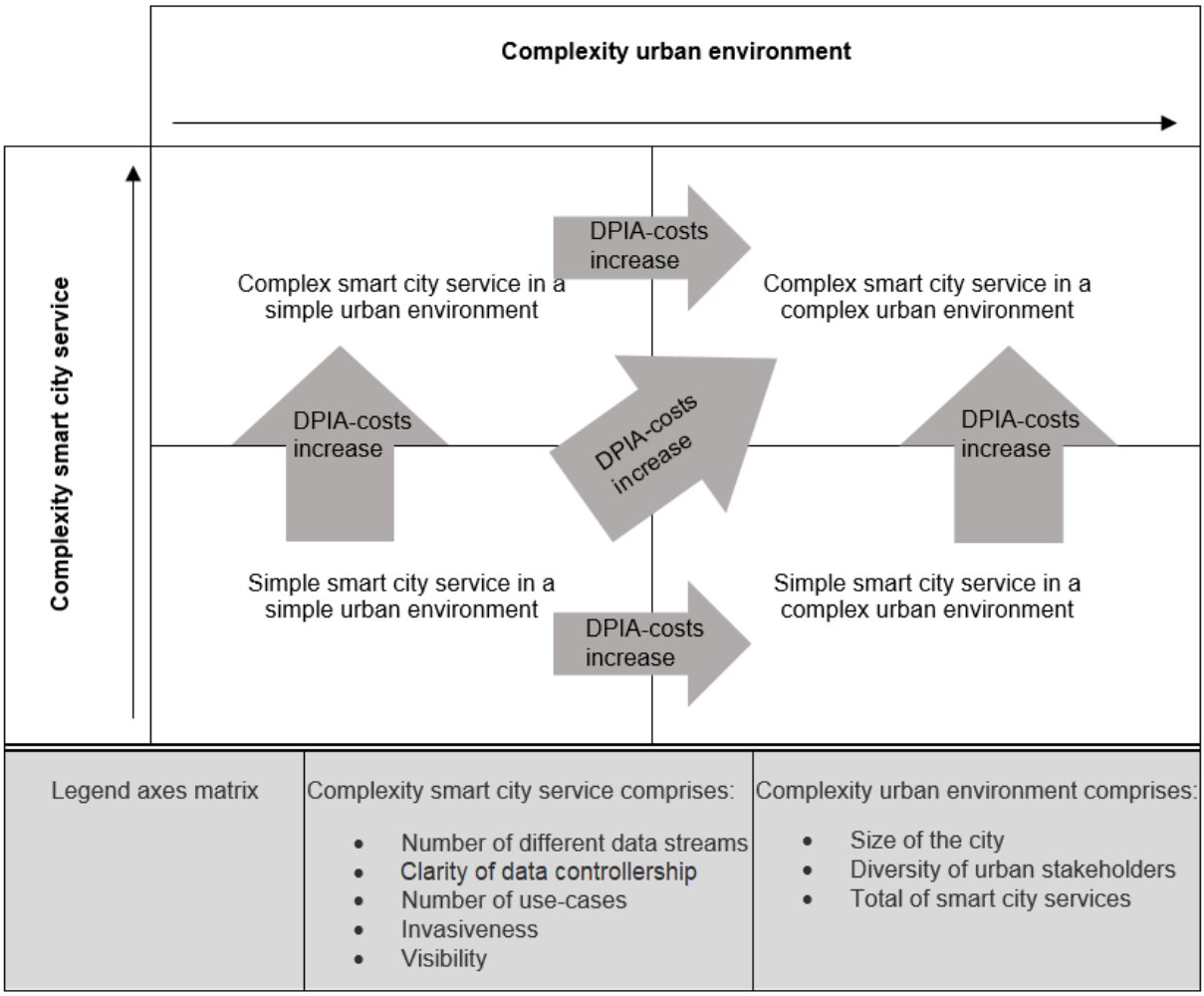

Figure 5. Final typology. Source: own creation based on the literature review, the stakeholder workshop and the interviews.

6. Discussion

The typology transcends the case-by-case analysis while still respecting the specificity of individual cases through the incorporation of an urban environment complexity dimension. In situ models have their own merit, but a more generic framework is needed to perform diligent analyses across and beyond the idiosyncratic. The continuous growth of cities demands a more systematic approach while allowing for inter-case scalability. This scalability relates to specific urban environments in which the typology is applied, e.g. environments with larger cities vs. more rural areas, but also to scalability over time and experience level, e.g. organizational learning effects can make DPIAs less costly overall but the relative cost difference framework remains valuable. We expect that the typology, though based on exploratory research from the Flemish case, can be generalized thanks to the amount of expert knowledge gathered, and especially because of the place-independence of the service complexity dimension. Furthermore, generalizability does not end at EU-borders because the impact-cost-approach is not unique to the DPIA and hence not EU-specific.

The framework breaks down the smart cities concept to a more granular level of services to build a deeper understanding of the 'smartness' of the city. It is exactly this granularity that protects the generalizability of the model. While no two urban environments are fully identical, service provisions can take a very similar form partly because of some technology players holding large parts of the smart city services market.

Data protection and privacy are bound to remain or become crucial issues worldwide, and this typology facilitates the understanding of data protection impact and data protection cost considerations. Furthermore, the model can be instrumentalized to direct (public) investments adding further value. Individual actors, more experienced in data protection procedures, can utilize the model to render DPIAs more cost-effective.

More broadly, as smartness is related to data, data protection can ensure that smartness is durable and sustainable over the long term. Research has shown that a lack of trust in smart city service providers can lead to a decrease in service use (Wright, 2012), arguably a backlash against technological development. Data gathering and data protection are becoming increasingly linked, the Californian, Indian and Chinese initiatives are only the latest in a string of regulatory straightening of historical misalignments (DLA Piper, 2019).

In short, three specific urban recommendations can be derived from the results. First, we recommend a matrix to compare service implementation scenarios and the resulting relative cost variances. Second, we recommend a typology to more efficiently direct financial resources (both public and private resources). A succinct analysis clarifies data protection needs in terms of resources of smart city services. Also, the typology can easily identify similar services and aid in shortening the learning curve for their implementation. Third, we recommend a matrix to explicate smart city service provision decisions and their related impact on the privacy of individuals. We believe that this will foster trust in the urban service provider and allow the actor to build a data protection reputation. We stress the importance of citizen trust to safeguard social cohesion and economic growth.

7. Conclusion and recommendations

This chapter investigates the determinants of the varying DPIA-costs in the context of Flemish smart city services. It was initially theorized that costs vary according to two main dimensions: the complexity of the urban environment in which a smart city service is provided, and the complexity of the smart city service itself.

During a workshop, these dimensions were developed following stakeholder inputs. The complexity of the urban environment is interpreted through three different subdimensions: i) city size, ii) the diversity of the urban stakeholders, and iii) the amount of smart city services in the urban region. This

interpretation leads to three different layers of the concept of urban environment complexity. Similarly, the smart city service complexity is understood in different ways by different participants: i) the amount of different data streams, ii) the clarity of data controllership, iii) the total amount of use-cases, iv) privacy invasiveness, and v) the visibility of the service. Again, these five aspects constitute different elements of the overarching construct.

Data from semi-structured interviews with DPOs from private sector companies, as well as public administrations, validated the relevance of the various layers of both complexities. To a different extent, the urban environment complexity and smart city service complexity influence the costs required to perform a satisfying DPIA. Empirical support is thus found for our initial proposition, namely that as the complexities of the urban environment in which a smart city service is offered and the smart city service itself increase, so do the costs of performing a DPIA on that smart city service.

For public and private stakeholders, the results of this study are useful to classify existing smart city services according to DPIA-costs or data protection requirements. Clustering services based on data protection needs, can make the DPIA-process more efficient. It allows a shortening of the learning curve and improves the quality of decision-making on DPIAs by learning from services that were performed in the same cluster. The proposed matrix reduces the complexity of the smart city service realm considerably by limiting variations to four options, which can be of particular value for actors that have little expertise as well as for players looking for an easy-to-understand framework. Furthermore, the intuitive typology can be utilized to communicate data protection efforts in a more tailored way to a broad audience.

Our analysis is constrained by the limited amount of both qualitative and quantitative data. This was to be expected as DPIA-processes are relatively new and smart city actors are still catching up with the regulation. Further research could extend the findings and the framework to possibly allow scoring of specific projects within the matrix. In order to move beyond conceptual modeling, more smart city service cases need to be documented and studied. This will allow the development of meaningful cut-offs for the various dimensions and layers.

It is important to note that the framework allows for scaling dependent on the specific urban environment. This can be considered as one of the main qualities of the matrix. Research has shown that in smart cities, the context is important: a smart city takes many forms, which widely vary between them (Karvonen et al., 2018; Kitchin et al., 2018). The final output of our analysis fully integrates this insight, as one of the dimensions is explicitly related to the context wherein the smart city service is provided. Nonetheless, the geographical focus of the study constitutes a limitation. As Flanders is

characterized by an urbanization consisting of relatively small cities (Statbel, 2019), the results cannot be simply generalized to larger cities. Further research in different contexts is needed.

Furthermore, the framework is suitable for use by frontrunners in terms of smart city transitioning as well as laggards. The focus on relative cost differences ensures continued usefulness in the sense that the underlying effort differentials are projected to remain valid. The framework can thus grow with the organization, e.g. dealing with learning effects over time.

Alternatively, future studies could broaden the type of interviewees to include project managers and IT-specialists, which could potentially offer different insights into the data protection process and the costs involved.

Likewise, a broader selection of urban stakeholders might be included in future research on data protection in smart city service development. Stakeholder complexity itself is a multi-layered concept and does not only depend on the number of stakeholders related to a specific smart city service and its context, but also to the attributes stakeholders possess (e.g. through differences in power, legitimacy and urgency, see e.g. Mitchell, Agle and Wood, 1997).

Finally, methods to estimate specific direct and indirect costs related to performing DPIAs deserve more attention. Our matrix is built on relative cost differences, but does not examine the absolute size of various direct and indirect costs, which could affect the initial implementation decision of a smart city service. Such an analysis could add an interesting dimension, as we would be able to develop 'veto' thresholds, under which certain smart city services might not be established due to excessive DPIA costs.

Chapter 3. Data control in smart city services: Pitfalls and how to resolve them[6,7]

Abstract

This chapter zooms in on data control in smart city services. Particular characteristics of these services, i.e. data-intensity and complex partnerships, challenge the differentiation between (joint) data controllers and data processors. However, a clear distribution of roles is a precondition for conducting a data protection impact assessment. After a short legal analysis of the data roles, through interviews with nine Flemish data protection officers, we found three situations cause problems in practice: a joint data controller taking up the role of data processor, a joint data controllership set-up, and outsourcing part of the data processing chain. This chapter shows these situations do occur in practice in smart cities and reveals specific problems that arise with respect to the fulfilment of the DPIA-obligation as a result. Problems stem from avoidance behavior towards data protection responsibilities, a general lack of information exchange and limited legal awareness on the part of smart city actors. Subsequently, we propose a set of measures to deal with these issues: linking data costs to data benefits in the rhetoric, integrating comprehensive processing and joint controller agreements in public procurement procedures, and raising awareness internally and externally.

[6] This chapter is published as an article in the European Data Protection Law Review, we thank two anonymous reviewers for their useful feedback on previous versions. Please cite as: "Vandercruysse, L., Buts, C., & Dooms, M. (2019). Data Control in Smart City Services: Pitfalls and How to Resolve Them. *European Data Protection Law Review*, *5*(4), 554–560."

[7] **Author contributions** - **Laurens Vandercruysse**: Conceptualization, Methodology, Formal Analysis, Investigation, Visualization, Writing - Original Draft; **Caroline Buts**: Validation, Writing - Review & Editing, Supervision; **Michaël Dooms**: Validation, Supervision.

1. Introduction

Article 35 of the General Data Protection Regulation (GDPR) installs a mandatory data protection impact assessment (DPIA) for data processing activities that entail '*high risks related to the rights and freedoms of individuals'* (Regulation (EU) 2016/679 (GDPR), 2016). This exercise comprises four steps: giving a comprehensive overview of the planned data processing activity and its purposes, assessing the necessity and proportionality, assessing the risks of data processing, and addressing the identified risks (Regulation (EU) 2016/679 (GDPR), 2016). Intuitively, it is clear the level of complexity of the DPIA-obligation depends on the specific nature and set-up of the data processing activity (Bartoli et al., 2011).

The GDPR also differentiates between two main actors in any data processing activity: i.e. data controllers and data processors. These concepts are central to the GDPR, and their descriptions and obligations are anchored in Articles 24 and 28, respectively (Regulation (EU) 2016/679 (GDPR), 2016). However, identifying data controllers and data processors is in practice not always straightforward. Especially when multiple stakeholders handle data, attributing roles and associated responsibilities can be complicated (Chamoso et al., 2018). These difficulties are amplified when a project entails a cooperation between public and private parties.

This study focuses on smart cities in Flanders, a region that is relatively new to public-private partnerships in such a context (Desdemoustier & Crutzen, 2017). We examine the influence of potential problems when identifying data control on the complexity to the fulfil the DPIA-requirement. In addition, we formulate recommendations on how to deal with such situations.

2. Smart city DPIA responsibilities: Data controllers vs. data processors

The DPIA-process was instituted by the legislator to ensure reflection on data collection, processing and protection, takes place before any new data processing activity is introduced (van Dijk, Gellert & Rommetveit, 2016). The A29WP defines a number of stakeholders to be involved in the exercise: data controllers, data processors, specialized consultants, and data subjects (Article 29 Working Party, 2017). However, central DPIA-stakeholders in practice can be limited to (joint) data controllers, on the one hand, and data processors, on the other hand.

The GDPR states that the (joint) data controller of a data processing is the actor determining the purposes and the means thereof (Regulation (EU) 2016/679 (GDPR), 2016). For example, the data controller is the actor in charge of a decision to improving safety, i.e. the purpose, by installing a number of a particular type of cameras, i.e. the means. The data controller carries the main data protection responsibilities regarding any data and is, as stated in section one of Article 24 of the

Regulation, charged with implementing and documenting all the appropriate safeguards to protect specific data to make sure the GDPR is complied with (Regulation (EU) 2016/679 (GDPR), 2016).

Article four of the GDPR establishes a data processor as '*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*' (Regulation (EU) 2016/679 (GDPR), 2016). The last five words of the definition constitute its most important part. The very definition of data processor already contains a reference to the data controller as being the actor in charge. Further responsibilities of the data processor are outlined in Article 28. Section one stresses the responsibility of data controller over data processor with regard to the adherence to the regulation (Regulation (EU) 2016/679 (GDPR), 2016). It can be deduced the legislator aims to make the data controller carry some risk when employing a data processor which is not compliant. Furthermore, Article 82, which details the potential right to compensation and possible liabilities, explicitly makes the data controller liable for any problems in the data custody chain of its data processing in section two (Regulation (EU) 2016/679 (GDPR), 2016).

Now, conducting the DPIA is a responsibility of the data controller, while the data processor is to provide the data controller with any necessary information (Regulation (EU) 2016/679 (GDPR), 2016). Even though this is a clear division of responsibilities in theory, extant research has demonstrated that the step before the attribution of role-based responsibilities, namely differentiating between data controllers and data processors as such, can be quite challenging (Van Alsenoy, 2019). Distinguishing between data controllers and data processors has long been a difficult endeavor because of certain room for interpretation and the non-mutually exclusive character of the defining features of both types of designations (Van Alsenoy, 2019). Moreover, complicated data controllership structures, which are common in smart cities, also affect data governance and thus the DPIA-process (Finch & Tene, 2018). Similarly, farming out data storage to cloud service providers adds further to the data management complexity, because questions of responsibility for the data in storage arise (Braun et al., 2018; Wright, 2013).

As mentioned, the end responsibility concerning the DPIA lies with the data controller (Bu-Pasha, 2020). This responsibility comes at a cost, e.g. performing the actual DPIA, and comes with accountability, e.g. liability when not conducting DPIA accurately. It might be tempting to avoid this end responsibility by claiming to be a mere data processor. However, it is important to note that Section 10 of Article 28 comprises a caveat to the pure voluntarist distribution of responsibilities over different smart city actors: '*if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing*'

(Regulation (EU) 2016/679 (GDPR), 2016). Here the legislator draws a much needed and clear line with respect to the stretchability of the concept processor.

3. Research questions and objectives

Smart city services put the theoretical division between data controller and data processor under considerable pressure, particularly where services management is conducted through platforms and when they are characterized by substantial out-house processing (Chamoso et al., 2018). Table 12 presents four possible situations, of which three cause problems when performing a DPIA.

Performing a DPIA on a smart city service	
Situation	**Division of responsibilities**
All data processing performed in-house by data controller	Straightforward
Joint data controller taking the role of data processor	Problematic
Joint data controllers	Potentially problematic
Data controller outsources to a data processor	Potentially problematic

Table 12. Scenarios and Division of Responsibilities. Source: own creation based on literature and interviews.

The division of responsibilities is quite straightforward when all activities are in-house. However, three alternative scenarios substantially complicate the division of responsibilities. First, cost minimizing companies have clear incentives to avoid assuming the role of data controller. Formally being a data controller comes with a series of responsibilities and taking on these responsibilities comes at a cost. For a DPIA in particular, the GDPR puts the onus of conducting the assessment on the data controller or the joint data controllers (Regulation (EU) 2016/679 (GDPR), 2016), while the data processors are merely obliged to provide the necessary information to their controller (Regulation (EU) 2016/679 (GDPR), 2016). We briefly remind that decisive power regarding the data processing can shift the data processor into the role of data controller (Regulation (EU) 2016/679 (GDPR), 2016). Therefore, avoiding data controller responsibilities through mere pro forma self-qualification as a data processor comes with a legal risk.

Second, even when there is no avoidance of responsibility, a joint controller set-up is more complicated than a single controller. The GDPR does not explicitly divide the controller responsibilities over the different actors but requires a division to be worked-out contractually (Regulation (EU) 2016/679 (GDPR), 2016). This can lead to potential unclarities regarding the DPIA.

Third, inherent characteristics of smart city services can render outsourcing of data storage and data analysis opportune (Hashem et al., 2016; van Dijk, Gellert & Rommetveit, 2016). While the data controller is still responsible, it becomes dependent on information from the data processor to perform a satisfying DPIA. The more data processors are involved, the more complicated it becomes to conduct a sound DPIA. Each additional actor causes more data flows and subsequently more risks that have to be mapped and mitigated (Finch & Tene, 2018).

Considering these complications, we formulate the following questions:

RQ1. Which problems arise from diverse data control set-ups in Flemish smart city services?

RQ2. How do these problems influence the DPIA process?

RQ3. How can these problems be mitigated?

Answering these research questions provides useful information for decisionmakers in the context of smart city services on how to deal with complicated data control settings and the ensuing cross-organizational and interacting data streams.

4. Methodology

As the GDPR has only been in applicability since May 2018, this research is exploratory. After reviewing the extant literature, we conduct nine semi-structured interviews with data protection officers (DPOs) of Flemish cities and of smart city service providers (SCSPs). Semi-structured interviews are flexible to explore practical phenomena bottom-up and enable a sound comparison of the results (Fossey et al., 2002; Lowe, 2005).

Section one of Article 37 of the GDPR obliges organizations, such as local authorities and cities, to appoint a DPO (Regulation (EU) 2016/679 (GDPR), 2016). Furthermore, private actors processing data that '*require regular and systematic monitoring of data subjects on a large scale*' are captured by this obligation (Regulation (EU) 2016/679 (GDPR), 2016). As a result, most smart city actors have a DPO.

Section one of Article 39 sets out the responsibilities of the DPO. During a DPIA, a DPO provides advice and monitors its correctness (Regulation (EU) 2016/679 (GDPR), 2016). As such the DPO constitutes a very knowledgeable interview subject. Focusing only on DPOs again facilitates sound comparisons of the interviews.

First, thirty-four DPOs of Flemish cities were approached regarding their experience in conducting DPIAs. Out of these thirty-four DPOs, four indicated enough experience and willingness to participate in an interview. While this constitutes a rather low response, we keep in mind the novel character of the topic and the subsequent scarcity of experienced DPOs. Nevertheless, major cities are represented and through the DPOs, we have access to most relevant knowledge.

Second, two hundred SCSPs were found through a publicly available list from Smart Cities Vlaanderen and Agoria (Reynaert, 2018; Smart Cities Flanders, n.d.). Smart Cities Vlaanderen proclaims to be the Flemish smart city community focused on businesses operating in 'Smart Government'-projects and stresses the importance of partnering with all parts of the quadruple helix (Smart Cities Flanders, n.d.). Its databases consist of 127 companies of which 123 made their contact details publicly available

(Smart Cities Flanders, n.d.). These 123 were contacted by email regarding their experience in performing DPIAs. Again, four respondents confirmed experience and accepted an interview. Agoria represents the Belgian technology sector and Agoria Smart Cities publishes a database of 94 smart city companies (Agoria, n.d.; Reynaert, 2018). This resulted in 17 duplicates with the Smart Cities Vlaanderen database. The remaining 77 companies were also contacted. One additional company indicated being quite far advanced in the DPIA process and able to provide useful information.

Subsequently, four DPOs of Flemish cities and five DPOs of SCSPs were interviewed and the interviews were transcribed verbatim. To guarantee the anonymity of the interviewees, we use pseudonyms. Table 13 presents the interviewees and their respective experience in conducting DPIAs.

Interviewee	**DPIA Experience Level**
City DPO 1	Conducted full DPIA
City DPO 2	Advanced planning stage
City DPO 3	Conducted full DPIA
City DPO 4	Conducted full DPIA
SCSP DPO 1	Conducted full DPIA
SCSP DPO 2	Advanced planning stage
SCSP DPO 3	Conducted full DPIA
SCSP DPO 4	Conducted full DPIA
SCSP DPO 5	Advanced planning stage

Table 13. Interviewees and DPIA Experience. Source: own creation based on interviews.

5. Results

This section contains the results of nine semi-structured interviews with DPOs of Flemish cities and SCSPs. The discussion that follows comprises four parts: Part one tackles the specificities of smart cities regarding the relation between data controllers and data processors; Part two describes potential complications that arise when joint data controllers avoid controller responsibilities; Part three zooms in on joint control and its inherent difficulties; and Part four discusses issues when outsourcing to data processors.

5.1. Specificities of smart cities

Smart city services differ in two important ways from other data processing operations, i.e. their public character and the high number of stakeholders involved (City DPO 3, personal communication, 16/04/2019; City DPO 4, personal communication, 23/04/2019; SCSP DPO 1, personal communication, 22/03/2019).

First, the public character of the services impacts data control because getting consent is difficult and sometimes impossible. For example, services like smart public lighting or the use of ANPR-cameras for crowd control operate in public space making it difficult to get consent from citizens that pass by (City DPO 2, personal communication, 21/03/2019; City DPO 3, personal communication, 16/04/2019).

Closely related to the public character is the unavoidability of certain services. Citizens might have no other option but to use the service because of its nature and design (City DPO 4, personal communication, 23/04/2019). From a moral point of view it could be argued that this data should be handled by public bodies (City DPO 1, personal communication, 14/03/2019; City DPO 2, personal communication, 21/03/2019). In public-private partnerships, however, it is likely that data is processed or even controlled by private companies that try to maximize its value.

Second, inherent to smart city services is their wide social reach (City DPO 3, personal communication, 16/04/2019). In addition to the elevated number of stakeholders, DPOs stress the implications of their varying interests and priorities (SCSP DPO 1, personal communication, 22/03/2019). Especially when public and private actors cooperate, control issues tend to arise regarding data processing grounds (City DPO 4, personal communication, 23/04/2019). A DPIA becomes more difficult when data is transferred between organizations. This mainly results from difficulties in aligning data protection policies (City DPO 1, personal communication, 14/03/2019; SCSP DPO 2, personal communication, 07/03/2019; SCSP DPO 4, personal communication, 18/03/2019; SCSP DPO 5, personal communication, 10/04/2019).

5.2. A joint data controller taking the role of data processor

In a joint control setting, it can happen that one of the controllers positions itself as data processor to avoid responsibilities that are inherently linked to the role of controller (City DPO 3, personal communication, 16/04/2019; SCSP DPO 1, personal communication, 22/03/2019; SCSP DPO 5, personal communication, 10/04/2019). Several private sector DPOs indeed confirm favoring the role of processor because of the burden attached to being data controller (SCSP DPO 1, personal communication, 22/03/2019; SCSP DPO 5, personal communication, 10/04/2019). At the same time, private sector DPOs underline their willingness to help data controllers to comply with the GDPR by providing the needed information (City DPO 3, personal communication, 16/04/2019; SCSP DPO 1, personal communication, 22/03/2019).

Depending on the set-up of the cooperation between public and private actors and the type of smart city service, this issue is amplified. Public services and services that handle sensitive information might require a stringent data management policy and an extensive DPIA to fully comply with the GDPR (City DPO 2, personal communication, 21/03/2019; SCSP DPO 5, personal communication, 10/04/2019). When one of the partners evades its responsibility, compliance becomes substantially more difficult. Responsibilities evolve together with the power to extract value from the data. Data controllers decide on the goals and means of data processing and as such decide on the value-extraction. This is a key factor in determining data control (SCSP DPO 3, personal communication, 27/03/2019).

5.3. Joint data controllers

A second potentially problematic situation arises when there are two or more joint controllers. Such a setting requires close cooperation between the joint data controllers to perform a satisfying DPIA (City DPO 2, personal communication, 21/03/2019). Even the decision on joint control itself might be challenging (City DPO 4, personal communication, 23/04/2019).

The information to be exchanged between parties varies but is usually of considerable amplitude. The attribution of roles and responsibilities might already be complicated but setting up secure joint control agreements (JCAs) that establish the responsibilities of all joint controllers is even more so. Nonetheless, the JCA can be a useful tool in that regard. However, for the completion of a DPIA the JCA should be very encompassing. Whether or not data is received from external parties as well as the nature of control constitute major elements when mapping data flows and assessing and mitigating risks (SCSP DPO 4, personal communication, 18/03/2019).

We note that joint control is not always an option for smart city Services. If the controlling parties do not have the same processing goals, nor do they decide on the means of processing together, it will likely result in two separate processing operations which potentially require two separate DPIAs (City DPO 4, personal communication, 23/04/2019; Regulation (EU) 2016/679 (GDPR), 2016).

5.4. Data controller outsources to a data processor(s)

In pure controller-processor relationships problems concerning data control and ensuing responsibilities can also occur. The information provided by the data processors becomes a key input (City DPO 3, personal communication, 16/04/2019; SCSP DPO 3, personal communication, 27/03/2019). As the DPIA-obligation rests on the data controller (Regulation (EU) 2016/679 (GDPR), 2016), a moral hazard problem arises for the data processor. From the latter's point of view, the risks of not providing certain information might not outweigh the competitive risk of disclosing proprietary processing information.

This is reflected in several data processing agreements for Flemish smart city services. While templates have been drawn up by public organizations (City DPO 1, personal communication, 14/03/2019), private partners tend to be wary of signing such documents (City DPO 2, personal communication, 21/03/2019). Local public administrations seem to be catching up, while some SCSPs are already skilled in composing that type of agreements (City DPO 1, personal communication, 14/03/2019).

The provision of information by the data processor is crucial for a DPIA (City DPO 3, personal communication, 16/04/2019; SCSP DPO 3, personal communication, 27/03/2019). If the expectations regarding all parties are not clear from the outset, the cooperation might suffer from time-consuming

meetings to rectify unclarities (City DPO 3, personal communication, 16/04/2019; SCSP DPO 3, personal communication, 27/03/2019; SCSP DPO 4, personal communication, 18/03/2019).

Another issue concerns the required level of detail of the information provided. The processor is responsible for all sub-processors and has a notification obligation vis-à-vis the controller (Regulation (EU) 2016/679 (GDPR), 2016). In practice, however, several parties are unsure about the level of detail to be provided (SCSP DPO 3, personal communication, 27/03/2019). Sub-processors constitute the final layer where problems can arise. While the controller is dependent on the processor for information, the processor relies on the sub-processor (Regulation (EU) 2016/679 (GDPR), 2016). Hence, processors might encounter the same issues at their level of the processing chain as they cause to the level above them.

6. Recommendations

The previous section presents three potential problematic situations that can arise regarding data control in the context of smart cities. These situations have remarkably similar origins and, as will be argued in this section, similar solutions.

Data rewards are linked to data responsibilities. It should be clear from the outset who will benefit from the data processing activity and how this benefit materializes. While all actors gain to a certain extent from being included in a data processing chain, decision-making actors, i.e. controllers, will be able to benefit more. It should be made clear that not formally assuming the role of data controller might be cost minimizing for some actors in the short run, but there is a real risk that this approach might not be profit maximizing, e.g. through legal risk. A clear division of responsibilities benefits all actors involved. Processing agreements could be formally integrated in the procurement process of local administrations (City DPO 2, personal communication, 21/03/2019). The bidder directly signs the data processing agreement and is bound by its terms when the bid is launched (City DPO 2, personal communication, 21/03/2019). The unilateral imposition of such an agreement facilitates the process and avoids unclarities afterwards.

The same approach could be taken for joint controller agreements. As such, rather than resorting to time-consuming ad-hoc problem solving, the division of responsibilities could be dealt with in a decisive manner when concluding the contract.

The provision of information up and down the processing chain is crucial. The type and detail of information that should be provided by each actor should be stipulated at the beginning of a data processing collaboration. Again, for public-private partnerships, this agreement could be integrated in the public procurement process. A clear chain of responsibility between controller and processor but

also between processor and sub-processor, should incentivize actors to take ownership. Partners higher up the processing chain should harness their power when contracts are concluded.

Awareness regarding potential data protection issues is often lacking in the organizations involved in a smart city project. First, it is important that public procurement divisions are aware of the difficulties encountered by smart city projects when data protection issues are not embedded in the procurement process. Potential problems as outlined above should be explained during workshops or dedicated learning moments. Data protection should be an organization-wide endeavor. Second, in-depth knowledge and expertise is crucial. Data protection personnel should be trained on relevant legal aspects and limitations.

Also, awareness about the legal position of the smart city actor in a smart city constitutes a matter of concern. Even when there is substantial internal awareness, this should still be disseminated beyond the organization. Especially smaller cities and SCSPs might not have data protection expertise in-house resulting in a minimal effort/cost approach. Such actors should be informed that avoidance of responsibility at the start of the project does not exempt them from legal responsibility later. The most important legal concepts, including the difference between data controller and data processor should be clearly explained.

Table 14 provides an overview of the potential problems and recommendations.

Performing a DPIA on a smart city service		
Situation	**Potential issues**	**Recommendations**
Joint data controller taking the role of data processor	Avoiding responsibility over data Lack of information Lack of awareness	• Stress link with value-extraction • Integrate JCAs in public procurement • Embed information provision duties in JCA from the start • Raise awareness internally • Raise awareness externally
Joint data controllers	Lack of information Lack of awareness	• Integrate JCAs in public procurement • Embed information provision duties in JCA from the start • Raise awareness internally • Raise awareness externally
Data controller outsources to data processor	Avoiding responsibility over data Lack of information Lack of awareness	• Integrate processing agreements in public procurement • Embed information provision duties in processing agreement from the start • Raise awareness internally • Raise awareness externally

Table 14. Summary of results. Source: own creation based on own research.

7. Conclusion

This study examines how particular data control settings influence the complexity of performing a DPIA for a smart city service. Nine semi-structured interviews were carried out with public and private sector DPOs. It seems that three specific set-ups cause problems concerning the DPIA, namely i) when a joint data controller takes the role of data processor, ii) when there are joint data controllers, and iii) when the data controller outsources to a data processor.

The issues that arise in the three situations are similar. They range from smart city actors avoiding data protection responsibilities, to a lack of information exchange between partners in smart city services, and to a general lack of awareness within and across smart city actors regarding legal responsibilities and corresponding room to maneuver. These constitute substantial problems when fulfilling data protection duties such as a DPIA.

We propose a combination of measures to resolve these practical problems in DPIA implementation. First, we suggest the formal integration of the processing agreement and JCA in the public procurement process. This binds private partners to a certain division of responsibilities ex ante. Second, information provision duties are incorporated in the processing agreement and JCA to avoid time-consuming ad-hoc meetings. Third, awareness should be raised within the organization. Data protection awareness should not be limited to data protection and IT departments but should be an organization-wide endeavor. Fourth, awareness should be raised beyond the organization to all partners of the smart city project. Most issues likely originate from a misconception by smart city actors regarding leeway that the GDPR offers in terms of sharing and avoiding data responsibility. As experience and knowledge between actors differs substantially, smart city service partnership meetings should become places of learning.

Chapter 4. The DPIA: Clashing stakeholder interests in smart cities?[8,9]

Abstract

The development of a smart city hinges on the collaboration of various stakeholder groups with diverging interests. From a technological perspective, smart cities are often considered as the pinnacle of urban efficiency. From a business perspective, there is a straightforward financial incentive to subscribe to that narrative. However, from a societal perspective, there is a clear friction regarding several values and norms. Data protection constitutes one such important area of conflict. This chapter focuses on the data protection impact assessment (DPIA) in the context of smart city service development, and identifies and evaluates the various stakeholder interests that feature during this particular data protection interaction.

Through sixteen data protection expert interviews, we identify eleven pertinent, distinct interests: i) compliance, ii) cost control, iii) data management, iv) efficiency, v) generation of trust, vi) income acquisition, vii) limiting impact on service performance, viii) reputation building, ix) risk management, x) safeguarding competition, and xi) safeguarding data security. The interests can be categorized in a financial, competition/ competitiveness, social, and risk theme. Using the analytical hierarchy process (AHP) method, we evaluate the salience of the interests in the context of the DPIA. We find generation of trust, safeguarding data security, and risk management to be the most salient. The relative lack of importance of financial and competition/ competitiveness interests is remarkable.

The results of this exploratory research support all smart city stakeholders in clarifying and rationalizing their data protection interactions, and serve as indicators for potential DPIA pitfalls. Furthermore, stakeholders can use these findings to maximize their influence on the DPIA through coalition building. Data protection authorities can utilize this explorative study as a starting point to develop participation guidelines. Diligent stakeholder interest consideration is central to sustainable smart city development, this chapter lays the groundwork for further research.

---

[8] This chapter is published as a chapter in Data Protection and Privacy Volume 14: Enforcing Rights in a Changing World, we thank two anonymous reviewers for their useful feedback on previous versions. Please cite as: "Vandercruysse, L., Dooms, M., & Buts, C. (2021). The DPIA: Clashing Stakeholder Interests in the Smart City? In D. Hallinan, R. Leenes, & P. De Hert (Eds.), *Data Protection and Privacy Volume 14: Enforcing Rights in a Changing World*. London: Bloomsbury Publishing."

[9] **Author contributions** - **Laurens Vandercruysse**: Conceptualization, Methodology, Formal Analysis, Investigation, Visualization, Writing - Original Draft; **Michaël Dooms**: Conceptualization, Methodology, Validation, Writing - Review & Editing, Supervision; **Caroline Buts**: Conceptualization, Validation, Writing - Review & Editing, Supervision.

1. Introduction

The development of smart city (SC) services requires cooperation of multiple stakeholders (Ruhlandt, 2018). There can be no SC service without a smart city service provider (SCSP) nor without an urban area to provide the service in.[10] Furthermore, it is evident that attracting and retaining users is key to any service provision. Additionally, sitting at the nexus of service provision, public governance and technological evolution, it is important SC growth is duly managed and regulated. The intricate ecosystem thus also requires regulation to guide stakeholders, consequently adding a regulator to monitor compliance. In general, the development of SC services is hence characterized by interactions between a wide variety of stakeholders, and the associated data protection interactions are no exception.[11]

This chapter focuses on one specific data protection interaction, namely the data protection impact assessment (DPIA). The DPIA, which was introduced by the general data protection regulation (GDPR), allocates the responsibility for assessing the impact of certain data processing activities on data protection to the data controller (Regulation (EU) 2016/679 (GDPR), 2016). From a stakeholder analysis perspective, the DPIA constitutes an interesting case for two main reasons. First, the DPIA is a relatively new data protection interaction and, as a result, can be expected to provide a more flexible development of stakeholder interactions than more established, formalized processes. The novelty leads to situations in which the various stakeholders still have to find their place and voice. Second, while the responsibility for the DPIA rests firmly on the data controller, the legislator chose to distribute some accountability to other stakeholders (Regulation (EU) 2016/679 (GDPR), 2016). This adds importance to the DPIA from the perspective of multiple stakeholders, and high-stake interactions tend to be characterized by more true interest revelations (Smith & Walker, 1993).

Taking into account the particular set-up of SC services, we conduct an explorative, descriptive analysis of stakeholder interests. First, we investigate which stakeholder interests emerge during the DPIA (RQ1). To that end, we carry out sixteen interviews with data protection experts representing an array of different SC stakeholder groups. Second, we evaluate the salience of the identified stakeholder interests during the DPIA (RQ2) by applying the analytical hierarchy process (AHP) method. As a case-study, we chose the region of Flanders, Belgium. Focusing on SCs in Flanders as a single case-study ensures an elevated value-added as: i) DPIA research with a regional focus is scarce, ii) data protection expertise in the region is limited (Desdemoustier & Crutzen, 2017; Smart City Institute, 2018), and iii)

[10] SCSP should here be interpreted broadly as any actor who provides a SC service as defined *infra*. However, explicitly excluding any actor merely selling a SC solution and thus not providing a service.

[11] Data protection interaction should here be interpreted as any interaction between various SC stakeholders concerning the topic of data protection.

Flanders constitutes an archetypal example in terms of urbanization in the European context (Tempels et al., 2012).

Stakeholders involved in DPIAs can build on our findings to organize ex-ante reflections on their interests, and how to balance these interests with those of other stakeholder groups. This could lead to more efficient DPIA processes and the formalization of coalitions of stakeholders with similar interests. The results also allow for more normative research in the direction of sustainability guidelines for SC data protection. Inclusive SC governance has been identified as a central success factor for durable and sustainable SC development (Anand & Navío-Marco, 2018), our findings offer novel insights in that regard.

This chapter is structured as follows: Section two presents the fundamentals; Section three comprises the methodology; Section four lays out the analysis; Section five discusses the wider implications of the findings; and Section six concludes.

2. Fundamentals

2.1. DPIAs

The GDPR forms the backbone of the legislative framework concerning data protection in the European Union (EU). The regulation has updated the data protection tools and procedures with regard to the 1995 Data Protection Directive (DPD) in response to the booming digital age (Ryz & Grest, 2016). Overarching GDPR principles encompass among others transparency, fairness and accountability (Goddard, 2017). The European legislator aspired a shift towards responsibilization of stakeholders handling personal data (Clifford & Ausloos, 2018). One specific measure of this responsibilization shift is the DPIA. This assessment of the impact of data processing operations on data protection is a new task attributed to the data controller.

The privacy impact assessment (PIA), sometimes referred to as the forerunner of the DPIA, has been in use as a data protection tool since the 1990's (Tancock, Pearson, & Charlesworth, 2010). The EU introduced its own variant of the DPIA in Article 35 of the GDPR. In case an envisaged data processing activity is anticipated to pose *"significant risks to the fundamental rights and freedoms of data subjects"* a DPIA is to be performed (Regulation (EU) 2016/679 (GDPR), 2016). Following Vandercruysse, Buts, and Dooms (2020) a SC service would constitute "*a solution to a societal demand based on technology that interacts with the physical world, where data collection and data use are central and several stakeholders, both public and private, are involved.*" (3) (Neirotti et al., 2014; Walravens & Ballon, 2013). This definition includes large-scale, systematic monitoring of public space, which is explicitly mentioned in paragraph 3 of Article 35 as a processing requiring a DPIA (Regulation

(EU) 2016/679 (GDPR), 2016). By consequence, it is expected that at least a subset of SC services would be subject to the DPIA obligation (Bu-Pasha, 2020).

Article 35 stipulates the specific requirements for such an assessment. It should as a minimum contain the following elements: i) a description of the foreseen data processing operation, ii) a description and justification of the necessity and proportionality of the operation, iii) an identification and assessment of the data protection risks resulting from the introduction of the operation, and iv) a plan with regard to the mitigation of the risks identified in the previous step (Regulation (EU) 2016/679 (GDPR), 2016).

The DPIA process aspires ownership of data protection choices, and ensuing risks, by data controllers. However, the design of the actual processes of DPIAs is largely left to the stakeholders in charge (Belgian Data Protection Authority, 2018). It is exactly this freedom of movement in terms of processes, and more particularly the freedom to put distinct emphases related to stakeholder interests, that is under investigation in this chapter.

It is vital to note that both the appropriate methodology and scope of the DPIA are subject to debate. Several of the most used methodologies differ quite considerably in terms of approach and focus (Bisztray & Gruschka, 2019; Gellert, 2018; Hart, Ferrara & Paci, 2020; Wright, Finn & Rodrigues, 2013). In addition, some were explicitly developed to suit local or sectoral needs (Georgiou & Lambrinoudakis, 2021; Todde et al., 2020). Regarding scope, for example, certain scholars assess the DPIA to be almost a full-blown fundamental rights assessment (Hallinan & Martin, 2020), while others imply that the DPIA should still focus primarily on (the risks to) the fundamental right to data protection (Demetzou, 2019). In many cases the debates on methodology and scope interlink, as should they. In practice, where in-depth expertise is often lacking and time is a real constraint, scope might follow from the methodology rather than vice versa. In that sense, the choice of methodology becomes all the more important. The width of their variety further underlines the value of this research, since this chapter makes abstraction of concrete methodologies to focus on the underlying interests. Deeper insight in these interests might uncover motives to choose certain methodologies over others. In addition, insights into the generic interests that feature during the DPIA as well as their relative salience should render the exercise more efficient, and could offer regulators a stepping stone to develop suitable (participation) guidelines.

2.2. DPIA stakeholder groups

Traditionally, stakeholders are most commonly identified through their stakes in a focal organization (Frooman, 2010; Frow & Payne, 2011). While this approach allows for, and has explicitly been combined with, a focus on the particular issues that this central organization is faced with, it has been argued that the emphasis on the organization unduly reduces the complexity of current organizational issues (Eskerod, Huemann, & Savage, 2015; Mele, 2002). This is especially problematic when multiple,

conflicting stakeholder perspectives and values are relevant (Roloff, 2008). Seeing the fundamental rights dimension of data protection, it becomes clear that the issues of data protection and DPIA are broader than the boundaries of any focal organization.

For the purposes of this chapter, DPIA stakeholders are thus to be interpreted following an issue-focused stakeholder management approach (Roloff, 2008), the issue at hand being 'the DPIA on a SC service'. In this context, a stakeholder can be defined as in Roloff (2008): "*a stakeholder is any group or individual who can affect or is affected by the approach to the issue*" (238) (Roloff, 2008).

Since the SC is an intricate multi-stakeholder environment, identifying an encompassing stakeholder list for SC issues can be a complex task (Calzada, 2018). In response, a wide variety of stakeholder categorizations have been developed (Calzada, 2018; Fernandez-Anez, Fernández-Güell & Giffinger, 2018; Haase et al., 2014; Khan, Pervez & Abbasi, 2017; Marrone & Hammerle, 2018; Robert et al., 2017). However, with regard to the DPIA, these classifications tend to be impractical as they gloss over highly relevant inherent DPIA characteristics (e.g. stakeholders concurrently belonging to different stakeholder groups, etc.).

Guidelines by regulators indicate which stakeholders play a role during the DPIA. Two guidelines are particularly relevant for the Flemish SC. On the one hand, there is the WP 248 by the Article 29 Working Party (A29WP). The A29WP is the predecessor of the European Data Protection Board (EDPB), which is the umbrella organization of all European data protection regulators. On the other hand, the national Belgian Data Protection Authority (DPA) issued Recommendation 01/2018.

Table 15 shows that the stakeholder groups comprised in the guidelines overlap considerably but are not identical. We distill our own list of stakeholder groups from the two guidelines, as shown in column three of Table 15. It is important to note that one stakeholder can, even simultaneously, be different types of stakeholders in different data processing operations. Therefore, the list of stakeholders should be interpreted firmly grounded in the specific data processing operation. Per data processing operation, we distinguish five major idiosyncratic stakeholder groups: i) (joint) data controllers, ii) data (sub-) processors, iii) specialized consultants/ researchers, iv) citizens, and v) the data protection authorities. What follows is a description of these different stakeholder groups.

DPIA stakeholder groups according to A29WP (Article 29 Working Party, 2017)	DPIA stakeholder groups according to Belgian DPA (Belgian Data Protection Authority, 2018)	DPIA stakeholder groups according to chapter
Data controllers	Controllers	(Joint) data controllers
Processors	Processors	Data (sub-)processors
Specialized consultants (internal, e.g. DPO and CISO, or external)	DPO	Specialized consultants/ researchers
Data subjects	Population concerned or their representatives	Citizens
	Population at large	
	Regulators	Data protection authorities

Table 15. DPIA stakeholder groups according to A29WP and Belgian DPA. Source: own creation based on respective guidelines.

2.2.1.(Joint) data controllers

A data controller decides independently on the purposes and means of the processing operation (Regulation (EU) 2016/679 (GDPR), 2016). Article 24 of the GDPR details the responsibilities of the data controller. These include the installation of the appropriate safeguards, both on a technical and an operational level, to guarantee that the operation complies with the regulation all along the processing chain. The DPIA is one of the specific obligations resting on the data controller under the GDPR (Marelli & Testa, 2018).

When more than one stakeholder decides on the purposes and means of a processing operation, they become joint controllers (Regulation (EU) 2016/679 (GDPR), 2016). The regulation stipulates that a division of responsibilities should be outlined contractually between the partners and that this should be clearly communicated. With regard to the DPIA, representatives of the different controllers can thus take all decisions jointly or tasks could be divided to some extent (Vandercruysse, Buts & Dooms, 2019).

2.2.2.Data (sub-)processors

Data processors can be used to process data that the controller has chosen to collect (Tikkinen-Piri, Rohunen, & Markkula, 2018). It is instructive to think of the processor as an instrument of the controller. Article 28 of the GDPR demarcates the responsibilities of the data processor (Regulation (EU) 2016/679 (GDPR), 2016). The processor is being utilized contractually by the controller to achieve predefined purposes through predefined means. An example could be a data controller that wants to map traffic flow densities through the use of cameras, and therefore enters into a contract with a data processor that will execute the idea. Note that a data processor in turn might outsource part of its processing to one or more sub-processors, creating a third processing layer (Regulation (EU) 2016/679 (GDPR), 2016).

With respect to the DPIA, paragraph 3 of Article 28 clearly states that the processor needs to assist the data controller in conducting this assessment by providing the necessary information (Regulation (EU) 2016/679 (GDPR), 2016). Technical information concerning the processing set-up used by the processor is needed to conduct a full DPIA, without this information risk estimations are deficient (Lindqvist, 2018).

2.2.3.Specialized consultants/ researchers

Specialized consultants and researchers can play a role in an advisory or control capacity. Paragraph 2 of Article 35 of the GDPR explicitly refers to the data protection officer (DPO) to be consulted in the DPIA process (Regulation (EU) 2016/679 (GDPR), 2016). Even though the explicit references to specialized consultants stop there, it might be useful to involve other specialists as well. In the context of Flemish city administrations a lack of data protection knowledge leads to the consultation of outhouse expertise (Desdemoustier & Crutzen, 2017), e.g. data protection lawyers and information security specialists. While not being standard procedure, some organizations regularly outsource substantial parts or even the entire DPIA process (Blume, 2018; Kloza et al., 2020). The European regulator explicitly foresees a situation where an external consultant becomes the leader of a DPIA (Article 29 Working Party, 2017).

2.2.4.Citizens

Citizens are stakeholders in the DPIA as *"where appropriate"* they should be consulted regarding their opinions by the controller (Regulation (EU) 2016/679 (GDPR), 2016). However, the controller can argue that such a consultation is in contravention to *"commercial or public interests or the security of processing operations"* (Regulation (EU) 2016/679 (GDPR), 2016). In contrast to the A29WP, which refers to 'data subjects', and the Belgian DPA, which differentiates between the 'population concerned or their representatives' and the 'general population', we opt for the more neutral 'citizens'. At the time of conducting the DPIA, i.e. ex ante the processing, any differentiation or specification is void of practical use. Especially regarding SC services, it is often impossible to narrow the 'general population' to the 'population concerned' or to a subset of potential 'data subjects' at this stage (an exception would be smart grids (Otuoze, Mustafa & Larik, 2018)). Following the definition, data collection in the context of a SC service regularly takes place in the public space. Therefore, one could argue that everyone who could ever utilize this public space, i.e. every citizen, is a 'concerned person' or 'data subject.'

In short, citizens do not have a fixed role in the DPIA process, despite their data being directly or indirectly used in the data processing operation. The feasibility of collecting a representative sample

as well as of doing a public consultation on the DPIA altogether remains an open question. The use of civil society organizations as a proxy could constitute an elegant solution to the sampling problem.

2.2.5.Data protection authorities

Finally, the national DPA can be an important player as the regulator overseeing compliance with the GDPR and the national data protection laws (Belgian Data Protection Authority, n.d.). In that regard, the DPA has consultation and control competences over the DPIAs performed within its jurisdiction (Regulation (EU) 2016/679 (GDPR), 2016). Additionally, paragraph 1 of Article 36 foresees for data controllers to consult the DPA when the controller feels that risks remain after implementation of the mitigation measures as indicated in the provisional DPIA (Regulation (EU) 2016/679 (GDPR), 2016). When asked for consultation, the DPA can provide advice in written form (Regulation (EU) 2016/679 (GDPR), 2016). Knowing the consequences of going against the advice of the authority, the controller should seriously consider the remarks (Albrecht, 2016).

2.3. Diverging and dynamic interests

Research has shown that stakeholder interactions tend to be more problematic when parties' interests differ (Axelsson & Granath, 2018; Grossi & Pianezzi, 2017; Herrschel, Dierwechter & Dierwechter, 2018; Moura & Teixeira, 2009). Generally, previous research on SC issues opposes business interests and (human) values such as transparency and trust (Capdevila & Zarlenga, 2015; Kitchin, 2016). However, too often these discussions merely offset a neoliberal dystopia, i.e. a SC solely created by and for business, with a co-created, participatory-governed utopia (Galic & Schuilenburg, 2020). Both SC versions then have fierce, natural proponents in the form of stakeholders, i.e. private business for the former version and citizens and civil society for the latter. We argue that the simplification of different stakeholders to unidimensional actors driven by irreconcilable goals and interests is injudiciously reductionist. The eventual SC will likely be neither a dystopia nor a utopia, but rather a set-up achieved through pragmatic compromise between stakeholders along the spectrum. In that sense, recognizing that the interests of the various stakeholder groups are not homogeneous is of vital importance. Also, the interests of stakeholders might change depending on the particular subject matter that is discussed. This means that it is important to note that one is a stakeholder in a wide variety of processes and procedures rather than 'a stakeholder in the SC.' In this chapter, we aim to provide a deeper and more granular understanding of what the particular interests are that feature in the DPIA and how these interests relate to one another in terms of salience.

So we argue that interests concerning the DPIA do not depend solely on individual stakeholder characteristics, but also on the stakeholder group that stakeholder belongs to in the specific context of a data processing operation. Any stakeholder involved in the data processing operation will belong

to one of the stakeholder groups outlined in Section 2.2 vis-à-vis that particular data processing. Inherent interests will be filtered through the lens of the legal role the stakeholder takes up.

It is instructive to think of inherent interests as the interests that are fundamental to the type of stakeholder, e.g. for a private business that would be income generation or cost effectiveness. Now, the stakeholder group to which the stakeholder belongs in the context of data processing also comes with a set of interests; these are then called data processing interests. For a data controller this could be diligent data management or transparency, while for a data processor this could be cost minimization. To perform a meaningful interest analysis, the end result of the interaction between both types of interests has to be studied rather than either category of interests in isolation. A concrete example can be found in contrasting the situation wherein a local public administration acts as the data controller of a certain processing activity with the one where the local public administration takes on the role of a processor. While the interests inherent to the local public administration remain the same, the data processing interests actually change. As a data controller, the administration has an incentive to perform the risk mapping of the DPIA very thoroughly, which might include performing audits of the data (sub-) processors. However, as a data processor, the same administration has a clear financial incentive to minimize the number of audits that are performed on its systems and processes.

This section highlighted the importance of the insights that this chapter sets out to gather. Two interlinked research questions will be answered:

RQ1: What are the different interests that feature during the DPIA?

RQ2: What is the salience of these identified interests?

2.4. Sustainable SC development

The development of SC services is currently often managed top-down, even though there is a growing body of academic literature underlining the importance of more inclusive governance modes and a general human-centric approach (Andreani et al., 2019; Calzada, 2018). Of course, the arguments in favor of inclusivity transcend the specific field of SC service data protection. Nonetheless, data protection offers a natural starting point to move towards SC development that is more inclusive, more human-centric, and more sustainable, because the GDPR requires by law that an assessment is made to balance business and the protection of fundamental rights in the form of the DPIA (Regulation (EU) 2016/679 (GDPR), 2016). This anchoring in law increases the success probability of an overhaul vis-à-vis situations where proponents of the human-centric approach are condemned to appeal solely on normative grounds. It could be expected that once stakeholders have been introduced to balancing these different values, there might be a spill-over into other domains.

The attainment of smarter, more livable and more sustainable cities is a common goal of all stakeholders, but it is important that strengthened sustainability is reached in a durable, inclusive manner.

3. Methodology

To answer our research questions, we opt for a single case-study. Rather than zooming in on one particular data processing operation, our case study concerns the Flemish SC environment. In concreto, interviewees as well as AHP participants were asked to reason in general terms. This case selection allows us to transcend the idiosyncratic and to gather more generalizable, multi-purpose insights (Seawright & Gerring, 2008).

Flemish municipalities predominantly indicate that they are just starting the SC transition process (Sustainable Development Flanders, n.d.). Multiple rankings show that Flanders is considerably lagging behind some regions in neighboring countries (European Smart Cities, n.d.; IMD Smart City Observatory, 2020). However, in an EU-context, the Flemish region represents the average case, which further safeguards the generalizability of our findings.

In an initial step, we identify the various interests through sixteen exploratory interviews with data protection experts and insights from the academic literature. In a second step, we apply an analytical hierarchy process (AHP) with input from representatives of the different stakeholder groups. This allows us to perform a balancing exercise concerning the interests gathered in step one.

3.1. Interviews

As the DPIA is the responsibility of the data controller, the latter acts as DPIA decision-maker. As this controller functions as a gatekeeper for other stakeholders and their respective interests, it is imperative to study their modi operandi. The DPO, which serves as the data protection expert within organizations (European Data Protection Supervisor, n.d.a), is probably the most knowledgeable person on internal data protection procedures. It should be noted that the GDPR explicates that the DPO is to be independent as well as well-embedded within decision-making organisms in the organization (Regulation (EU) 2016/679 (GDPR), 2016). The A29WP prescribes that the DPO is not to actually conduct the DPIA, but rather provide the necessary advice and guidance (Article 29 Working Party, 2017). Nonetheless, the lack of expertise within organizations arguably leads to a situation whereby the DPO becomes the main steering force behind the DPIA. Furthermore, the A29WP explicitly recommends that the DPO be consulted on, among others, the methodology for the assessment and the GDPR states that the DPO has a control function with regard to any DPIA (Article 29 Working Party, 2016; Regulation (EU) 2016/679 (GDPR), 2016). Based on the above, the DPO can

currently be conceived as embodying the data protection strategy of the data controller. However, this situation is subject to change as intraorganizational awareness and expertise grows.

Additionally, as organizational expertise on data protection is scarce (Desdemoustier & Crutzen, 2017; Vandercruysse, Buts and Dooms, 2019), it is useful to include the views of specialized consultants and researchers. WP 248 by the A29WP clearly indicates that a controller can choose to fully outsource the DPIA process, rendering the paid consultant the de facto DPIA decision-maker (Article 29 Working Party, 2017). It should be noted that the accountability ultimately remains with the data controller (Regulation (EU) 2016/679 (GDPR), 2016). Nonetheless, outsourcing the complete DPIA process signals a shortage of time and/or absence of expertise within the organization. Consequently, an in-depth and critical assessment of the work performed by the consultant is often lacking.

As required to answer research question RQ1, the semi-structured interview allows for bottom-up gathering of noteworthy ideas and concepts (Blandford, 2013). As a result, it serves as a basis to build our stakeholder interest analysis. The individual approach permits candid conversation concerning stakeholder goals without interference and judgment of other stakeholders (Hartmann, 1995).

Concretely, we contact three different types of specialists to optimize representativeness: i.e. DPOs working at public sector data controllers, DPOs working at private sector data controllers, and specialized (research) consultants. Specialists were stratified by their place of work because while the legal roles provide the lenses through which stakeholders regard the DPIA, one could also expect public sector DPOs, private sector DPOs and consultants to have different starting points to which the appropriate lens is subsequently applied. City administrations, SCSP communities, renowned law offices, consultancy practices, and university knowledge centers were all within our scope. A total of 240 organizations was contacted by electronic mail with the question if their primary stakeholder group in the SC was either that of data controller, or that of data protection consultant. If so, they were requested to delegate their DPO, or, when applicable, best placed consultant, to an interview. The vast majority of organizations indicated their experience with the DPIA process was too limited to offer any useful insights. The positive response rate of only 6,67% underlines the scarcity of knowledge on the subject and highlights the added-value of this explorative study. The final sample consists of five DPOs working at city administrations, five DPOs working at private SCSPs, and six data protection consultants.

Face-to-face interviews took place at the offices of the interviewees between March and August 2019, and lasted 40 to 80 minutes on average. Subsequently, interviews were transcribed verbatim. The interview guide can be found in Table A.2 in Appendix 2. Since most interviews were conducted in Dutch, relevant quotes were then translated to English by the authors.

3.2. AHP

As mentioned, the variety of interests gathered during the interviews are then ranked by importance (for the consensus over stakeholder groups as well as for some stakeholder groups individually) through an AHP. The AHP was developed by Saaty around 1980 to aid in complex decision-making (Saaty, 1980). While the tool is mostly used to rank different policy alternatives based on a set of predefined, scorable criteria, the AHP can also be utilized to determine the salience of various interests in a specific context (Amponsah, 2011; Mehregan et al., 2011; Shahin & Mahbod, 2007). As one of the premier multi-criteria decision-making (MCDM) methods allowing for the incorporation of subjective qualitative data (Ramanathan & Ganesh, 1995), the AHP is well-suited for answering research question RQ2.

Following Chen and Wang (2010) and Saaty (2008), conducting an AHP in order to find a relative weighing of different interests comprises seven steps. *First*, the list of relevant interests is compounded, and related interests are grouped together in overarching themes. This is based on the results of the sixteen expert interviews. *Second*, a survey is circulated demanding respondents to perform pairwise comparisons between the importance of themes of interests, as well as of the importance of individual interests belonging to the same theme. In particular, survey respondents attribute a score between 1 and 9 to each comparison; 1 meaning both (themes of) interests are of equal importance, 9 meaning the former of the (themes of) interests is absolutely more important than the latter. Table A.3 in Appendix 2 delves deeper into the concrete scoring mechanism. *Third*, result matrices are developed based on the scores per respondent for the themes of interests as well as per theme of interests. *Fourth*, the leading eigenvectors of the various result matrices are calculated and standardized to sum to one. Relative weights of the themes and individual interests can now be derived. *Fifth*, individual result matrices are converted into result matrices at the level of each stakeholder group, this entails calculating result matrices consisting of the geometric means of the individual result matrices. The standardized leading eigenvectors again represent the respective relative weights. *Sixth*, since we are interested in a global ranking of interests, we calculate the result matrices of the geometric means of the result matrices at the stakeholder group level. This method is preferred over calculating arithmetic averages result matrices, because the influence of weight attributions of individual stakeholder groups is better represented this allows for diverging and even conflicting stakeholder interests (Forman & Peniwati, 1998; Ossadnik, Schinke & Kaspar, 2016). *Last*, the consistency ratio (CR) per matrix is calculated (Saaty & Tran, 2007). This ratio indicates the consistency of the various rankings. A ratio up to 0.2 is considered to indicate a tolerable consistent ranking for grouped responses (Golany & Kress, 1993; Ho, Newell & Walker, 2005; Wedley, 1993).

Over 300 organizations were directly or indirectly contacted to fill out the AHP survey. These organizations encompass all different stakeholder groups identified in Section 2.1. Specifically, we approached: multiple umbrella organizations representing over 250 private companies active in SC projects, over 40 local public administrations, sixteen specialized consultants or researchers, eleven civil society organizations as a proxy for the stakeholder group 'citizens', and five data protection authorities. At the beginning of the survey, organizations were asked to indicate their primary stakeholder group in the SC. They were asked to fill out the survey from that perspective. In the end, eighteen organizations filled out the survey in its entirety: eleven self-identifying data controllers, one self-identifying data processor, four self-identifying specialized consultants and researchers, one self-identifying civil society organization, and one self-identifying data protection authority. In total 32 organizations commenced the survey, of which fourteen organizations dropped out. As participation was terminated just after the research scope and objectives were explicated, the dropout is likely the result of lacking necessary experience. Experiences in the interview process as well as talks with the relevant umbrella organizations taught that only very few SCSPs and local public administrations have concluded a DPIA at the time of writing. The sample of eighteen, while limited, is surely defendable (Boral et al., 2020; Dweiri et al., 2016; Gharizadeh Beiragh et al., 2020; Haber, Fargnoli & Sakao, 2020). Respondents probably represent the state-of-the-art in the Flemish region.

4. Analysis

4.1. DPIA interests

As stated, we conducted exploratory interviews with data protection experts to compile a comprehensive list of interests that feature in the DPIA. The questioning was purposely left open as to not influence the specialists. Interests purely related to the form of the DPIA were excluded as they are outside the scope of this study. The results are displayed in Table 16.

Interest	Short description	Most mentioned by
Compliance	Making sure the company is compliant with the current legislation	SCSP DPO
Cost control	Limiting investment in the DPIA process	Cons
Data management	Making sure the data protection and data management policies are aligned	SCSP DPO
Efficiency	Maximizing simplicity, and efficacity, of DPIA working processes and procedures	Cons
Generation of trust	Generating trust in citizens from within the organization	City DPO
Income acquisition	Making sure the person performing the DPIA keeps an eye on the current product offering of the company and can signal if opportunities for new, complementary products would arise from e.g. the mapping of the new data flows	Cons
Limiting impact on service performance	Limiting the impact of data protection on the performance of the service	City DPO
Reputation building	Making sure potential business partners are aware of the organization's data protection efforts	City DPO/ SCSP DPO
Risk management	Making sure data protection risks are limited to a level the organization is willing to carry	Cons
Safeguarding competition	Making sure data protection requirements do not impact the ability of smart city actors to compete	Cons DPO/ SCSP DPO
Safeguarding data security	Making sure the collected data is secure	City DPO/ SCSP DPO

Table 16. List of interests. Source: own creation based on interviews.

We now briefly explain each of these interests, we will tackle them in alphabetical order.

4.1.1.Compliance

A first DPIA interest is pure compliance (Kwon & Johnson, 2013). Compliance of the DPIA should be interpreted as the DPIA fulfilling all explicit legal demands, each demand can be thought of as a separate box and a compliant DPIA would tick all these boxes (Zerlang, 2017). A legal data protection consultant considered this interest to be primordial (Cons 1, personal communication, 24/04/2019). While this interest might sound like a conditio sine qua non for any business procedure, in practice it seems that there sometimes is a disparity. An interviewee explained that this interest stems from an effort to rectify historical misalignment of data processes and IT-infrastructures with data protection legislation (Capgemini, 2019):

> *"An important factor would be to just comply with the legal provisions of the GDPR. Actually straightening the nonconformity from a historical point on view*" (City DPO 2, personal communication, 21/03/2019).

4.1.2.Cost control

The importance of limiting financial investment in the DPIA process is also regularly mentioned during the interviews. Financial costs can be related to attributing manhours, hiring legal or technical expertise, procuring technical products, or instituting novel organizational measures (Bergkamp, 2002; Data Protection Commission, 2019). As private sector businesses are profit-maximizing, cost considerations feature in all decision-making processes. A consultant noted that cost control is indeed important, but limiting costs has to be evaluated on a case-by-case basis, as cost control is always relative to a reference price:

> *"A very important thing is indeed to take financial cost as a reasonable consideration. You just can't ignore that. But what it costs exactly, that depends on the project*" (Cons 3, personal communication, 22/07/2019).

Additionally, cost control was interpreted by a private sector DPO as limiting costs springing from performing DPIAs which are not up-to-par, notably because of underestimations of risk or the utilization of very strict legal interpretations (Bojanc & Jerman-Blažič, 2008; SCSP DPO 4, personal communication, 18/03/2019).

4.1.3.Data management

Third, the experts refer to the alignment of data protection and data management policies (Thompson, Ravindran, & Nicosia, 2015). The DPIA process offers an opportunity to reflect on new data streams in a very systematic way. This allows for a rationalization of data management procedures (Horák, Stupka, & Husák, 2019). A private sector DPO stated that this interest constitutes the most salient in the current era of the ever growing data realm:

> *"Certainly for the private sector, the use of a lot of Cloud and SaaS-solutions makes your data management a huge exercise and it is difficult to restrain that growth. One of the biggest challenges for me today is just keeping data flows and data under control*" (SCSP DPO 3, personal communication, 27/03/2019).

It is important to note that there are benefits to be had from doing the DPIA with an eye on the data management. Smart fact-based data management facilitates efficient resource allocation because all data is secured in an optimal way, i.e. not 'over-secured' (Cons 2, personal communication, 16/07/2019).

4.1.4.Efficiency

Efficiency has to be interpreted as dealing with data protection in a simple, methodical way. While efficiency can have a financial component (European Data Protection Board, 2019), it should be seen

more broadly as maximizing simplicity, and efficacity, of working processes and procedures while still reaching the DPIA objectives (SCSP DPO 4, personal communication, 18/03/2019). The concern of data protection, and the DPIA, becoming a hindrance for staff is shared across sectors (Oderkirk, Ronch, & Klazinga, 2013). A public sector DPO mentioned weighing legal needs and practical implications:

> *"I mainly think that the practical in relation to the purely legal is a factor to be reckoned with. Pragmatism is very important to me, also in terms of budget*" (City DPO 3, personal communication, 16/04/2019).

Data protection consultants are primarily concerned with 'sensible' efficiency. More particularly with regard to the DPIA, scoping and project management are vital to handling the DPIA process efficiently (Cons 2, personal communication, 16/07/2019). Efficiency can be interpreted as dealing with the DPIA obligation in a methodical way:

> *"I think efficiency is very important. You have to get the right profiles together from the start. You have to establish the right rhythm to review the DPIA. One of the biggest problems I see in doing DPIAs is the lack of a plan, there is no thought-out approach*" (Cons 3, personal communication, 22/07/2019).

4.1.5.Generation of trust

Next, there is an interest in generating trust in SC projects (Yeh, 2017). As trust is generated through interaction, most respondents consider this to be part of their awareness and communication campaigns (City DPO 2, personal communication, 21/03/2019). Trust is emitted, thus the DPIA process should be used as a lever to induce staff with a data protection mindset (Wright, 2013). One public sector DPO stated exactly that:

> *"To me, awareness among employees is most important. People who think about the concepts of data protection and privacy; that is something that has really taken off lately*" (City DPO 2, personal communication, 21/03/2019).

Furthermore, the DPIA effort should not end when the document is 'finalized'. Transparency is a central principle in the GDPR and a data protection policy should abide by that (Wright, 2012). Interviewees plan to clearly communicate about their efforts, also regarding the DPIA. Citizens should know what their data is used for and what the ensuing risks are. Transparency induces trust. This interest has gained importance due to the currently perceived 'Big Brother'-society (SCSP DPO 1, personal communication, 22/03/2019; Cons 6, personal communication, 28/08/2019). Flemish citizens regard the SC as a potential privacy threat (imec-SMIT-VUB & imec.LivingLabs, 2019). Multiple

respondents mentioned that once trust is gone, it is very hard to get it back. It is clear that a lack of communication is detrimental to the survival of the SC. One private sector DPO put it strikingly as:

> *"It is very important to persuade people that our services are not terrifying*" (SCSP DPO 1, personal communication, 22/03/2019).

4.1.6.Income acquisition

A sixth interest is the possibility of acquiring income as a result of the DPIA exercise. While a DPIA is initially costly, a well-designed DPIA could also indirectly generate income (Cons 4, personal communication, 30/07/2019). Mapping novel data flows might lead to the discovery of new, complementary products that the data controller can then commercialize. However, the potential for revenue generation depends on the profile of those performing the DPIA as well as the time available to investigate all options (Cons 3, personal communication, 22/07/2019). This is a contingency that, at this time, is often not met in practice. Most businesses thus tend to see the DPIA process as a pure cost:

> *"I see the GDPR as a necessary evil instead of something that actually generates income*." (SCSP DPO 5, personal communication, 10/04/2019).

4.1.7.Limiting impact on service performance

Pragmatism featured frequently during the interview series. Having a data protection policy and conducting a required DPIA is important. However, for most interviewees data protection does not constitute their core business. A service is designed to perform a function and the obligatory DPIA is another hurdle to take (Song et al., 2012). The idea that the central functions of the service are to be kept and that the data protection considerations should not unnecessarily impede business goals is a recurring thought (Lenard & Rubin, 2010; City DPO 2, personal communication, 21/03/2019). Notwithstanding that substantial efforts and investments are required for the DPIA, the core business remains central. A well-thought out GDPR strategy might partly resolve the tension between service performance and data protection (SCSP DPO 1, personal communication, 22/03/2019). Service performance does not equal service quality, as one interviewee stated:

> *"Realizing data protection and DPIAs in a good way is a quality, because you give the people involved a higher level of privacy*" (Cons 5, personal communication, 13/08/2019).

4.1.8.Reputation building

An interest related to the competitiveness of SC stakeholders in the data economy is the development of a data protection reputation (Fombrun & Shanley, 1990; Wright, 2012). We interpret reputation building as making sure potential business partners are aware of the organization's data protection

efforts. Evidently, a strong reputation for data protection can induce citizen trust, but building a reputation is a broader concept (Casaló, Flavián & Guinalíu, 2007; City DPO 4, personal communication, 23/04/2019). For example: an established data controller publishing a full DPIA report on its website could garner trust from citizens who perceive this as very transparent, while business associates might positively or negatively judge the procedures on a more technical level. Alternatively, investing in two-factor authentication software might not necessarily prompt higher trust levels of citizens, but could boost reputation with potential collaborators.

4.1.9.Risk management

A substantial part of the DPIA process is about mapping and mitigating uncovered risks of the data processing activity (Article 29 Working Party, 2017). Risk management in that context is to be understood as an individual interest. While risk management efforts cover fields beyond data protection, for data controllers and processors the DPIA constitutes an integral part of risk management (Trudel, 2009). The DPIA could be used as a tool to establish the optimal level of risk for the controller or processor. A data protection consultant stated this to be the foremost criterium:

> *"The most important criterium is risk reduction to a level that is acceptable for the organization, to result in an acceptable level of risk for the organization*" (Cons 2, personal communication, 16/07/2019).

4.1.10. Safeguarding competition

Competition is crucial in a free market economy (Lipczynski, Wilson & Goddard, 2005). Data protection obligations can be perceived as additional hurdles to competition for data processing services (Engels, 2016). These markets are already notoriously concentrated (City DPO 3, personal communication, 16/04/2019; Cons 5, personal communication, 13/08/2019). The DPIA, being a quite intensive and costly exercise, can present an obstacle for some small or new providers (Cons 3, personal communication, 22/07/2019). It is possible to instrumentalize the DPIA to safeguard competition by providing some of leeway as well as clear guidelines. A city DPO illustrated this as follows:

> *"We actually have a policy that aims to attract start-ups, avoids extensive order books, and uses a shortened tendering procedure for all IT purchases. We try to lower the threshold*" (City DPO 4, personal communication, 23/04/2019).

Additionally, the DPIA can be used as a signal from the SCSP demonstrating that their product is safe and that data risks are well-considered (Wright, 2013). Such a signal, optionally combined with a recognized certification scheme, could stimulate competition (Cons 2, personal communication, 16/07/2019).

4.1.11. Safeguarding data security

Three quarters of the specialists indicate safeguarding data security as an interest. Data security is important in a broad sense, regarding data protection as well as the DPIA process (European Data Protection Supervisor, n.d.b; van der Haak et al., 2003). Its substance was stressed in multiple interviews:

> *"I think everything starts and ends with data security*" (Cons 3, personal communication, 22/07/2019).

Additionally, a 2019 citizen survey in Flanders and Brussels reveals data security as one of the most important considerations for citizens in the SC (imec-SMIT-VUB & imec.LivingLabs, 2019).

Central to the IT-infrastructure, data security constitutes the backbone of a good data protection policy (Court of Justice of the European Union, 2014; SCSP DPO 3, personal communication, 27/03/2019). Performing a DPIA without a correct securitization of data is futile (Kitchin, 2016; City DPO 1, personal communication, 14/03/2019).

Another more specific contemplation related to data security was access control. During the DPIA, the access control procedures could be optimized (SCSP DPO 5, personal communication, 10/04/2019).

4.2. DPIA themes

It can be argued that some of the interests in Section 5.1 are more closely related than others. Consequently, we opted to group connected interests in overarching themes. This grouping constitutes a useful overview and is necessary for the two-layered AHP ranking process in Section six.

Four main themes can be discerned: i) financials, ii) competition/ competitiveness, iii) social, and iv) risk. The financials theme consists of three underlying interests. The common denominator is the relation to the financial situation of the organization conducting the DPIA. Income acquisition and costs control go to the raison d'être of private business. Efficiency, though broader than just financial, relates to the avoidance of indirect costs. The theme comprising limiting the impact on service performance, reputation building and safeguarding competition is named competition/ competitiveness. The two former interests concern the competitiveness of individual organizations; having a more performant service will render an organization more competitive, just like having a better reputation will. The latter interest goes to managing broader market dynamics. Trust generation is classified under the social theme, as this generation of trust requires widespread internal and external interaction. Last, the risk theme encompasses four different interests: compliance, data management, risk management, and safeguarding data security. Following Gellert (2018), we consider compliance to be intrinsically related to risk in the sense that, although GDPR principles are not scalable, their implementation is to some

extent (Gellert, 2018). In practice, compliance levels do vary, and different compliance levels entail their proper of legal risk. In short, data management goes to managing operational risk. The risk management interest has to be interpreted as establishing the optimal level of overarching risk for the organization. Evidently, safeguarding data security concerns technical risk.

An overview of the composition of the themes is presented in Table 17.

Theme	Interest and preference	Justification
Financials	Cost control	Inherent financial component
	Efficiency	
	Income acquisition	
Competition/ competitiveness	Limiting impact on service performance	Primarily impact competition for SC services, either directly or through effect on competitiveness of individual actors
	Reputation building	
	Safeguarding competition	
Social	Trust generation	Communication and awareness strategies
Risk	Compliance	Risk management, either legally or technically
	Data management	
	Risk management	
	Safeguarding data security	

Table 17. Four DPIA themes and their composition. Source: own creation based on interviews.

4.3. Coming to a consensus

4.3.1.The general consensus

Eighteen individual respondents representing all five DPIA stakeholder groups identified in Section 2.2 participated in the AHP process. While the sample is limited, it suffices for the explorative purposes of this study (Nikou & Mezei, 2013; Sambasivan & Fei, 2008). The DPIA is indeed a relatively novel specialist process and knowledge on the subject is limited. Furthermore, a higher quantity of respondents does not necessarily indicate a better representation of the subject as the quality of respondents prevails for an AHP process.

To find the general consensus weights for each interest, grouped responses per stakeholder group were weighted equally. We thus determine an ideal situation wherein stakeholder groups are thoroughly consulted and their remarks are considered carefully, we find this situation to be most insightful as a baseline for further research. In Table 18, the general consensus weights are displayed.

Theme	Weight	Interest and preference	Weight
Financials	10%	Cost control	1%
		Efficiency	6%
		Income acquisition	3%
Competition/ competitiveness	8%	Limiting impact on service performance	2%
		Reputation building	4%
		Safeguarding competition	1%
Social	32%	Generation of trust	32%
Risk	50%	Compliance	6%
		Data management	7%
		Risk management	15%
		Safeguarding data security	22%

Table 18. Results global AHP. Source: own creation based on AHP analysis. Note: CRs of all matrices are <0.2.

Even though risk is the most salient theme according to the data protection experts, generation of trust is essential when performing a DPIA. During the interviews, generation of trust and safeguarding security were also indicated as crucial. Financial and competition/ competitiveness considerations do not feature prominently.

4.3.2.Contrasting public and private data controllers

SC services can be developed by both the public and private sector. The responsibility for the subsequent DPIA can thus lay on either a public organization or a private company. We briefly analyze whether interests also depend on the sector of the stakeholder responsible for the DPIA. Geometric averages are calculated of the matrix inputs of all respondents identifying themselves as primarily public data controllers. We do the same exercise for private data controllers. These weights are shown in Table 19.

Public data controllers			Private data controllers	
Interest	**Weight**		**Weight**	**Interest**
Cost control	3%		1%	Cost control
Efficiency	6%		3%	Efficiency
Income acquisition	1%		2%	Income acquisition
Limiting impact on service performance	2%		2%	Limiting impact on service performance
Reputation building	4%		9%	Reputation building
Safeguarding competition	1%		2%	Safeguarding competition
Generation of trust	47%		57%	Generation of trust
Compliance	8%		9%	Compliance
Data management	7%		6%	Data management
Risk management	6%		5%	Risk management
Safeguarding data security	14%		5%	Safeguarding data security

Table 19. Contrasting public and private data controllers. Source: own creation based on AHP analysis. Note: CRs of all matrices are <0.2.

As presented by Table 19, the attributed weights are quite similar for public and private players. However, notably generation of trust seems to be even more important to private sector data controllers. This might be the result of a disadvantage at the starting point, as they are sometimes perceived less trustworthy than their public sector counterparts (imec-SMIT-VUB & imec.LivingLabs, 2019; van Zoonen, 2016). Another explanation could be that a loss of trust is harder to recover from for businesses (Braun, Fung, Iqbal & Shah, 2018). Additionally, also reputation building is more salient an interest for the private sector. Being competitive in a trust-based niche thus requires a solid reputation. Safeguarding data security was assigned a considerably higher weight by public sector controllers, possibly because of a sector wide information security awareness campaign (Flemish Government, n.d.).

4.3.3.Contrasting data controllers and specialized consultants/ researchers

Another potentially interesting distinction in DPIA interests can be found between internal staff conducting DPIAs and external specialists. Seeing the scarcity of data protection expertise in the Flemish SC, there is high practical relevance in this comparison.

We calculate the geometric mean of the result matrices of all data controllers as well as the geometric mean of the result matrices of all specialized consultants/ researchers. The results are shown in Table 20.

Data controllers			Specialized consultants/ researchers	
Interest	**Weight**		**Weight**	**Interest**
Cost control	2%		1%	Cost control
Efficiency	5%		6%	Efficiency
Income acquisition	2%		1%	Income acquisition
Limiting impact on service performance	2%		5%	Limiting impact on service performance
Reputation building	5%		3%	Reputation building
Safeguarding competition	1%		2%	Safeguarding competition
Generation of trust	50%		28%	Generation of trust
Compliance	9%		9%	Compliance
Data management	7%		6%	Data management
Risk management	6%		22%	Risk management
Safeguarding data security	11%		16%	Safeguarding data security

Table 20. Contrasting internal and external DPIAs. Source: own creation based on AHP analysis. Note: CRs of all matrices are <0.2

Some of the numbers in Table 20 are remarkable. Data controllers tend to stress trust generation as an interest when performing DPIAs. However, specialized consultants and researchers attribute considerably more weight to risk, in particular risk management and safeguarding data security. This can possibly be explained by the fact that specialized consultants and researchers are hired expertise, and they might focus more on objective, measurable indicators. Such measures are more convincing for the client than the more intangible generation of trust. Also both the data controller and the specialized consultants might consider generation of trust an internal task.

5. Discussion

The originality of the research is both in the used methods and its substance. The novelty of the substance is four-pronged.

First, we have demonstrated a generic role-based approach to the stakeholder system implicated in the DPIA process coupled with associated interests. An easy-to-operationalize stakeholder framework to research the issue of DPIA was missing, as is clear from the plethora of SC stakeholder classifications available in the literature (Marrone & Hammerle, 2018; Haase et al., 2014; Robert et al., 2017). The explicit establishment by the legislator of legal roles in the DPIA process is interesting from a stakeholder management point of view as it formalizes the involvement of a number of predefined stakeholder groups, while leaving the concrete methodologies and practicalities up to the controller decision-maker. An academic field which has outgrown sole preoccupation with the financial interest of a central organization and is moving into ever expanding subject matters, can learn from the results of this study in the sense that legal grounding of formal involvement can rationalize stakeholder

analyses and provide much needed clarity in the stakeholder management practice. Even though the stakeholders were mapped with an eye on the DPIA specifically, we argue that the mapping can be generalized to include most data related interactions. The generic role-based approach has the advantage over the actor-based approach in the sense that generalizability is maximized. Both individual data interactions as well as aggregated ones can be modeled using the framework.

Second, we mapped interests that feature during the DPIA. These interests constitute a new finding in the field of data protection. While literature is available that broadly contrasts human values with financial motives supporting the development of the SC (Herrschel, Dierwechter & Dierwechter, 2018; Grossi & Pianezzi, 2017), a more nuanced view was missing. Financial interests and social interests were brought up as well as more technical interests. The value of the results is in the variety of views consulted and the openness with which the subject was approached. We are confident that the scope of the results reaches beyond the mere DPIA process, arguably they are of importance in any data protection environment. This deeper and more granular understanding of interests is vital to move toward a less conflictual model in terms of SC development. The findings show that private data controllers are very concerned with the generation of trust when it comes to the DPIA. This is in stark contrast with the neoliberal dystopian SC that is too often sketched. The results provide insights into the potential tensions that would need to be managed to render SC development progress more durable.

Third, we bundled the findings concerning the stakeholder map and the interests into an AHP analysis. While explorative in nature, following the lack of knowledge available, the results clearly show that stakeholders are mainly concerned about trust generation when it comes to SC data protection. This corresponds to what other researchers have stressed recently (Khan et al., 2017; Braun et al., 2018), and it underlines the importance of reaching sustainability in an inclusive and human-centric fashion. Unsurprisingly, risk management and data security interests also feature prominently in the DPIA. Notably, financial and competition/ competitiveness considerations do not seem to substantially affect stakeholder interactions. However, we have found interesting differences between interest rankings of various stakeholder groups.

Fourth, we were able to distill a series of insights concerning the current DPIA practice. Notably, our findings show that there is a clear need for data controllers to get concrete guidance on how to involve citizens in the DPIA process. The salience of the generation of trust interest holds over all individual analyses. It is evident, and it was mentioned by interviewees, that citizen trust requires deep interaction with citizens, but extant literature as well as practice show that citizen involvement is currently still rare (Breuer & Pierson, 2021; Christofi et al., 2021). Furthermore, some of the popular

DPIA methodologies might not sufficiently tailor for this. Also, compliance as such does not feature prominently in the DPIA interest rankings. This can be considered surprising as the novel accountability and risk-based measures of the GDPR, among which the DPIA, are sometimes considered to have (boosting) compliance as their primary aim (Gellert, 2018). In contrast, the risk theme as a whole is deemed quite important throughout. It can be derived that DPIAs are performed with a holistic view on a range of risks rather than with a narrow checklist-based compliance view. Additionally, comparing DPIAs conducted by private data controllers and public data controllers showed that the underlying interest rankings are less different than could reasonably be expected from previous literature on the neoliberal SC. It might even be concluded that there is a business case for generating trust by performing a sound DPIA. Last, care should be taken when outsourcing (part of) the DPIA since the final product delivered by the consultant might not sufficiently reflect the interests of the data controller. Therefore, raising awareness and knowledge internally remains key.

6. Conclusion

Stakeholder interactions are central to the SC. This chapter focuses on one particular data protection interaction, namely the DPIA. We argue that five stakeholder groups come with a set of related interests, which constitutes the starting point of our investigation. Evidently, performing DPIAs is more problematic when stakeholder groups represent diverging goals or interests, ceteris paribus. Through an explorative case study of the Flemish SC, we answer two interlinked research questions. First, we investigate and present the various interests that feature when conducting a DPIA exercise. Second, we study the salience of these interests.

In a first step, we compound an extensive list of possible interests through a series of sixteen in-depth data protection expert interviews. We identify eleven separate interests that play a role in the DPIA: i) compliance, ii) cost control, iii) data management, iv) efficiency, v) generation of trust, vi) income acquisition, vii) limiting impact on service performance, viii) reputation building, ix) risk management, x) safeguarding competition, and xi) safeguarding data security. Subsequently, we classify them following four overarching themes: i) financials, ii) competition/ competitiveness, iii) social, and iv) risk. The wide variety of themes demonstrates the potential extent of the stakeholder interaction problem, also in terms of balancing interests, with regard to the DPIA.

In a second step, we perform an AHP analysis to rank the interests according to their importance. To that end, we circulate a survey to over 300 organizations active in the Flemish SC. The final response sample consists of eighteen organizations with at least one self-identifying as primarily belonging to each of the five stakeholder groups. When assuming equal power between all stakeholder groups, we find the risk theme to be the most prominent with exactly 50% of the total weight. The three most

salient individual interests are: generation of trust, safeguarding data security, and risk management. Notably, interests belonging to the financial and competition/ competitiveness themes are deemed of relatively little importance. Further remarkable finds are that private sector data controllers tend to be more concerned with trust generation than their public counterparts. In addition, specialized consultants and researchers consider the risk theme more weighty than data controllers. The relative unimportance of the financial and competition/ competitiveness themes holds throughout these analyses.

The results of our analysis are useful for SC stakeholders belonging to any of the five stakeholder groups. Data controllers, as the stakeholders responsible for carrying out the DPIA, can utilize the list of interests and their indicative salience as a starting point to think about potential DPIA problems, or data protection more broadly. This will render DPIA processes more efficient. Data processors can make use of these findings to organize their thoughts on the DPIA, as they tend to be a stakeholder group wary of participating in the process. The results hint at the potential benefits involvement can entail for them. The analysis gives specialized consultants and researchers a unique insight into the broader dynamics of the DPIA and the needs of their potential clientele. Citizens, or the organizations representing them, can instrumentalize these explorative finds to optimize their influence in the DPIA process. The findings provide a view on the natural compatibility of interests, and thus chances of success of potential stakeholder group coalitions. Data protection authorities can build on these results to develop in-depth guidelines with respect to the safeguarding of participation in the DPIA, as well as with respect to speaking to the interests of the regulated groups.

At the same time, the findings point to the importance of SC service development components like generation of trust and safeguarding data security over more traditional pure-play business interests. This arguably shows an evolution towards increased human-centricity, and underlines the value of such an evolution and the congruence thereof with long term business objectives. Tailoring to the citizens of the SC could render DPIAs more efficient and more effective, and in turn lead to long term sustainability of SC service development.

We note that this research is explorative. Due to the current scarcity of DPIA experts, any research endeavor will necessarily be explorative. However, the results will remain useful, be it as an indicative base line. Broader surveys could strengthen our findings, though (salience of) interests might for example depend on cross-national differences in stages of SC development.

Further, this chapter made abstraction of the various extant DPIA methodologies to focus on the underlying interests. However, it is possible that the reasoning of the interviewees as well as the AHP participants was colored by their experience with varying DPIA methodologies, i.e. experience with a

single methodology might lead one to reduce the DPIA concept to the result of this particular methodology. Nonetheless, our research tailors for that as findings are built upon grouped responses within as well as over different stakeholder groups. Extreme experiences likely at least partially cancel each other out.

As documented, the consensus weights of the interests were calculated as if all stakeholder groups had an equal say in the DPIA, i.e. the stakeholder groups were all attributed the same weight. While this arguably indicates an ideal type balanced situation, in reality the voice of some will likely be more influential than that of others. While this falls outside the scope of this chapter, more in-depth research in that direction is also needed through case studies. In that respect especially operationalization of power imbalances and the dynamic aspect of stakeholder interests might prove to be interesting.

Additional further avenues for future research are the calculation of cost differentials between DPIAs conducted focusing primarily on some of the various interests, the mapping of the variety of DPIAs in practice, and the integration of the stated interests of individual citizens in the framework.

Chapter 5. Beyond data controllership: Merits of a generic DPIA by hardware and technology suppliers[12,13]

Abstract

This chapter discusses the position of hardware and technology suppliers in the data protection impact assessment process. While various stakeholders should be involved, either as required by the General Data Protection Regulation or as suggested by guidance of the Article 29 Working Party, developers of hardware and technological solutions are seemingly overlooked. We argue that deeper engagement of this stakeholder group imposes itself. In addition to an analysis of the current situation, we present a recommendation based on the introduction of a basic generic DPIA to be performed by hardware and technology suppliers during the product development stage. The substantial benefits of such an approach are subsequently outlined.

[12] This chapter is published as an article in the European Data Protection Law Review, we thank two anonymous reviewers for their useful feedback on previous versions. Please cite as: "Vandercruysse, L., Buts, C., & Dooms, M. (2020). Practitioner's Corner · Beyond Data Controllership: Merits of a Generic DPIA by Hardware and Technology Suppliers. *European Data Protection Law Review*, *6*(1), 133–136."

[13] **Author contributions** - **Laurens Vandercruysse**: Conceptualization, Methodology, Formal Analysis, Investigation, Visualization, Writing - Original Draft; **Caroline Buts**: Validation, Writing - Review & Editing; **Michaël Dooms**: Supervision.

1. Introduction

The introduction of the General Data Protection Regulation (GDPR) marked a shift with regard to the treatment of data processing organisations, which are now more accountable for data processing operations (Lindqvist, 2018). In particular, the data protection impact assessment (DPIA) constitutes a considerable advance vis-à-vis the Data Protection Directive 95/46/EC (DPD) (Urquhart, Lodge & Crabtree, 2019). Section one of Article 35 of the GDPR states that a data controller aiming to institute a data processing that is "*likely to result in a high risk to the rights and freedoms of natural persons"* is to conduct an ex ante assessment of the ensuing data protection risks (Regulation (EU) 2016/679 (GDPR), 2016). The legislator thus opts to put the onus for risk assessment and risk mitigation firmly on the data controller. While this approach undoubtedly intends to force a mentality shift in data controllers, the main decision-maker in charge of deploying technological solutions, we argue that the legislator partly overlooks data protection problems that originate at the technological development stage. This chapter aims to demonstrate and highlight the merits of shifting the responsibility of the DPIA up the supply chain to include the level of the hardware and technology supplier. We argue that this approach entails considerable benefits, most notably from an economic and compliance monitoring perspective.

2. The missing link in the prevailing DPIA-practice

The DPIA as an accountability mechanism consists of five steps laid out in Sections seven and eleven of Article 35 (Regulation (EU) 2016/679 (GDPR), 2016), ie: i) an in-depth description of the foreseen processing operation including purposes and, when pertinent, the legitimate interests pursued, ii) a context specific evaluation of the necessity and proportionality of the processing operation, iii) an evaluation of the data protection risks springing from the processing operation, iv. a mitigation plan with regard to the identified risks, and v. a review of the DPIA-process when there is a change of the risk. Going through these steps should ideally entail a collaboration between several actors involved in the data processing. The Article 29 Working Party (A29WP) provides some guidance in WP 248 (Article 29 Working party, 2017). The suggested stakeholder list is displayed in Table 21. It is argued that the full processing picture can only be attained by taking into account the various perspectives of all stakeholders involved. The data controller, eventual processors, and the data protection officer (DPO) are key actors during this exercise (Article 29 Working party, 2017).

DPIA-stakeholders
Data controller(s)
Processors
Specialised consultants (internal, e.g. DPO and CISO, or external)
Data subjects
Data protection authority

Table 21. List of DPIA-stakeholders (Article 29 Working party, 2017).

The DPIA driving seat is occupied by the data controller, when applicable in combination with a joint controller. Processors act on behalf of the data controller to attain predefined processing goals with predefined processing means (Regulation (EU) 2016/679 (GDPR), 2016). In the context of the DPIA, processors provide the technical processing information required to fulfil the DPIA-requirement in full to the controller (Regulation (EU) 2016/679 (GDPR), 2016). The advice of the organisation's DPO, the principal internal data protection specialist, is to be carefully considered (Article 29 Working party, 2017; Regulation (EU) 2016/679 (GDPR), 2016). In case the data controller relies on data protection consultants for the DPIA-procedure, the latter constitute additional stakeholders. When the DPIA is entirely outsourced to a consultant, an explicit possibility under the WP 248 (Article 29 Working party, 2017), allows that the consultant acts as the main decision-maker. When appropriate, the data subjects are also to be consulted for the DPIA as part of the standard procedure (Regulation (EU) 2016/679 (GDPR), 2016). They may provide critical input in particular during the risk identification stage. However, the GDPR provides an exemption in cases where the controller can justify that citizens' participation is in contravention to business interests (Regulation (EU) 2016/679 (GDPR), 2016). When considerable data protection risks remain after risk mitigation, the DPA is to be consulted on the processing operation (Regulation (EU) 2016/679 (GDPR), 2016). Furthermore data controllers can opt to seek the views of the DPA on a voluntary basis as well.

We argue that there is an important stakeholder missing from the suggested list by the A29WP, namely the hardware and technology suppliers. Just as the data processor, these hold considerable technical information needed to diligently perform a DPIA. Furthermore, the WP 248 explicitly foresees in DPIAs being performed on technology products, in addition to (sets of similar) processing operations as required by Article 35 (Article 29 Working party, 2017). However, currently there is no straightforward way to enforce the DPIA-participation of hardware and technology suppliers, nor to induce these actors to go through the trouble of performing a basic DPIA at the product development stage. Nonetheless, there are considerable benefits from a stronger involvement of actors higher up the technological supply chain.

3. Benefits of increased DPIA-involvement of hardware and technology suppliers

On the one hand, in a DPIA-process led by a data controller, the actors that developed the hardware and technology to set up a data processing operation dispose of indispensable information regarding the conception and the technical specifications of the product. Much like the processor, their informational input is crucial to all the steps of the DPIA, in particular those concerning risk identification and mitigation. However, unlike the processor, whose responsibilities concerning the DPIA are lined out explicitly in Article 28 and who is referenced extensively throughout the GDPR and the recitals (Regulation (EU) 2016/679 (GDPR), 2016), references to the hardware and technology supplier are scarce and mostly indirect. It could be argued that the original hardware and technology supplier might consecutively enter into a service agreement with the data controller, becoming a data processor as well, and as such '*solve*' the enforceability problem concerning DPIA-involvement. However, this type of vertical integration is not always present or possible, nor should it be relied upon. An instructive example can be found in the market of smart cameras where hardware is sold separately from data processing solutions. It is exactly in this type of pure sales transactions that the need for information from the hardware and technology supplier is most pressing, as an additional actor is added to the processing chain. We believe there is a public interest in enticing hardware and technology suppliers to contribute to the DPIA, especially seeing the increasingly intricate nature of hardware and technology and the penetration rate of deployment of such products in the public space.

On the other hand, a basic DPIA by the hardware and technology supplier during the development stage of the hardware and technology with data processing capabilities could add substantial value. While the A29WP merely hints to the fact that *"a DPIA can also be useful for assessing the data protection impact of a technology product"* (Article 29 Working party, 2017), we would argue that in most cases such an exercise would definitely be useful. First, there is the economic efficiency argument. Rather than having data controllers (needlessly) duplicate risk assessment efforts, it is more sensible for the supplier to perform a basic assessment on its product and/ or a series of its predefined standard uses. At the same time, this would allow data controllers to zoom in on risks springing from the specific deployment of the hardware and technology. They arguably constitute the more *'hidden'* risks of which discovery brings the most value-added to the assessment. As data controllers' resources are finite, a template basic DPIA would spur the data controller to study more in-depth certain particularities while not glossing over more general (technical) risks. Also risks originating from the deployment of a technology in a community by a particular type of actor, i.e. public or private, should be covered more extensively in the DPIA performed by the data controller. The time- and cost-efficiencies resulting from the basic DPIA can be spent to that end. Second, the accountability principle of the GDPR is honoured more fully. The DPIA at the development stage would render developers

responsible for the product choices they make, while not relieving data controllers from their data protection responsibilities. The risk-based approach is moved up the technological supply chain, inducing hardware and technology suppliers to take data protection considerations into account. Third, a centralisation of the basic risk assessment at the level of the hardware and technology suppliers could stimulate uniformity in data protection risk identification. Rather than having hardware and technology customers generate distinct terminologies of data protection risks, the supplier has the opportunity to guide the customers. Reduced fragmentation of data protection risk classifications will stimulate the development of a common language. As a result it will also facilitate monitoring efforts by local DPAs. Lastly, a DPIA at the development stage can incentivise suppliers to embrace the privacy-by-design and privacy-by-default principles (Regulation (EU) 2016/679 (GDPR), 2016). The less data protection risks a product entails, the less expensive the basic DPIA-process becomes, ceteris paribus. Though recital 78 of the GDPR encourages these players to think about data protection in the design stage and while setting defaults, references in Article 25 solely cover the data controller (Regulation (EU) 2016/679 (GDPR), 2016). A widespread adoption of requirements concerning privacy-by-design and privacy-by-default by public authorities during procurement processes could change the incentive structure for suppliers (Regulation (EU) 2016/679 (GDPR), 2016). The suggested basic DPIA could provide an additional impetus.

Table 22 provides an overview of the proposed process and indicates how this differs from the current DPIA, as well as the resulting benefits.

4. Conclusion

While the privacy impact assessment (PIA) is well-known in most of the Anglo-Saxon world (Clarke, 2009), the DPIA constitutes a novel challenge for data processors active in the European Union. Particularly the compilation of an exhaustive overview of data protection risks originating from the deployment of a particular data processing activity and the development of a tailored risk mitigation plan demand detailed information from a variety of different actors. While the A29WP already includes an extensive list of stakeholders of the DPIA-process, we argue that the WP overlooked one vital actor, i.e. the hardware and technology supplier.

Both in the current DPIA-practice, as well as in an ideal case scenario we investigate, the involvement of the supplier of hardware and technology could be very beneficial. During a DPIA led by the data controller, the coverage of DPIA-obligations of the data processor should ideally be extended to the supplier of hardware and technology used for the data processing. At least suppliers should be incentivised to contribute to the DPIA. Without the technical specifications and related information that this supplier disposes of, any risk estimates and mitigation plans are incomplete at best.

Step	Actor in charge	Current DPIA-role	Recommended DPIA-role	Advantages of the recommended approach
Development of hardware and technology with data capabilities	Hardware and technology supplier	Provision of information or no involvement	Generic DPIA on basic use and ensuing data protection risks	• No duplication of risk assessment efforts • Responsibilisation of developers higher in the supply chain • Promotion of uniformity in data protection risk identification • Simplification of monitoring efforts of DPAs • Advancement of privacy-by-design and privacy-by-default

Development of specific use-case	Data controller	Full DPIA-process with help from specialised (research) consultants/ data processors/ citizens/ DPA	In-depth DPIA with actor specific, urban specific and service specific characteristics and risks, building on the generic DPIA	• Adoption of a generic basis while allowing for flexibility and specificity
				  • Inclusion of *'hidden'*, more value-added risks
				  • Evaluation of (the gravity of) specific risks dependent on the community role (public or private)
				• Better implementation of a risk-based approach

Table 22. Overview of the DPIA-recommendation. Source: own creation.

Furthermore, we suggest the adoption of a generic DPIA by the hardware and technology supplier at the stage of product development on a list of basic uses. This document could then be built upon by the data controller deploying the hardware and technology for a specific use-case. From an economic viewpoint, the avoidance of duplication of basic data protection risk identification efforts is a real asset. Moreover, this approach would allow a responsibilisation of the developer of hardware and technology, while safeguarding flexibility in assessing and addressing data protection risks in a particular situation. With the basic DPIA already performed, the data controller can focus on use-case specific risks. Centralisation of the basic DPIA-process disseminates a common risk classification, which in turn simplifies the monitoring task of the local DPAs. The introduction of a DPIA-obligation for the supplier could also constitute a substantial economic incentive for an accelerated adoption of the privacy-by-design and privacy-by-default principles.

In short, though the A29WP planted the seed for a hardware and technology focused DPIA in the WP 248, we recommend more stringent steps to increase the accountability of the hardware and technology suppliers of data processing operations.

Chapter 6. Public procurement as a safeguard for competition: The case of smart city services[14,15]

Abstract

Through the adoption of the European Union's Digital Strategy, the European Commission aims to tackle pressing issues specific to markets of data-intensive services. One of these issues is the substantial and durable competitive advantage that emerges from having exclusive access to large sets of data. The Digital Markets Act proposal, a prime pillar of the Digital Strategy, allows for the identification of gatekeepers. These gatekeepers would then be subject to additional obligations, for example enabling wider data access. This chapter focuses on the market for smart city services and proposes the adoption of a more proactive approach through public procurement. We argue the onus should be on preventing service providers from becoming gatekeepers, rather than attempting to repair a competitive space once a gatekeeper has arisen.

[14] This chapter is published as an article in the European Competition and Regulatory Law Review, we thank two anonymous reviewers for their useful feedback on previous versions. Please cite as: "Vandercruysse, L., Buts, C., & Dooms, M. (2021). Public Procurement as a Safeguard for Competition: The Case of Smart City Services. *European Competition and Regulatory Law Review*, *5*(2), 102–111."

[15] **Author contributions** - **Laurens Vandercruysse**: Conceptualization, Methodology, Formal Analysis, Investigation, Visualization, Writing - Original Draft; **Caroline Buts**: Conceptualization, Writing - Review & Editing, Supervision; **Michaël Dooms**: Conceptualization, Supervision.

1. Introduction

Healthy competition is a driver for economic growth and consumer welfare (Brodley, 1987). The advent of digital markets and widespread 'datafication' has put pressure on legislators and regulators to look beyond their current legislative and regulatory toolboxes. There is a growing understanding that a lot of the more traditional regulatory instruments were not designed to cope with the very specific issues that data-intensive markets bring (Capobianco & Nyeso, 2018).

The European Union's (EU) Digital Strategy is considered the Commission's answer to the ever-growing powers of big tech (European Commission, 2020f). Particular points of interest of the strategy include addressing undue market power and stimulating free and fair competition (European Commission, 2020f). The trifecta of the Digital Services Act (DSA), the Digital Markets Act (DMA), and the Data Governance Act (DGA) is supposed to help tackle for example social media platform accountability issues, abuses of privileged gatekeeper positions, and exclusive data hoarding (European Commission, 2020b; European Commission, 2020c; European Commission, 2020d).

While these legislative initiatives are valuable, we argue they lack the proactiveness that is vital for the initiatives to be 'future-proof'. In addition, entry into applicability of these acts is likely too late to avoid winner-take-all issues emerging in new technological markets.

The market for smart city services is a typical example. Suited to this specific market, this chapter proposes a more proactive intervention, consisting of embedding tailored data protection and data sharing clauses in public procurement processes. The practical proposal builds on empirical data gathered through 19 interviews with Belgian and Dutch experts working in the domain of data protection and public procurement.

This chapter consists of five sections. Section two grounds the proposal by providing the necessary context on the status of competition in digital market spaces. Section three addresses the qualitative methodology. Section four presents our proposed public procurement intervention based on the interview results. Section five concludes.

2. Competition in digital markets

Safeguarding competition in online markets is a salient topic among policy-makers across the EU. The European Commission's DMA proposal, a cornerstone of the EU's Digital Strategy, is a testament to the pertinence, persistence and prevalence of residual competition issues escaping the scope of the current competition policy framework. Furthermore, there are currently several national legislative processes underway that aim to address many of the same concerns (Kayali & Scott, 2021).

Underlying these initiatives is a shared understanding that digital markets, and digital platform markets in particular, demand a fundamentally different approach than most traditional business sectors (Capobianco & Nyeso, 2018; Cennamo, 2019). The concerned markets are subject to conditions that are not found, or at least not ordinarily (combined) to the same extent, in offline environments. These markets are often characterized by market structure inclinations leading to natural monopolies (Clemons & Madhani, 2010; Loertscher & Marx, 2020). This means that due to the set-up of the service provision, market forces are as such that they would lead to a market with a single dominant provider. More concretely, the existence of considerable economies of scale and economies of scope in a context where users are confronted with substantial switching costs, as well as subjected to direct and indirect positive network effects, produce winner-take-all situations in the case of digital service markets (Buiten, 2019; Engels, 2016; Evans & Schmalensee, 2012).

There is a consensus that the common root factor of the mentioned adverse market forces is exclusive access to data (Engels, 2016; Graef, 2015).

While economies of scale are also related to installed server capacity and resource sharing, exclusive access to data offers scale advantages as well (Carlsson, 2004; Nuccio & Guerzoni, 2019). Let us assume that setting up an online platform service costs a certain amount of investment (sunk cost), while adding a single user to the platform would not increase costs but would increase revenue potential (Evans & Schmalensee, 2012). Large fixed costs coupled with next to no marginal costs and positive marginal revenues lead to scale advantages.

Moreover, economies of scope can be directly traced back to exclusive access to data. Data that was collected in a certain context, for example social networking, can be used to offer superiorly personalized services in another market, for example the market for payment services. The exclusive access to data on online social interactions as well as interests provides the data controller a competitive advantage in terms of tailoring and personalization in a plethora of related and seemingly unrelated markets (Gal & Petit, 2020).

In the same vein, switching costs are to a large extent a product of exclusive access to data by a data controller. For example, switching costs in online platform markets mostly emerge from the switching user having to become familiar with the set-up and functionality of the new platform as well as having to create a new platform profile (Tucker, 2019; Hsieh, Hsieh & Feng, 2011). It is evident that these switching costs could be lowered considerably if platforms would adopt an interoperability mindset and fully endorse data portability (Budzinski, 2008). While Article 20 of the General Data Protection Regulation (GDPR) explicitly creates a right to data portability and recital 68 clarifies an interoperable format should be utilized, it still allows incumbent data controllers considerable freedom in how to

implement the exercise of that right (Regulation (EU) 2016/679 (GDPR), 2016). It is clear that incentives run contrary to offering the most efficient solution.

Last, network effects relate to exclusive data access too (Nuccio & Guerzoni, 2019). Consider a search engine: the more exclusive search data the search engine disposes of, the more performant the search engine will become relative to competitors (Stucke & Ezrachi, 2016). In turn, the search engine will attract more users because it is the most performant service, leading to even more exclusive access to data and rendering the service even more performant. The indirect network effect follows the same dynamic. The more exclusive data access the search engine has, and the more traffic it consequently generates, the higher the value of the search engine website as a venue for advertising and the more advertisers will thus be willing to spend (Stucke & Ezrachi, 2016).

It can thus be comfortably concluded that exclusive data access generates market power. Possessing market power means having the possibility of implementing price increases and/ or quality reductions without being disciplined by the market (Landes & Posner, 1981). While this is obviously problematic from the viewpoint of consumer welfare, an equally important problem concerns data protection. While the level of data protection offered by a service provider is gaining importance as a quality feature, indicating growing consumer interest, the market power of the large tech companies mostly shatters any incentives for them to offer better data protection (Bonneau & Preibusch, 2010; Buiten, 2019). It should be noted that data protection is not just a service quality feature but also, and primarily, a fundamental right recorded in the EU Charter of Fundamental Rights (Charter of Fundamental Rights of the European Union, 2012). Nonetheless, recent history shows a bleak picture when it comes to big tech's data protection compliance track record (Data Protection Commission, 2020; Belgian Data Protection Authority, 2020; French Data Protection Authority, 2020).

Following this diagnosis, an intervention imposes itself. This is where the EU's Digital Strategy comes in, particularly the recent DMA proposal. A core concept in the DMA proposal is that of "*gatekeeper*," i.e. an undertaking which acts as an intermediary between different actors and which derives considerable durable market power therefrom (European Commission, 2020b). Notwithstanding the final operationalization is lacking at the time of writing, it is evident that most large platforms would likely fulfill the eventual requirements and thus be subject to the related obligations (European Commission, 2020b).

Even though the proposal contains clauses concerning enhanced interoperability, improved data access and prohibited data usage for gatekeepers (European Commission, 2020b), it fails to get to the heart of some of the underlying issues. We argue that this is related to a scoping issue. Rather than only targeting undertakings that have become gatekeepers, it would be more useful to also prevent

strong gatekeeper positions to arise. Exclusive access to data is both a conditio sine qua non for obtaining a gatekeeper position, as well as a product of holding a gatekeeper position. Therefore, a preemptive intervention, i.e. before a gatekeeper position is obtained and the undertaking thus falls within the scope of the proposed DMA, could prove to be more efficient.

The smart city services market would particularly benefit from this insight as it is still emerging and true gatekeepers are not yet present (Grand View Research, 2020). Arguably, the potential detrimental effects of having gatekeeper positions in a smart city are even more elevated than having them in the online-only world as there is no 'off-button' for the real world nor is there an option for users to delete their individual profile. To effectively avoid the dystopia where a limited set of private companies scrapes and stockpiles all data created in the public sphere to generate excessive profits with an absolute disregard for data protection, a more data-focused approach imposes itself. A second pillar of the Digital Strategy of the EU, the DGA proposal, offers pertinent building blocks (European Commission, 2020c). The possibility for European data spaces where sectoral data can be widely accessed and shared, and the prohibition of exclusive arrangements concerning data use in Article 4 are valuable interventions (European Commission, 2020c). However, they belong to the realm of the reactive regulatory paradigm, i.e. to be able to pool data and to make arrangements about data usage, data first has to be created and collected. The relative lack of enforcement in the wake of the entry into applicability of the GDPR further underscores the need for more proactive regulatory instruments (Satariano, 2020; Stolton, 2020).

This chapter proposes a two-pronged intervention at the stage of smart city service public procurement which will, together with the DGA proposal, likely keep the smart city realm free of gatekeepers as they are known today and consequently safeguard or upgrade offered data protection levels.

The public procurement process uniquely lends itself to instrumentalization for competition and data protection conservation for three distinct reasons.

First, the large majority of smart city services will have to go through a public procurement process. Seeing that these services are to be implemented in the public space, the public authority will be a notable stakeholder, and in many cases a driving-force (Finch & Tene, 2018; Lopes, 2017). Roll-outs are expected to largely exceed current thresholds for direct contracting, and thus will be subject to public procurement regulation (Edwards, 2016; Organisation for Economic Co-operation and Development, 2010). In conclusion, a public procurement intervention would have a good coverage of smart city services, and at a time when data collection is yet to be commenced.

Second, public procurement constitutes a large part of total demand in most regions (Georghiou et al., 2014). Cities have the potential to be market makers rather than market takers because of their significant combined purchasing power (Finch & Tene, 2018), especially when cities group in regional or national umbrella organizations. Purchasing power is an instrument that can turn larger counterparties more sensitive to any extra requirements embedded in the public procurement process.

Last, there are several precedents. Embedding environmental, social and labor law requirements in public procurement documents has become common (McCrudden, 2004). This stems from a wider trend of utilizing these procedures to serve broader policy goals (Stentoft Arlbjørn & Vagn Freytag, 2012; Telgen, Harland & Knight, 2007). Much like environmental, social and labor law, data protection law is horizontal legislation and thus could likely lend itself to, and benefit from, a similar crosscutting approach.

3. Methodology

The practical recommendations set out in Section four are based on insights from 19 semi-structured expert interviews conducted between May and October 2020 (Galletta, 2013). We diligently followed expert interview methodologies, ensuring balanced results and avoiding common pitfalls (Bogner, Littig & Menz, 2009).

Interviews tackled experiences with the roll-out of smart city services in general, and related data protection practices and public procurement processes. Though the consensus on what constitutes a smart city service is constantly evolving, its definition commonly includes: the achievement of a societal purpose, the presence of virtual-to-physical links, and the processing of large datasets (Vandercruysse, Buts & Dooms, 2020). Interviews focused on services containing all three elements.

Interview subjects were data protection and public procurement specialists working in the public and private sector in Belgium or the Netherlands. Both public and private sector experts were included to come to a balanced and realistic proposal. The total sample consisted of: seven experts at city administrations (City 1-7), three experts at city umbrella organizations (City organization 1-3), one expert at a government agency (Government agency 1), seven experts at private smart city service providers (Company 1-7), and one expert at a university (University 1).

Though the scope of our research is in a first instance limited to Belgium and the Netherlands, the inherent international dimension of the smart city sector and the diversity of experts we interviewed, strengthen our belief that these results could also offer insights relevant to other geographies. Furthermore, as our expert sample includes both frontrunners in smart city services as well as late adopters, these results can be expected to hold widely.

4. Results

4.1. Current situation

A short series of explorative questions at the start of the interviews strongly confirmed the relevance of the points addressed in Section two.

First, 16 out of 19 interviewees indicate that at least some smart city service markets are already to some extent concentrated (Data protection and public procurement specialists, personal communication, 29/05/2020 – 16/10/2020). While the market for innovative mobility scanners for example is well-endowed with small and medium-sized enterprises (SMEs), markets for solutions with large infrastructure components and those for digital enforcement solutions are quite concentrated (City 2, personal communication, 4/06/2020; University 1, personal communication, 16/10/2020). Competition should thus be safeguarded/ upgraded rather sooner than later.

Second, 18 out of 19 interviewees indicate that they often show flexibility in terms of drafting the data processing agreement for smart city services (Data protection and public procurement specialists, personal communication, 29/05/2020 – 16/10/2020). Additionally, only 5 out of 19 interviewees indicate that the public partner acts as the sole controller, so the sole decision-maker, for the data gathered in the context of the smart city service (Data protection and public procurement specialists, personal communication, 29/05/2020 – 16/10/2020). These combined insights show that private actors play an important role in determining data processing conditions as well as in the distribution of data control. It is exactly this power and the consequent privileged data access that eventually lead to the creation of gatekeeper positions.

Third, 17 out of 19 interviewees indicate that setting up a smart city service entails some form of collaboration between public and private actors (Data protection and public procurement specialists, personal communication, 29/05/2020 – 16/10/2020). While pilot projects escape formal public procurement for the time being, final roll-outs do not (City 4, personal communication, 10/06/2020; Company 5, personal communication, 13/07/2020). This underlines the strength of an intervention at this stage in smart city development.

4.2. Public procurement intervention

To tackle the issues that are currently arising, we propose an intervention as displayed in Figure 6.

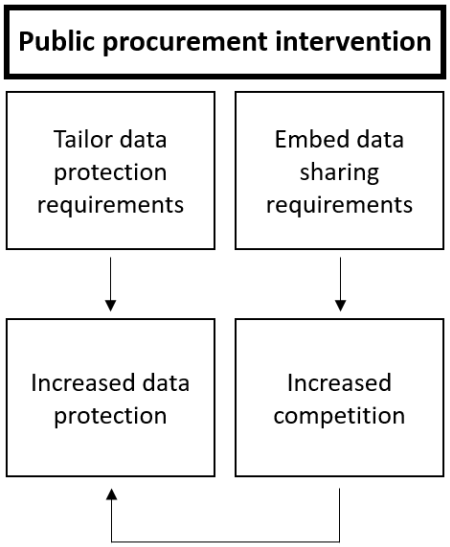

Figure 6. Visual summary overview of the public procurement intervention. Source: own creation.

First, data protection requirements tailored to smart city services should be embedded in the public procurement process. This will lead to a direct upgrading of the level of data protection, and will prevent undue data control and secondary data usage. This will impede the achievement of gatekeeper status for private service providers. Second, data sharing clauses should be formally integrated in the public procurement documents as a standard practice. The obligation of data sharing will lead to pro-competitive effects further lowering market power of private actors. This will likely induce an increase of the level of data protection through the development of more data protection friendly alternatives or the creation of new markets.

4.2.1.Data protection clauses

4.2.1.1. Problem statement

Including data protection requirements in tendering processes is already becoming more common (City 3, personal communication, 8/06/2020; City 4, personal communication, 10/06/2020; City 6, personal communication, 21/08/2020; Company 1, personal communication, 19/06/2020; University 1, personal communication, 16/10/2020). Nevertheless, a recurring remark both from private sector bidders and public sector data protection specialists is that these clauses are not sufficiently tailored (City 5, personal communication, 3/07/2020; City 7, personal communication, 5/06/2020; Company 5, personal communication, 13/07/2020). Mostly the integration of data protection is limited to a few default paragraphs setting out general legal obligations under the GDPR, and a standard data processing agreement (City 3, personal communication, 8/06/2020; City organization 2, personal

communication, 13/07/2020; City organization 3, personal communication, 10/07/2020; Company 3, personal communication, 2/07/2020; Company 4, personal communication, 8/07/2020). While reminding service providers of their responsibilities under the GDPR in the context of the submission of their bid can be somewhat useful as an awareness-raising tool, it is clear that the mere repetition of GDPR articles might not induce service providers to evaluate and tweak their product to the tender. Additionally, the use of a standard data processing agreement is no doubt preferred to not having a data processing agreement at all, but overlooks the particularities of the individual service (City 7, personal communication, 5/06/2020; Company 4, personal communication, 8/07/2020; Company 5, personal communication, 13/07/2020). Necessarily mismatches (Company 7, personal communication, 28/07/2020), unclarities (City organization 3, personal communication, 10/07/2020), and data responsibility gaps will remain (City 5, personal communication, 3/07/2020). The signature of the data processing agreement has become a 'tick-the-box exercise' with no real discussion on data storage, data usage, and data controllership taking place until problems arise (Company 3, personal communication, 2/07/2020; Company 4, personal communication, 8/07/2020; University 1, personal communication, 16/10/2020).

4.2.1.2. Towards service-specific data protection demands and smart city processing agreements

Building on the experiences of the interviewed experts, we propose a two-tiered approach combining the inclusion of service-specific, plain language data protection demands, as well as of a specific data processing agreement template for smart city services.

The development of service-specific data protection requirements demands an in-depth analysis of the desired service and its functionalities (City 6, personal communication, 21/08/2020; City 7, personal communication, 5/06/2020; Government agency 1, personal communication, 7/07/2020). Though not as rigorous as an actual data protection impact assessment (DPIA), this approach will result in a preliminary assessment of data protection implications. Tendering public administrations should be wary of purely copying articles of the GDPR into their tender documents. Not only is this legally problematic, experiences show that administrations lack the resources to effectively monitor compliance (City 5, personal communication, 3/07/2020; Government agency 1, personal communication, 7/07/2020). We therefore recommend starting from the functionality needed for completion of the policy goal and strictly abiding by the data minimization principle, i.e. define the data that is absolutely necessary, in concertation with the process owner and the data protection officer (DPO). Further, include the exhaustive list of desired data streams into the body of the tender and clarify that processing of any other data is prohibited.

Further, service providers should submit a data protection report along with the bid. The report should contain at least an analysis of privacy-by-design and privacy-by-default features of the proposed solution and a visual overview of the proposed internal data governance structure (City 2, personal communication, 4/06/2020; City 7, personal communication, 5/06/2020). The report ensures that the private partner has performed a data protection analysis of the service, which makes the private partner aware of certain insecurities. This set-up at the same time minimizes the effort required from the administration.

The conclusion of data processing agreements is a second recurring difficulty in the market for smart city services (City 3, personal communication, 8/06/2020; City 7, personal communication, 5/06/2020; City organization 1, personal communication, 29/05/2020). City umbrella organizations, like the Association of Flemish Cities and Municipalities and the Association of Dutch Municipalities, have developed data processing agreement templates, but such a template is often identical for catering services and for high-tech big data solutions (Company 4, personal communication, 8/07/2020). It is evident that these services demand different approaches, which also follows from the risk-based approach required by the GDPR. We argue that data processing agreements for smart city services should have certain uniform clauses to avoid the problems currently faced by public administrations. These stricter clauses should not necessarily be applied in cases where data processing is not related to smart cities. The concerned clauses relate to data controllership, and data breach reporting (City 1, personal communication, 26/05/2020; City 2, personal communication, 4/06/2020; City 4, personal communication, 10/06/2020). First, the public administration should always be the data controller. Due to the public nature of the services, it is important data controllership is not held solely by a private company (City 2, personal communication, 4/06/2020; City 4, personal communication, 10/06/2020; City 7, personal communication, 5/06/2020). This ensures that data access and data management follows the requirements of the public administration (City 4, personal communication, 10/06/2020; City 6, personal communication, 21/08/2020). This also safeguards options for data sharing. Second, a data breach should be reported timely to the public administration under penalty of heavy fines included in the processing agreement (City 1, personal communication, 26/05/2020; Company 1, personal communication, 19/06/2020). We recommend against including fines for data breaches per se, but solely on the non-reporting of data breaches. The concept ‘data breach’ should be interpreted in its broadest sense.

4.2.2.Data sharing clauses

4.2.2.1. Problem statement

Private service providers try to frame the GDPR as an obstacle preventing data sharing alluding to data security and data protection (Company 1, personal communication, 19/06/2020; Company 2, personal communication, 29/06/2020; Company 6, personal communication, 14/07/2020; Company 7, personal communication, 28/072020). However, case law on 'essential facilities' under Article 102 TFEU clarifies that the GDPR does not preclude open data per se and that not sharing data in itself might even constitute a breach of competition law (Kerber, 2019; Tombal, 2020). Nonetheless, in an attempt to avoid missing out on flashy novel smart city services, public administrations have adopted a hands-off approach. So while it is well established that data sharing can have significant pro-competitive effects, public administrations do not currently seem to have any stringent data sharing requirements embedded in their tender documents (City 1, personal communication, 26/05/2020; City 2, personal communication, 4/06/2020; City 4, personal communication, 10/06/2020; City 5, personal communication, 3/07/2020).

4.2.2.2. Towards embedded data sharing clauses and sound data governance

Data sharing clauses should be central to the tender and defined as a conditio sine qua non for bids. Full open data is preferred as it ensures flexibility and the highest benefits (City organization 1, personal communication, 29/05/2020; City organization 3, personal communication, 10/07/2020). Open data safeguards innovation through unforeseen uses and is of considerable importance for start-ups and SMEs (European Commission, 2018a; Narayanan, Huey & Felten, 2016). However, partial data sharing requirements already constitute an advance in comparison to the current situation. This can take the form of making data open to a series of trusted third parties, e.g. universities, or a group of preselected potential private partners in the run-up to a public procurement process.

For now, the seeming lack of legal basis hampers data sharing. From this angle, we look with great expectation to a series of recent legislative initiatives. First, the forthcoming entry into applicability of the directive on open data and the re-use of public sector information (European Commission, 2018a). While this directive does not cover personal data, aggregate and anonymized data are squarely addressed. Second, the DGA proposal, which explicitly mentions that data covered by data protection regulation is part of the scope for opening up. Lower tier governments are free to take initiatives of their own volition building on this dynamic of EU actions. In addition, as safeguarding competition is arguably a key public interest, the current legal framework might already offer sufficient scope for intervention.

Another recommendation concerns the choice of an appropriate data governance framework. Sound data governance is a cornerstone of solid data protection. To allow for systematic data sharing, a general overhaul of the data governance structure might impose itself (European Commission, 2018a). For example, care should be given when determining the legal basis for data sharing and the infrastructure should be well adapted (City 5, personal communication, 3/07/2020), e.g. if the legal basis is consent, a more intertwined and automated network of systems might be needed to fulfill an access request or a consent withdrawal (Company 5, personal communication, 13/07/2020; Tombal, 2020). Data sharing should also happen timely, as most data loses value over time (Buiten, 2019). Sufficient server capacity should be foreseen for all interested parties to access the data at any given time while safeguarding the continuity of the original service (Gleeson & Walden, 2016). Evidently, data sharing protocols should be checked against other relevant sector-specific regulation (Kerber, 2019).

To underline the importance of embedded data sharing clauses, we shortly list the main benefits applied to a smart city setting. Benefits of data sharing are three-fold: it counteracts lock-in of citizens, it counteracts vendor lock-in dynamics, and it generally mitigates the supplier power of the private partner.

First, data sharing facilitates the user's exercise of the right to data portability under the GDPR (Ni Loideain, 2019). Secure but wide data sharing undermines the power of the incumbent service provider. By consequence, the negotiation position of the individual user compared to the service provider strengthens, enticing private companies to innovate in line with users' demands. Data can be portable to direct competitors and to companies offering complementary services (Colangelo & Maggiolino, 2017). Facilitating such transfers will render both market spaces more competitive (Company 6, personal communication, 14/07/2020). To comply with the data sharing clauses embedded in the tender, service providers will benefit from picking a widely used data standard and from making their systems as interoperable as possible (Company 1, personal communication, 19/06/2020; Company 6, personal communication, 14/07/2020). Both evolutions could foster growth in the market of smart city service providers. Multi-homing, i.e. users using similar services of multiple providers at the same time, has been established as decreasing lock-in (Evans & Schmalensee, 2012). Data sharing can certainly help in that respect.

Second, data sharing eases vendor lock-in dynamics (City 3, personal communication, 8/06/2020; Company 6, personal communication, 14/07/2020). Similar to the right of data portability at the level of the individual user, any form of opening data to a wider circle of actors makes the procuring entity less dependent on its incumbent supplier. Furthermore, the usage of common data standards and

increased interoperability of systems lowers switching costs for the public administration (Company 6, personal communication, 14/07/2020).

Third, data sharing reduces the general market power that service providers derive from their incumbent position (City organization 3, personal communication, 10/07/2020; Government agency 1, personal communication, 7/07/2020). In contrast to vendor lock-in, this market power can be conceived more broadly. Exclusive data access brings power in several affected markets (City organization 1, personal communication, 29/05/2020; Company 2, personal communication, 29/06/2020; Kerber, 2019). Data from security cameras can be used for public security, but also for applications such as crowd control, counting of visitors, and environmental management. An incumbent can instrumentalize data insights to better tailor services in other domains. Data sharing levels the playing field and reduces the business value of data in the context of a contract.

5. Conclusion

While curtailing the power of big tech eventually made its way to the top of the political agenda, gaining progressive insights has been costly both in financial terms as in terms of fundamental rights protection. The legislative catch-up has been slow and actions were only taken after the damage had been done. In contrast, this chapter recommends adopting a more proactive approach to avoid the same mistakes during the "*smart city transformation*."

Based on 19 expert interviews, we propose a two-pronged intervention in the public procurement process to boost competition and data protection levels. Figure 9 displays this intervention visually.

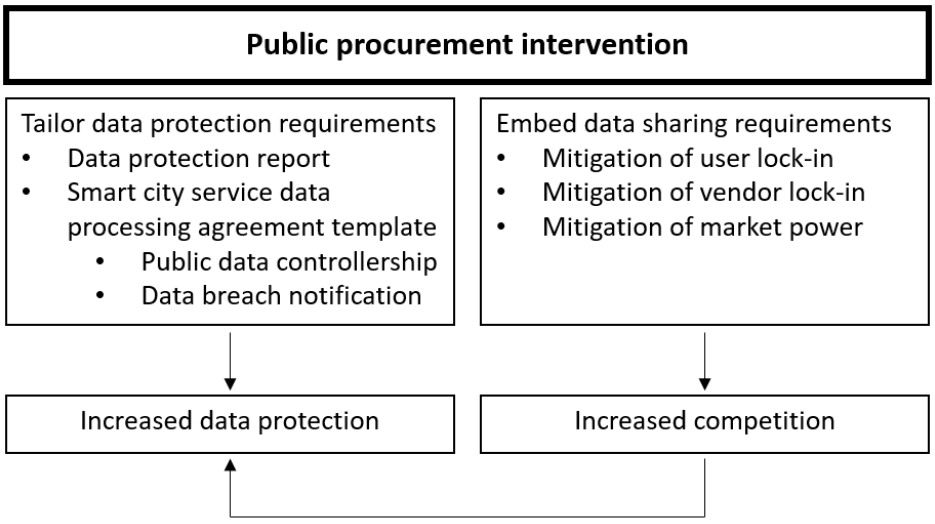

Figure 4. Visual conclusion of the public procurement intervention. Source: own creation.

The intervention entails embedding tailored data protection clauses as well as data sharing requirements in the tenders of public administrations.

First, bids should include the submission of a data protection report, answering demands derived from an in-depth functional analysis of the desired service, and the signing of a data processing agreement template specifically for smart city services outlining public data controllership and stringent data breach notification obligations. Current data protection clauses as part of the public procurement process are too general and overlook important key characteristics of smart city services. This tailoring would lead to a direct improvement of the level of data protection.

Second, data sharing requirements should be embedded in tenders. This boosts competition, which would lead to lower prices and higher quality of smart city services, e.g. better data protection. Data sharing alleviates lock-in risks at different levels and diminishes market power of service providers preventing the development of gatekeeper positions.

Further research should look into the influence of the suggested intervention on public procurement transaction costs and the balancing of the expected cost increase with the pro-competitive effect of data sharing.

Chapter 7. Public procurement of smart city services: An exploration of data protection related ex-ante transaction costs[16,17]

Abstract

This chapter examines data protection related ex-ante transaction costs borne by the private sector in the context of smart city service (SCS) public tendering in the European Union (EU) after the introduction of the General Data Protection Regulation (GDPR). The aims are to explore the determinants of ex-ante transaction costs related to data protection as well as to grasp their relevance towards (tender) competition. Based on an econometric analysis of a survey sample of 72 individual SCS tender bids, several insights emerge.

First, the potential of relationship management to foster more private sector investment in data protection for SCSs is established, i.e. stronger ties between parties lead to higher private sector investment.

Second, it is found that investing more in data protection can further boost both internal capabilities and organizational reputation of tendering organizations. This finding provides empirical backing for an often-propagated selling point for 'doing data protection right,' namely to increase the scope for spill-over benefits.

Third, our results show a positive correlation between SCS complexity and data protection related ex-ante transaction costs. This is an indication that the risk-based approach promoted by the GDPR is applied in practice.

Finally, the analysis exposes a potential problem concerning the market for data protection originating from the dominant approach concerning SCS tender bid evaluation. This evaluation is not perceived by the evaluated companies as having data protection as a core component. By consequence, there is no strong competition in that specific area. To induce the private sector to structurally develop SCSs that can be expected to safeguard fundamental rights of citizens, a more thorough evaluation of data protection aspects of bids imposes itself. Such an overhaul is likely to demand additional public sector resources and expertise, but this investment is potentially a necessary condition to be able to rely on sound market competition to (continue to) produce data protection friendly SCSs.

[16] This chapter is currently under review as an article. Please cite as: Vandercruysse, L., Dooms, M., & Buts, C. (2022). *Public procurement of smart city services: An exploration of data protection related ex-ante transaction costs* [Unpublished manuscript]. Department of Business, Vrije Universiteit Brussel.

[17] **Author contributions** - **Laurens Vandercruysse**: Conceptualization, Methodology, Formal Analysis, Investigation, Visualization, Writing - Original Draft; **Michaël Dooms**: Conceptualization, Methodology, Writing - Review & Editing; **Caroline Buts**: Conceptualization, Supervision.

1. Introduction

The General Data Protection Regulation (GDPR) aims to safeguard the fundamental right to data protection for the more than five hundred million people residing in the European Union (EU). The regulation is built on two prime pillars: on the one hand, increasing accountability and transparency of data controllers, and, on the other hand, empowering data subjects (Regulation (EU) 2016/679 (GDPR), 2016; Veale et al., 2018). The practical elaboration of the pursuit of increased accountability and transparency leads to the introduction of a series of new obligations; these include commanding comprehensive privacy-by-design and privacy-by-default practices, and requiring a data protection impact assessment (DPIA) when the data processing operation is considered 'high risk' (Laurer & Seidl, 2021).

Ensuring such compliance can be costly, especially for small and medium-sized enterprises (SMEs) (Christensen et al., 2013; Härting et al., 2020). In the five years following its introduction, interest into the potential collateral damage the GDPR caused to competition has begun to rise. Recent research has conjectured that the relation between data protection and competition can be considered a tradeoff to some extent (Gal & Aviv, 2020), European Commission proposals like the Data Governance Act and the Digital Markets Act also point in that direction (European Commission, 2020b; European Commission, 2020c). Even though this tradeoff reasoning is gaining traction among both the research and policy-maker community, empirical research on the presence, and the size, of the competitive hurdle that the GDPR introduced is rare.

Smart city services' development offers an opportunity to assess this hurdle.

The evolution in EU data protection law largely took place concurrently with the advent of smart municipal service provision. Smart city services (SCSs) range from intelligent street lighting to sensor-based garbage collection schemes. The variety of SCSs aims to tackle issues along almost the entire spectrum of public authority competences by making use of technology (van Zoonen, 2016). While SCSs can differ widely, a common feature concerns the collection and processing of personal data, which renders the services subject to the GDPR (Edwards, 2016; Vandercruysse et al., 2020). Furthermore, considering the guidance by the Article 29 Working Party on 'high risk,' it can be argued that SCSs have the potential to be important data protection enforcement targets (Article 29 Working Party, 2017). This higher likelihood of enforcement action by authorities can arguably push private service providers to more diligently comply with GDPR obligations, ceteris paribus.

Furthermore, as public authorities are forced to purchase most products and services through formal public procurement procedures, competition between private providers takes place in a relatively closed environment and following a well-documented step-wise process (Directive 2014/24/EU, 2014;

Onur & Tas, 2019). The administrative and procedural specificities of participating in a tender also prompt the private tenderers to follow a strict methodology and process for bid submission preparation and often thus comparatively better monitor the associated tendering costs.

For these reasons, bids for SCS tenders offer great potential to provide insight into the data protection cost structure of private providers following GDPR introduction.

Following the methodology of De Schepper, Haezendonck, and Dooms (2015), applied in the context of public-private partnership project tendering, this chapter focuses specifically on an exploration of the data protection related ex-ante transaction costs borne by private sector actors. More specifically, the research considers the size of the data protection related transaction specific investment as well as on the determinants and pay-off of this investment. Primary data is gathered through a survey with individual SCS tender bids as the unit of analysis, and a total set of 72 observations is collected. Even though this sample is limited, it suffices for a first exploration of this cost type. It is important to note that, to the best of our knowledge, this research is the first to focus on data protection related ex-ante transaction costs in any tender process.

In addition to practical and actionable insights with respect to data protection investment for the private sector, this research derives specific recommendations for the public sector to enhance SCS data protection levels. Also, from a wider frame, our findings can be used to support public policy improvements concerning data protection and competition with empirical evidence.

The chapter is structured as follows: Section two offers the fundamentals, Section three highlights the model and the research questions, Section four explicates the quantitative methodology, Section five presents the results, Section six discusses their implications, and Section VII concludes.

2. Fundamentals

2.1. SCSs, public procurement and the GDPR

Increasing budgetary pressure combined with falling hardware and software costs force public authorities to look for technological aids to permit them to ‘do more with less’ (Edwards, 2016). The central idea is that the use of technology allows authorities to perform their traditional tasks more efficiently and/ or effectively as well as to venture into new avenues of public service provision.

The trend toward an increasing digitization of public administration is also apparent at the local level (Fontana, 2014), and the ubiquity of the often elusive ‘smart city’ concept can be considered an important driver in that regard. While the abundance of definitions for ‘smart city’ demonstrates the lack of consensus concerning its conceptualization (Dameri, 2017), it is generally accepted that smart cities are characterized by a technology pervasiveness which largely transcends current levels (Camero

& Alba, 2019; Lee et al., 2013). It is therefore instructive to think of smart cities as being made up of building blocks, with the individual SCSs as the main building blocks.

Extant literature shows that an SCS can be defined based on the presence of a series of characteristics, notably: i) the service aids in serving a public interest, ii) the service processes personal data, and iii) the service entails (processing of data collected by) sensors or other hardware components (Vandercruysse et al., 2020 based on Neirotti et al. (2014) and Walravens & Ballon (2013)). From this characteristics-based definition follows the necessity to analyze the concepts of public procurement and the GDPR.

First, the definition indicates that an SCS is to serve the public interest. Since serving the public interest is the core task of local authorities, it can be discerned that these authorities would likely be a driving force behind the adoption of various SCSs. Research has shown that local authorities in most cases lack the in-house expertise to develop SCSs (Smart City Institute, 2018), thus adoption would largely entail procurement in this context. Public procurement is the formal administrative procedure that the public sector is obliged to employ when purchasing above certain thresholds (Organisation for Economic Co-operation and Development, 2011). Based on the principles of transparency and fairness of competition, public buying in the EU is regulated both at the European level as well as the national level (Bovis, 2005; Kutlina-Dimitrova & Lakatos, 2016). Taking into account the nature of SCSs – high-tech data processing and hardware components –, growing market maturity and related increasing SCS size, and the fact that thresholds can be surpassed at relatively low levels (Organisation for Economic Co-operation and Development, 2011), i.e. a few thousand euros, it can be derived that many SCSs would pass through a public procurement procedure.

Second, as per its definition, SCSs process personal data. Therefore, these services fall squarely within the scope of the GDPR. This regulation is the primary legislative instrument for data protection in the EU (Albrecht, 2016). As the successor of the 1995 Data Protection Directive, the GDPR entered into force in May 2016 and into applicability two years later (Tikkinen-Piri et al., 2018). Expanding accountability and transparency of data controllers and empowering data subjects are its central tenets (Voss, 2016). It is evident that complying with novel legislation comprises a cost component for all regulated entities. However, measures targeting enhanced accountability and transparency are particularly relevant (and potentially costly) for data controllers that are active in high risk data processing. The risk-based approach is a novelty of the GDPR compared to its predecessor, and it entails that additional activities are to be carried out, e.g. a DPIA, or general measures are expected to be performed more extensively, when the data processing can be considered as 'high risk' to the rights and freedoms of individuals (Gellert, 2018). The Article 29 Working Party offers some guidance as to

the qualification of high risk by way of some examples: i) "*systematic and extensive evaluation of personal aspects relating to natural persons […] on which decisions are based that produce legal effects concerning the natural person or similarly significant*," ii) "*large scale processing of special categories of data […], or of personal data relating to criminal convictions and offences*," and iii) "*systematic monitoring of a publicly accessible area on a large scale*" (Article 29 Working Party, 2017). In addition, the Article 29 Working Party offers factor-based guidance; notable risk factors are: i) "*large scale processing*," ii) "*matching or combining datasets*," and iii) "*innovative use or applying new technological or organizational solutions*" (Article 29 Working Party, 2017). It can be derived that a considerable number of SCSs could be considered high risk. For example, most security solutions working with cameras would constitute systematic monitoring of a public space (e.g. crowd monitoring in a busy shopping street), any service aiming to offer personalized service to city residents would likely constitute a large scale processing including bringing together data from different sources, and pervasive employment of Internet-of-Things objects would arguably fall in the 'innovative use'-category. As a result, data protection costs along the SCS development process can be expected to be relatively important.

Additional costs, whatever their origin, are likely to produce competitive effects. Research into the nexus of data protection and competition is gradually gaining academic interest. Extant research covers the GDPR's potential harms to competition in general, i.e. Gal and Aviv (2020) offer a comprehensive review of areas of tension between the EU's data protection law and competition. A different strand of papers attempts to establish some of these effects on competition empirically (Jia et al., 2019; Seo et al., 2018). Notably, Vandercruysse, Buts, and Dooms (2021) set out to assess the effect of the GDPR on competition for SCS tenders. The authors find indications for a potential negative effect of the introduction of the GDPR on the number of bids for SCS tenders. In this chapter, we aim to offer a more granular understanding of the GDPR's impact on the cost structure of individual tenderers as well as insight into potential benefits of making these additional data protection costs. To that end, we make use of the theoretical framework of transaction cost economics to perform an analysis of ex-ante transaction costs related to data protection.

2.2. Transaction cost economics

This chapter will view data protection costs in the context of tender bid submission preparation applying the theoretical lens of transaction cost economics. What follows is a general overview of relevant transaction cost theory concepts, the applied model is presented in the next section.

The field of transaction cost economics is based on the seminal works of Coase (1937) and Williamson (1975). Transaction costs originate from the search for, the conclusion of and the follow-up of a

transaction (Parker & Hartley, 2003). These costs can be considered a market inefficiency of which traditional economic models often make abstraction (Dugger, 1983). However, in many scenarios, an assumption of market inefficiency would be the more appropriate model for reality. Rather than going to the market and buying a service of the exact quality one would like for one's reservation price, in reality this process would give rise to search costs to find the correct service – imagine searching online, going to different stores, etc. –, costs related to the conclusion of a service contract – imagine drawing up or reading a contract, negotiating on price or extra services, etc. –, and following-up the contract – imagine checking whether the service has been delivered according to the desired standards, and going to court if it has not. In general, transaction costs can be split between ex-ante transaction costs and ex-post transaction costs (Petersen et al., 2019). The former concerns costs related to finding an appropriate supplier and establishing the terms of the trade, while the latter comprises contract monitoring and enforcement costs (Carbonara et al., 2016).

The principal factors theorized to determine the magnitude of transaction costs are the level of asset specificity, the contracting uncertainty, and the contracting frequency (Williamson, 2007). First, the level of asset specificity refers to the extent to which investments which are made in order to do a certain transaction are non-re-deployable (Parker & Hartley, 2003). Legal fees for drawing up a specific contract can be considered largely asset-specific. Unless the contract can be re-used for very similar transactions in the future, the usefulness of the acquired legal services is limited to the transaction at hand. The higher the asset-specificity, the lower the amount of costs that can be spread over various dealings and thus the larger the transaction cost for this particular transaction, ceteris paribus. Second, uncertainty with respect to contracting concerns the likelihood of a transaction failing (Lingard et al., 1998). Not winning a tender constitutes a failing transaction, but having a contract terminated (or a tender cancelled) as a result of unforeseen circumstances would as well. The idea is that contracting uncertainty is inversely related to the expected value of a particular transaction. As a result, environments characterized by high uncertainty create incentives to limit transaction investments. Third, contracting frequency denotes the strength of the relationship antecedents between the contracting parties (Akbar & Tracogna, 2018). Frequent dealings between two parties can render the process of contracting more efficient and reduce transaction costs across the board. However, at the same time, a strong relationship between parties can induce parties to go above and beyond and thus increase asset-specific investments (Williamson, 2007).

Previous research has suggested that the scope for inter-project spillover benefits can make transaction investments exceed what can be expected from the three standard transaction cost determinants, notable inter-project spillover benefits are reputation enhancement and capabilities upgrading (Kang et al., 2009). The reasoning goes that if making certain transaction investments can

offer rewards beyond the particular transaction ecosystem, this can prompt parties to revise appropriate investment levels upwards.

As mentioned, this work concentrates on data protection related ex-ante transaction costs. Because of the inherent features of public procurement – a tender is issued, bids are submitted, a winner is chosen and competition is de facto terminated –, ex-ante costs arguably bear the most relevance for competition (Dudkin & Välilä, 2005). Therefore, the application of the above theory as outlined below will make abstraction of all other transaction costs.

3. Model and research questions

To analyze the ex-ante transaction costs related to data protection emerging from tendering for SCSs, we employ the methodology developed by De Schepper et al. (2015) and adapt it to the particular context of SCS tendering. The authors define three important levels of analysis: i) the influence of contracting uncertainty and frequency on the level of asset-specific investment, ii) the impact of contracting uncertainty, frequency and asset-specific investment on spill-over effects, iii) the effect of frequency and asset-specific investment on contracting outcome. In what follows, the relevance of these three levels for the case of data protection costs in the context of SCS tender submission will be explained.

First, we focus on the impact of uncertainty and frequency on the level of transaction-specific data protection investment. Following the theory, one would expect that an increase in the uncertainty of winning an SCS tender would cause a decrease in the willingness to invest in data protection in the context of that tender. Factors that increase contracting uncertainty are intensified competition and lead time length. Alternatively, a higher frequency of having worked with the contracting authority in question before, or even similar authorities, could boost trust and increase data protection investment willingness. In that regard, direct organizational contact is likely important. Therefore, outsourcing data protection tasks will reduce the level of direct contact, ceteris paribus, and thus also the strength of the relationship between contracting authority and tenderer, as well as trust levels.

Second, we investigate whether uncertainty, frequency and transaction-specific data protection investment volume influence the level of spill-over benefits. A first question is to what extent competition levels and lead time impact the potential for attaining an enhanced data protection reputation or strengthened data protection capabilities. While heightened uncertainty should theoretically make SCS tenderers invest less, the open question remains if they then also invest in a way that might not be efficient in the long run, i.e. quick fixes rather than structural improvements with a scope for benefits beyond the particular tender. The analysis with regard to frequency is analogous. Also, the correlation between the size of data protection investment and potential spill-

over benefits will be addressed; does investing in data protection provide benefits beyond direct data protection effects?

Third, the final level of analysis encompasses SCS tender success factors. We intend to identify the determinants that can influence the probability of winning such a tender. In a first instance, it can be hypothesized that strong existing relations with the contracting authority in question affect win probability. Also, extensive experience in serving the public sector in general could potentially offer an edge over competitors. Last, it is our aim to establish whether the level of transaction-specific data protection investment influences the outcome of the SCS tender procedure, i.e. does investing in data protection pay-off and can data protection be a competitive advantage?

It can be concluded that the model allows for a thorough examination of the substance and clout of SCS tender data protection investment post GDPR introduction. Keeping in mind the limited sample and the explorative aim of this chapter, the overarching research questions (RQs) can be formulated as follows:

RQ1. What are the determinants of data protection related ex-ante transaction costs in the context of SCS tenders in the EU post GDPR introduction?

RQ2. What is the competitive relevance of data protection related ex-ante transaction costs in the context of SCS tenders in the EU post GDPR introduction?

The full model is displayed in Figure 10.

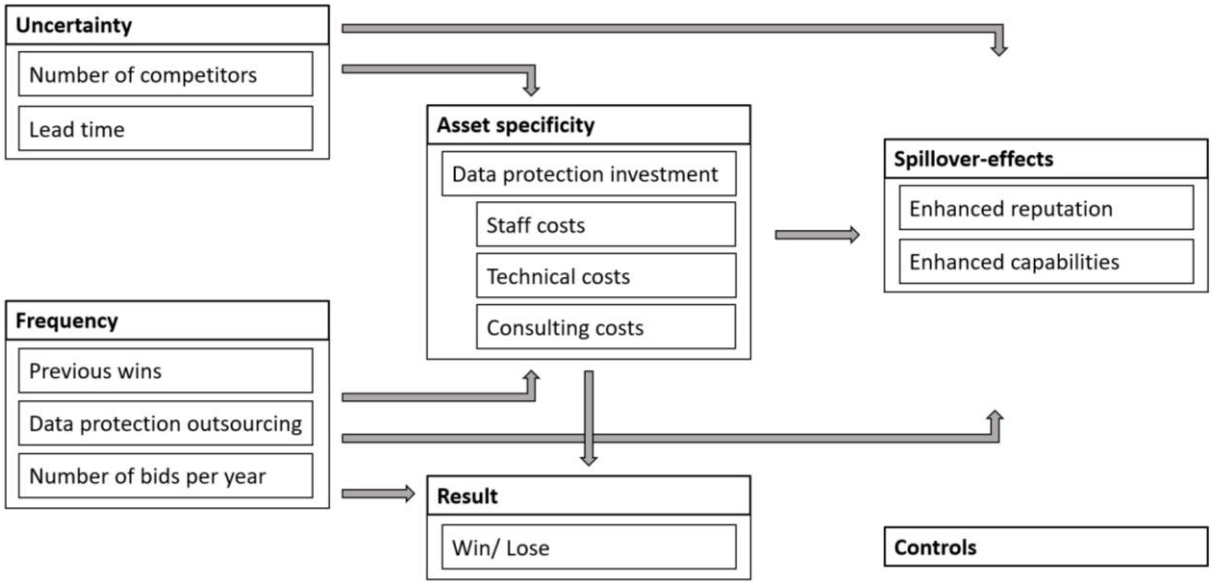

Figure 5. Theoretical model. Source: own creation based on De Schepper et al. (2015).

As can be discerned, this research has strong potential to deliver value beyond academia. From a private sector viewpoint, the answers to these questions are highly relevant for strategy concerning

cost control and data protection investment. For the public sector, findings can aid in managing private SCS provider incentives and create a market space in which data protection can flourish.

4. Methodology

The methodology section starts with an overview of the operationalization of the different variables, subsequently the data collection process is explained, and, last, the utilized econometric models are described.

4.1. Variable operationalization

First, a translation of the four principal transaction cost concepts outlined in Section two into metrics imposes itself.

As a proxy for asset specificity, we create the variable *DataProtectionSubInv*. The variable indicates to what extent the ex-ante transaction costs related to data protection are substantial relative to the financial value of the SCS tender. The scoring mechanism is a 7-point Likert scale ranging from "*strongly disagree*" to "*strongly agree*." Rather than a numeric variable, a scale was opted for to facilitate the response process. Nonetheless, an additional, optional survey question was added to gauge actual financial size of the concerned costs (cfr. Section 5.1.1.).

The concepts of 'spill-over effects' and 'uncertainty' are operationalized completely following De Schepper et al. (2015), mutatis mutandis. In contrast, we added a metric to the 'frequency' concept. The metrics measuring the strength of the historic relationship between tender issuer and SCSP, and the internal capacity of the SCSP are kept. But we also included a metric for the number of SCS tenders in which an SCSP competes annually. The rationale is that even though this experience is not with the contracting authority in question, it can arguably still offer a trust advantage.

In addition, *Win* is created as a dummy variable indicating whether or not the bid on the SCS tender was successful. This variable features as the dependent variable in our final regression analysis.

Finally, we defined a series of pure control variables. Controls are included for SCS tender size, SCS tender complexity, SCSP size, year of tender issuance, country of tender issuance, and type of public procurement procedure.

An exhaustive list of the different variables and their respective operationalization is given in Table 23.

Variable	Description	Operationalization
➢ Asset specificity		
DataProtectionSubInv	This variable indicates to what extent the investment in data protection in the context of the SCS tender was substantial in relation to the total size of the project	7-point Likert scale

➢ Spill-over effects		
EnhancedCapabilities	This variable indicates to what extent the investment in data protection in the context of the SCS tender enhanced the capabilities of the tenderer	7-point Likert scale
EnhancedReputation	This variable indicates to what extent the investment in data protection in the context of the SCS tender enhanced the reputation of the tenderer	7-point Likert scale
➢ Uncertainty		
NumberOfCompetitors	This variable indicates the level of competition for the SCS tender	7-point scale
LeadTime	This variable indicates to what extent the lead time was long (opening of bidding period to announcement of winner) of the SCS tender	7-point Likert scale
➢ Frequency		
PreviousWins	This variable indicates to what extent the tenderer has previously won tenders by the SCS procurer	7-point Likert scale
DataProtectionOutsourcing	This variable indicates to what extent data protection efforts were outsourced	7-point scale
NumberOfBidsPerYear	This variable indicates the number of SCS tenders in which the tenderer participates annually	7-point scale
➢ Result		
Win	This variable indicates whether the tenderer won the SCS tender	Dummy
➢ Controls		
Size	This variable indicates the financial size of the SCS tender	7-point scale
Complexity	This variable indicates the complexity of the SCS concerned in the tender	7-point Likert scale
StartUp	This variable indicates whether the tenderer was a start-up	Dummy
UpscalingStartUp	This variable indicates whether the tenderer was an upscaling start-up	Dummy
EstablishedSME	This variable indicates whether the tenderer was an established SME	Dummy
EstablishedMultinational	This variable indicates whether the tenderer was an established multinational	Dummy
Year dummies	This variable indicates whether the SCS tender was closed in 2017, 2018, 2019, 2020 or 2021	Dummy
Country dummies	This variable indicates whether the SCS tender was issued in Belgium, France, Germany, Luxemburg, the Netherlands, or another EU country	Dummy
Open	This variable indicates whether the SCS tender was issued as part of an open procurement procedure	Dummy

Restricted	This variable indicates whether the SCS tender was issued as part of a restricted procurement procedure	Dummy
Negotiated	This variable indicates whether the SCS tender was issued as part of a negotiated procurement procedure	Dummy
CompetitiveDialogue	This variable indicates whether the SCS tender was issued as part of a competitive dialogue procurement procedure	Dummy
InnovationPartnership	This variable indicates whether the SCS tender was issued as part of an innovation partnership procurement procedure	Dummy
OtherProcurement	This variable indicates whether the SCS tender was issued as part of another procurement procedure	Dummy

Table 23. Overview of operationalized variables (core variables). Source: own creation.

4.2. Data collection process

Data was collected by way of a survey. The survey consisted of 31 questions and took approximately 5 minutes to complete. The unit of analysis of the survey was individual SCS tender bids submitted post GDPR introduction, respondents could thus enter multiple bids if desired. Respondents were asked to evaluate whether or not the tender could be considered an SCS tender in the initial stage of the survey, to that end they were offered our SCS definition. With an eye on safeguarding consistency and comparability, respondents were asked to respond using balanced 7-point scales to the maximum possible extent. Common methodological guidelines with respect to survey construction were abided by, following the principles established by Callegaro et al. (2015).

Over 1,000 private smart city service providers (SCSPs) based in the EU were contacted directly. In addition, a number of EU smart city community initiatives were approached as well with the ask of circulating the survey among their members. All general contact email addresses were gathered from organization websites through desk research. Initial contact encompassed an email outlining the aims of the study, highlighting the potential practical value of any findings, and containing a link to the online survey. In case of non-response, up to five reminders were sent. In a final stage, non-respondents were approached telephonically as well. Throughout, the authors were available to answer any questions both via email as well as via telephone.

Our final sample consists of 72 useable survey responses.[18] While this sample is limited, this sample size suffices for the explorative aim of this chapter. In our view, the response rate is limited for two main reasons. First, an important number of SCSP representatives indicated that their company had

[18] Useable means that at least two out of three standard ex-ante transaction cost theme questions were completed.

not yet participated in any tender process. It appears that quite some SCSPs try to develop the 'proof-of-concept' stage outside a framework of public-private collaboration. Furthermore, while the smart cities concept has been around for some time, the actual full-fledged implementation of SCSs is still quite a novelty. Second, our survey contained questions on company characteristics, on particular project features, but also on more technical data protection matters. This entails that likely several SCS project collaborators would have to be involved in order to be able to complete the survey, which might be discouraging to some respondents. The large drop-out rate, i.e. over 50 %, around the first questions on data protection, seems to suggest as much. The limited sample size impacts representativeness, especially in view of the EU-wide analysis. However, notable points of interest for both academia and policy can still be distilled. The principal value of this chapter lies in the cutting-edge nature of the insights, and the application of the transaction cost economics framework to data protection.

4.3. Econometric models

The survey data was recoded to allow for econometric investigation using STATA (Statacorp, 2009). A statistical approach allows for discovery of trends that might not be readily observable by people in practice due to its capacity to process a large number of observations and the possibility to enter controls (Cameron & Trivedi, 2005). In addition, the approach ensures a certain level of generalizability beyond individual case-studies (Wooldridge, 2015).

Our analysis is based on two main regression types. On the one hand, three standard ordinary least squares regressions (OLS), and, on the other hand, a logistic regression. The regressions will be presented following the structure of the three levels of analysis identified by De Schepper et al. (2015). Level 1 constitutes the impact of uncertainty and frequency on the level of data protection related ex-ante transaction costs, level 2 concerns the influence of uncertainty, frequency and the level of ex-ante transaction costs related to data protection on spill-over benefits, and level 3 investigates the effect of frequency and the level of data protection related ex-ante transaction costs on contracting outcome.

The level one OLS regression is presented in Equation 1 (E1):

E1. $DataProtectionSubInv_i = Constant + \beta_1 NumberOfCompetitors_i + \beta_2 LeadTime_i + \beta_3 PreviousWins_i + \beta_4 DataProtectionOutsourcing_i + \beta_5 NumberOfBidsPerYear_i + \beta_6 Size_i + \beta_7 Complexity_i + \beta_8 UpscalingStartUp_i + \beta_9 EstablishedSME_i + \beta_{10} EstablishedMultinational_i + \beta_{11} Y2021_i + \beta_{12} Y2020_i + \beta_{13} Y2019_i + \beta_{14} Y2018_i + \beta_{15} Belgium_i + \beta_{16} France_i + \beta_{17} Germany_i + \beta_{18} Netherlands_i + \beta_{19} OtherEU_i + \beta_{20} Restricted_i + \beta_{21} Negotiated_i + \beta_{22} CompetitiveDialogue_i + \beta_{23} InnovationPartnership_i + \beta_{24} OtherProcurement_i + \varepsilon_i$

with i referencing to the SCS tender ranging from 1 to 63.

Level two concerns two OLS regressions as the spill-over benefits, i.e. capability enhancement and reputation enhancement, are inspected individually. Both Equation 2.1 (E2.1) and Equation 2.2 (E2.2) are run to that end.

E2.1. $EnhancedCapabilities_i = Constant + \beta_1 DataProtectionSubInv_i + \beta_2 NumberOfCompetitors_i + \beta_3 LeadTime_i + \beta_4 PreviousWins_i + \beta_5 DataProtectionOutsourcing_i + \beta_6 NumberOfBidsPerYear_i + \beta_7 Size_i + \beta_8 Complexity_i + \beta_9 UpscalingStartUp_i + \beta_{10} EstablishedSME_i + \beta_{11} EstablishedMultinational_i + \beta_{12} Y2021_i + \beta_{13} Y2020_i + \beta_{14} Y2019_i + \beta_{15} Y2018_i + \beta_{16} Belgium_i + \beta_{17} France_i + \beta_{18} Germany_i + \beta_{19} Netherlands_i + \beta_{20} OtherEU_i + \beta_{21} Restricted_i + \beta_{22} Negotiated_i + \beta_{23} CompetitiveDialogue_i + \beta_{24} InnovationPartnership_i + \beta_{25} OtherProcurement_i + \varepsilon_i$

with i referencing to the SCS tender ranging from 1 to 61.

E2.2. $EnhancedReputation_i = Constant + \beta_1 DataProtectionSubInv_i + \beta_2 NumberOfCompetitors_i + \beta_3 LeadTime_i + \beta_4 PreviousWins_i + \beta_5 DataProtectionOutsourcing_i + \beta_6 NumberOfBidsPerYear_i + \beta_7 Size_i + \beta_8 Complexity_i + \beta_9 UpscalingStartUp_i + \beta_{10} EstablishedSME_i + \beta_{11} EstablishedMultinational_i + \beta_{12} Y2021_i + \beta_{13} Y2020_i + \beta_{14} Y2019_i + \beta_{15} Y2018_i + \beta_{16} Belgium_i + \beta_{17} France_i + \beta_{18} Germany_i + \beta_{19} Netherlands_i + \beta_{20} OtherEU_i + \beta_{21} Restricted_i + \beta_{22} Negotiated_i + \beta_{23} CompetitiveDialogue_i + \beta_{24} InnovationPartnership_i + \beta_{25} OtherProcurement_i + \varepsilon_i$

with i referencing to the SCS tender ranging from 1 to 61.

The regression for level three constitutes a logistic model, because the dependent variable is a dummy. The model is displayed in Equation 3 (E3):

E3. $Win_i = Constant + \beta_1 DataProtectionSubInv_i + \beta_2 NumberOfCompetitors_i + \beta_3 LeadTime_i + \beta_4 PreviousWins_i + \beta_5 DataProtectionOutsourcing_i + \beta_6 NumberOfBidsPerYear_i + \beta_7 Size_i + \beta_8 Complexity_i + \beta_9 UpscalingStartUp_i + \beta_{10} EstablishedSME_i + \beta_{11} EstablishedMultinational_i + \beta_{12} Restricted_i + \beta_{13} Negotiated_i + \beta_{14} CompetitiveDialogue_i + \beta_{15} InnovationPartnership_i + \beta_{16} OtherProcurement_i + \varepsilon_i$

with i referencing to the SCS tender ranging from 1 to 63.

5. Results

The exploration of the results starts out with a set of descriptive statistics and data visualizations, the subsequent econometric analysis section contains the substantive empirical research.

5.1. Descriptive statistics

From the descriptive statistics in Table 24 some interesting insights can be discerned, notably concerning SCS tender size, commonly used public procurement procedures, SCS tender competition levels, and data protection outsourcing.

Variable	Observations	Mean	Std. Dev.	Min	Max
➢ Asset specificity					
DataProtectionSubInv	63	3.8095	1.6930	1	7
➢ Spill-over effects					
EnhancedCapabilities	61	4.5902	1.6671	1	7
EnhancedReputation	61	4.6721	1.7769	1	7
➢ Uncertainty					
NumberOfCompetitors	72	4.9722	1.8536	1	7
LeadTime	72	4.6806	1.5089	1	7
➢ Frequency					
PreviousWins	72	3.4306	1.6936	1	6
DataProtectionOutsourcing	72	2.3611	1.7386	1	7
NumberOfBidsPerYear	72	4.6111	1.9104	1	7
➢ Result					
Win	72	0.6806	0.4695	0	1
➢ Controls					
Size	72	4.4167	1.8366	1	7
Complexity	72	5.1528	1.1341	3	7
StartUp	72	0.1389	0.3483	0	1
UpscalingStartUp	72	0.2917	0.4577	0	1
EstablishedSME	72	0.3889	0.4909	0	1
EstablishedMultinational	72	0.1806	0.3873	0	1
Y2021	72	0.3472	0.4794	0	1
Y2020	72	0.4028	0.4939	0	1
Y2019	72	0.1528	0.3623	0	1
Y2018	72	0.0833	0.2783	0	1
Y2017	72	0.0139	0.1179	0	1
Belgium	72	0.2917	0.4577	0	1
France	72	0.1528	0.3623	0	1
Germany	72	0.0694	0.2560	0	1
Luxemburg	72	0.0139	0.1179	0	1
Netherlands	72	0.0694	0.2560	0	1
OtherEU	72	0.4028	0.4939	0	1
Open	72	0.5278	0.5027	0	1
Restricted	72	0.1250	0.3330	0	1
Negotiated	72	0.1250	0.3330	0	1
CompetitiveDialogue	72	0.0833	0.2783	0	1
InnovationPartnership	72	0.0972	0.2983	0	1
OtherProcurement	72	0.0417	0.2012	0	1

Table 24. Overview of descriptive statistics (core variables). Source: own creation.

First, the range € 100,000 to € 199,999 constitutes the average size of an SCS tender in our sample. Also, Figure 11 displays that our sample contains tenders of a wide variety of sizes. SCS tenders valued

below € 10,000 are rare, but this was to be expected seeing inherent SCS characteristics. SCS tenders between € 10,001 and over € 1,000,000 are well-represented.

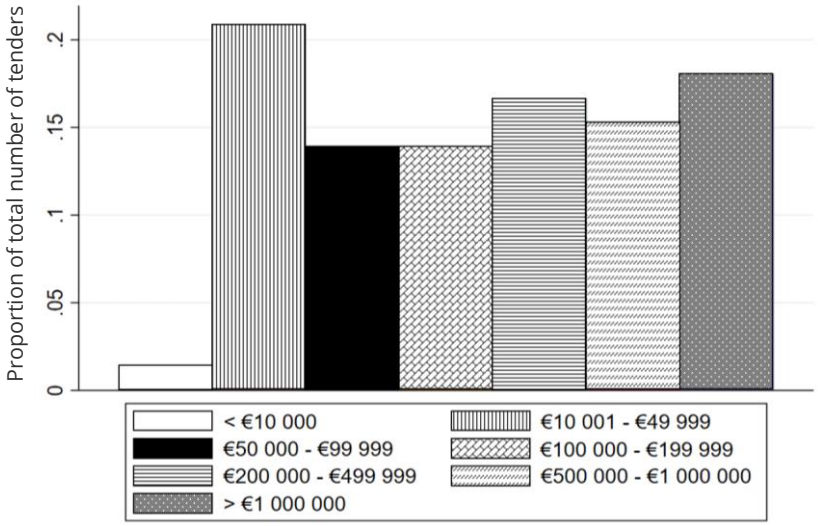

Figure 6. Overview SCS tender size (n=72). Source: own creation using STATA.

Second, Figure 12 demonstrates that the large majority of SCS tenders is issued through an open public procurement procedure. Utilization of procedures tailoring more to collaboration and negotiation, like the competitive dialogue and the innovation partnerships, is rather rare.

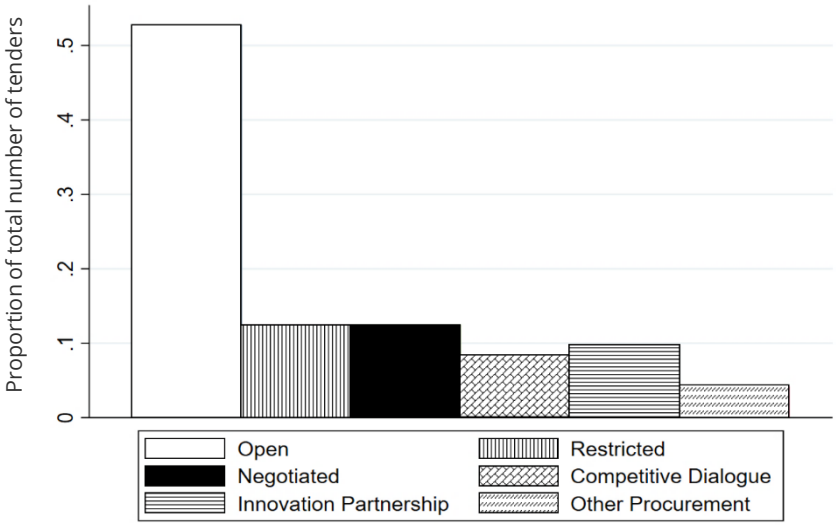

Figure 7. Overview SCS tender public procurement procedure type (n=72). Source: own creation using STATA.

Third, an average SCS tender receives between four and five bids. Figure 13 shows that our sample also contains a good number of tenders to which more than 6 tenderers participated.

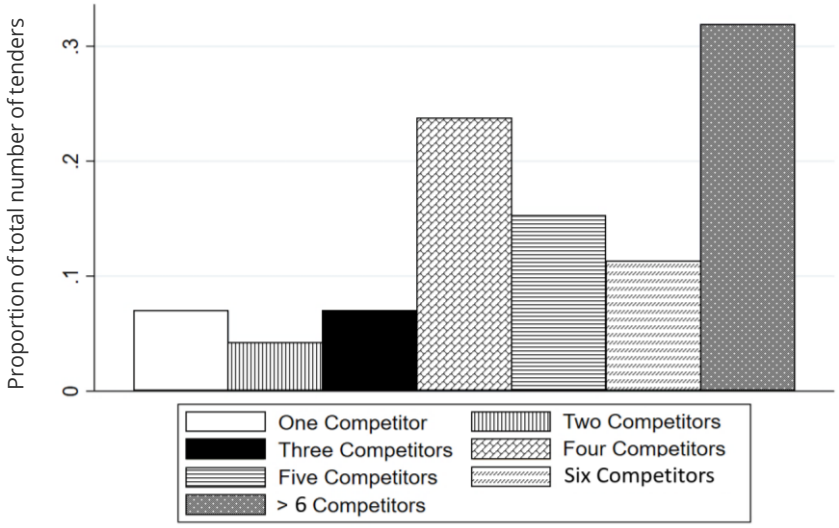

Figure 8. Overview SCS tender competition level (n=72). Source: own creation using STATA.

Last, examining the degree of outsourcing regarding data protection in the context of SCS tenders, we find that the average level is relatively low. As Figure 14 shows, in over 40 % of observations there is no outsourcing whatsoever, the average sits around 20 % of outsourcing.

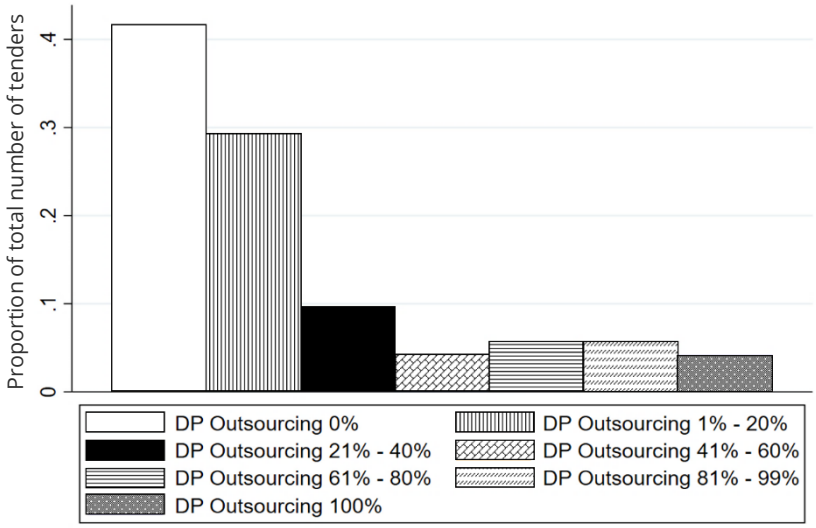

Figure 9. Overview SCS tender data protection outsourcing level (n=72). Source: own creation using STATA.

5.1.1.Focus on costs

As part of the survey, we opted to also include some questions with an aim to gauge ex-ante transaction costs related to data protection size and composition. To the best of our knowledge, concrete data on these topics is non-existent. For these more specific questions, respondents were offered the option to indicate that they were not able to formulate a reliable answer.

Table 25 presents the operationalization of the additional cost variables, while Table 26 displays their descriptive statistics.

Variable	Description	Operationalization
➢ Sum of data protection related ex-ante transaction costs		
DP Investment	This variable indicates the size of the investment in data protection in the context of the SCS tender in relation to the total size of the project	8-point scale
➢ Composition of data protection related ex-ante transaction costs		
Staff Cost	This variable indicates the size of the staff costs in man-days as part of the investment in data protection in the context of the SCS tender	7-point scale
Technical Cost	This variable indicates the size of the technical costs in man-days as part of the investment in data protection in the context of the SCS tender	7-point scale
Cons Cost	This variable indicates the size of the consulting costs in euros as part of the investment in data protection in the context of the SCS tender	7-point scale

Table 25. Overview of operationalized variables(additional cost variables). Source: own creation.

Variable	Observations	Mean	Std. Dev.	Min	Max
➢ Sum of data protection related ex-ante transaction costs					
DP Investment	49	4.4082	2.0708	1	8
➢ Composition of data protection related ex-ante transaction costs					
Staff Cost	50	3.9600	2.0599	1	7
Technical Cost	46	3.5435	1.9172	1	7
Cons Cost	45	3.0000	1.8708	1	7

Table 26. Overview of descriptive statistics (additional cost variables). Source: own creation.

Table 26 displays the descriptive statistics of the additional cost variables. In our explorative sample, the average size of ex-ante transaction costs related to data protection borne by the tenderer in the context of an SCS tender is between 4 % and 5 % of the total financial value of said tender, Dudkin and Välilä (2005) determined that total transaction costs in public-private partnerships can amount to over 10 % of the financial value. Figure 15 shows all responses to the cost size question split between the various possible answers.

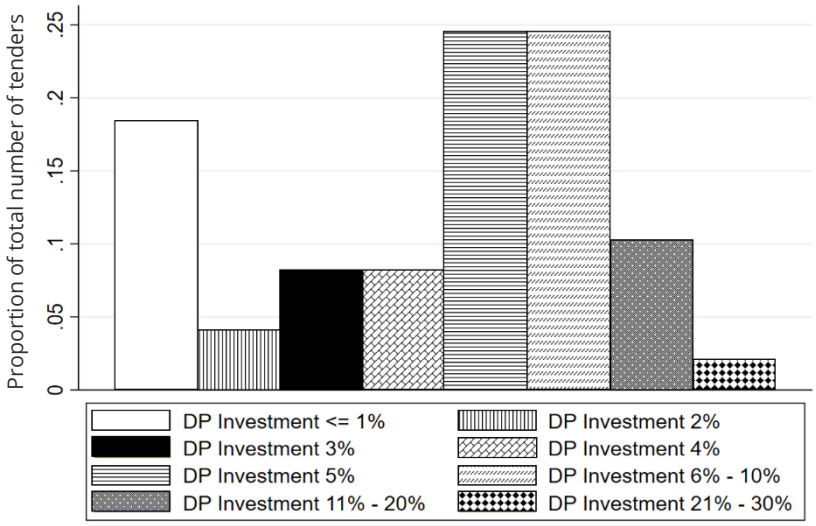

Figure 10. Overview relative size of SCS tender data protection investment (n=49). Source: own creation using STATA.

Focusing on cost composition, we find that staff costs are at four to five man-days on average, while technical costs are closer to three man-days, and consulting costs amount to a sum between € 3,000 and € 5,000 on average. The visualizations of this more granular cost data can be found in Figures A.4 through A.6 in Appendix 3. It has to be noted that this cost data is to be interpreted as merely explorative seeing the limited amount of data.

5.2. Econometric analysis

A general technical comment on the econometric analysis regards multicollinearity. We ran multicollinearity analyses for all regressions to confirm none of the correlations between independent variables exceed 0.8, stronger intervariable correlations can render regression estimates spurious (Berry & Feldman, 1985). These analyses do not point to multicollinearity. Furthermore, since correlations between variables measuring different aspects of the same transaction cost concept are well below the 0.8 threshold, we opt to include all different metrics in the respective regressions and analyze these metrics individually.

The examination of the regression results is organized in three parts, i.e. the three different levels of analysis as set out in Section four.

5.2.1. Uncertainty and frequency explaining the level of data protection related ex-ante transaction costs

Full OLS regression results for this first level are presented in Table 27.

First, one observes that uncertainty does not impact data protection related ex-ante transaction costs in our explorative sample. A larger uncertainty in the form of longer lead times or an increased number

of competitors does not cause SCS tenderers to limit their data protection costs, nor does increased competitive pressure seem to induce larger ex-ante data protection investments.

Second, there is a significant positive correlation between the strength of the historic relationship between tenderer and tendering authority, and the perception of having done a substantial ex-ante data protection investment. As the number of tenders that the tenderer has previously won from the tendering authority increases, so does the data protection investment on the SCS tender. Also, the perceived size of the ex-ante data protection investment correlates with the level of data protection outsourcing. A possible explanation could be that these outsourced costs are more visible than their internal counterparts, and thus are accounted for more consistently.

Third, a strong negative correlation between the financial size of the SCS tender and respondents reporting "*substantial data protection investment*" can be discerned. The explanation is rather straightforward: as tender size increases, the relative size of any transaction cost type decreases, ceteris paribus. This is in line with findings from previous research (Dudkin & Välilä, 2005).

Last, the results empirically show a positive correlation between the complexity of an SCS project and the size of ex-ante transaction costs related to data protection in the context of its tender. This finding somewhat confirms that the risk-based approach propagated by the GDPR (Gellert, 2018), i.e. the fact that larger risks – here proxied by complexity – demand more stringent, and thus expensive, data protection measures, is indeed applied in practice. It basically underlines the inherent scalability of the GDPR, i.e. project characteristics influence data protection costs.

Regression type	Standard OLS
Dependent variable	DataProtectionSubInv
Number of observations	63
F(24, 38)	2.90
Prob > F	0.0016
R-squared	0.6468
Adj R-squared	0.4238
Root MSE	1.2852

Variable	**Coef.**	**Std. Err.**	**P>t**
➢ Uncertainty			
NumberOfCompetitors	0.1150	0.1176	0.334
LeadTime	0.0380	0.1622	0.816
➢ Frequency			
PreviousWins	**0.3297*** **	0.1211	0.010
DataProtectionOutsourcing	**0.3424** **	0.1375	0.017
NumberOfBidsPerYear	-0.1607	0.1443	0.273
➢ Controls			
Size	**-0.5291*** **	0.1462	0.001
Complexity	**0.5355** **	0.2218	0.021

UpscalingStartUp	0.4599	0.8993	0.612
EstablishedSME	0.1589	0.8160	0.847
EstablishedMultinational	1.1344	0.8571	0.194
Restricted	**0.9047***	0.5261	0.094
Negotiated	-0.6901	0.6314	0.281
CompetitiveDialogue	-1.0271	0.7245	0.164
InnovationPartnership	0.6143	0.6997	0.385
OtherProcurement	**2.7071****	1.1496	0.024
Constant	-0.0589	2.7520	0.983
Legend: coefficient are attributed * when significant at the 0.10 level, ** when significant at the 0.05 level, and *** when significant at the 0.01 level Remark: year and country dummies are included but not reported			

Table 27. OLS regression results of model based on E1. Source: own creation.

5.2.2. Uncertainty, frequency and the level of data protection related ex-ante transaction costs explaining the level of spill-over benefits

Table 28 displays the results of the two regressions for the second level of analysis.

Interestingly, the results of the regressions with the two distinct spill-over benefits as dependent variables are practically identical.

First, there is a positive correlation between the size of the ex-ante data protection investment in the context of the tender and the extent to which the tenderers capabilities and reputation are reported to be enhanced. This is a promising find as it seems to suggest that there are benefits to be reaped from investing in data protection apart from compliance, and that the scope for attaining these benefits grows with data protection investment size.

Second, one observes a positive relation between going through a competitive dialogue procurement procedure and enhancing the company's capabilities and reputation. The explanation is quite intuitive. A competitive dialogue procedure can be considered a learning environment to some extent, as due to its set-up there is ample room for discussion and negotiation between the various parties (Buccino et al., 2020). Apparently a more involved procedure leads to a more conscious registration and realization of spill-over effects. The fact that the results also demonstrate a negative correlation between going through a restricted procurement procedure, which is at the other end of the public procurement procedure type spectrum (European Commission, 2020e; Hueskes et al., 2017), and enhancing the company's capabilities and reputation, is a further indication in that direction.

Regression type	Standard OLS	Standard OLS
Dependent variable	EnhancedCapabilities	EnhancedReputation
Number of observations	61	61
F(25, 35)	2.99	2.13
Prob > F	0.0015	0.0194
R-squared	0.6810	0.6036

Adj R-squared	0.4532	0.3205
Root MSE	1.2328	1.4647

Variable	**Coef.**	**Std. Err.**	**P>t**	**Coef.**	**Std. Err.**	**P>t**
➢ Asset specificity						
DataProtectionSubInv	**0.5008*** **	0.1611	0.004	**0.4824** **	0.1914	0.016
➢ Uncertainty						
NumberOfCompetitors	-0.0646	0.1158	0.581	0.1026	0.1376	0.461
LeadTime	**0.4705*** **	0.1569	0.005	**0.3190***	0.1864	0.096
➢ Frequency						
PreviousWins	0.0370	0.1380	0.790	-0.0151	0.1640	0.927
DataProtectionOutsourcing	-0.0565	0.1425	0.694	-0.0580	0.1694	0.734
NumberOfBidsPerYear	-0.1399	0.1703	0.417	-0.0254	0.2023	0.901
➢ Controls						
Size	-0.0324	0.1674	0.848	0.2030	0.1989	0.315
Complexity	-0.4178	0.2606	0.118	-0.4017	0.3097	0.203
UpscalingStartUp	0.1890	0.9353	0.841	0.3527	1.1113	0.753
EstablishedSME	0.0661	0.8073	0.935	-0.2385	0.9592	0.805
EstablishedMultinational	0.1900	0.8459	0.824	0.3498	1.0050	0.730
Restricted	**-1.2782** **	0.5270	0.021	**-1.8404*** **	0.6262	0.006
Negotiated	-0.1383	0.6222	0.825	-0.0843	0.7393	0.910
CompetitiveDialogue	**2.0428*** **	0.7313	0.008	**1.4693***	0.8689	0.100
InnovationPartnership	0.2827	0.6802	0.680	0.6869	0.8081	0.401
OtherProcurement	1.8429	1.1982	0.133	0.9229	1.4236	0.521
Constant	1.4263	2.6431	0.593	-2.0773	3.1403	0.513
Legend: coefficient are attributed * when significant at the 0.10 level, ** when significant at the 0.05 level, and *** when significant at the 0.01 level Remark: year and country dummies are included but not reported						

Table 28. OLS regression results of models based on E2.1 (left) and E2.2 (right). Source: own creation.

5.2.3. Frequency and the level of data protection related ex-ante transaction costs explaining tender outcome

The results of the logistic regression run to gather the determinants of SCS tendering success are shown in Table 29.

First and foremost, our explorative results indicate that there is no significant correlation between the level of ex-ante data protection transaction investments and the probability of eventually winning the SCS tender. From a competitive point of view, this find is quite remarkable. It suggests that data protection levels might currently lack the potential to be a competitive edge in the public sector market based on our sample, e.g. employing expensive state-of-the-art data protection technologies cannot truly be valorized in competitive terms.

Second, unsurprisingly, we find a negative correlation between the number of competitors and the probability of winning the SCS tender, ceteris paribus.

Last, compared to start-ups, upscaling start-ups, established SMEs, and established multinationals have a higher likelihood of winning an SCS tender. In our sample, newer start-ups are thus confronted with a significantly lower success probability. It is possible that opting for companies with longer track records is used as a risk-mitigation strategy (Johnson et al., 2021), i.e. the probability of being confronted with teething problems is reduced.

Regression type	Logistic regression
Dependent variable	Win
Number of observations	63
LR chi2(16)	19.86
Prob > chi2	0.2265
Log likelihood	-30.169852
Pseudo R2	0.2476

Variable	**Coef.**	**Std. Err.**	**P>z**
➢ Asset specificity			
DataProtectionSubInv	0.0782	0.3017	0.796
➢ Uncertainty			
NumberOfCompetitors	**-0.4955***	0.2582	0.055
LeadTime	0.5201	0.3490	0.136
➢ Frequency			
PreviousWins	-0.0250	0.2518	0.921
DataProtectionOutsourcing	-0.2754	0.2610	0.291
NumberOfBidsPerYear	-0.1118	0.2285	0.625
➢ Controls			
Size	-0.3776	0.3177	0.235
Complexity	0.1653	0.4511	0.714
UpscalingStartUp	**2.7679***	1.5116	0.067
EstablishedSME	**3.2369****	1.4257	0.023
EstablishedMultinational	**3.6575****	1.7136	0.033
Restricted	0.6782	1.0912	0.534
Negotiated	1.1275	1.2279	0.358
CompetitiveDialogue	-1.7471	1.3454	0.194
InnovationPartnership	**3.1934***	1.9063	0.094
OtherProcurement	-2.2946	1.8553	0.216
Constant	-0.4427	2.5199	0.861
Legend: coefficient are attributed * when significant at the 0.10 level, ** when significant at the 0.05 level, and *** when significant at the 0.01 level			

Table 29. Logistic regression results of model based on E3. Source: own creation.

In a context where the number of observations is low and the number of different combinations of covariates is high, the likelihood ratio (LR) chi-square test can be biased (Allison, 2014; Kuss, 2002). Therefore, to assess the goodness of fit of the logistic model, we ran a Hosmer-Lemeshow test with ten groups (Hosmer & Lemeshow, 1980). The test is positive with regard to the model fitting our data as can be discerned from Table 30.

Goodness-of-fit test	
Number of observations	63
number of groups	10
Hosmer-Lemeshow chi2(8)	2.67
Prob > chi2	0.9532

Table 30. Goodness-of-fit test for logit regression of model based on E3. Source: own creation.

6. Discussion

As a starting point for the discussion we refer back to the theoretical model laid out in Section 3. Figure 16 displays the various positive (+) and negative (-) correlations, as well as lack thereof (O), that we found empirical backing for.

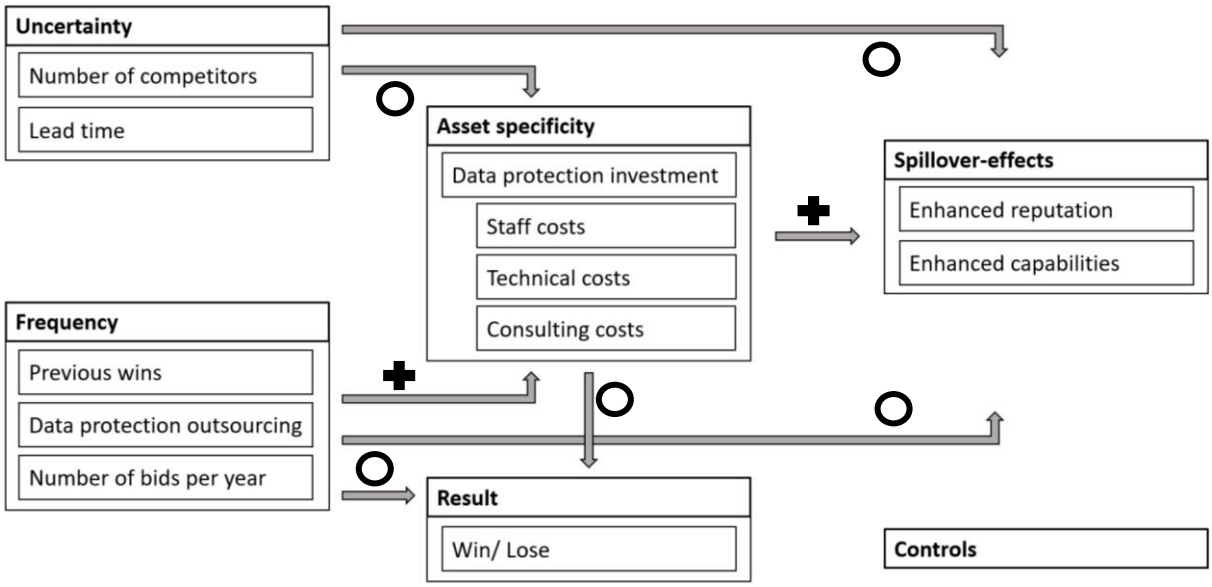

Figure 11. Empirical results with regard to theoretical model. Source: own creation based on De Schepper et al. (2015).

We note that our results should be cautiously interpreted as the sample size is limited. However, this explorative chapter draws attention to various points of interest and can serve as a basis for further research. There are three main results leading to highly pertinent implications for academia as well as policy and practice.

First, we established that strong historic relations between tenderer and tendering authority, and project complexity, influence the level of ex-ante data protection investment. The former underlines the importance of relationship management to stimulate the private sector to invest more in data protection of SCSs. Interestingly, this also puts into perspective the assumption that vendor preferencing from the part of the public authority is always bad per se. In our sample, it seems that it induces the party benefiting from the preferencing to invest more rather than less. The latter demonstrates that GDPR compliance does not (solely) constitute a fixed cost. The fact that SCS complexity is directly proportional to data protection costs controlling for project size, shows that business is likely indeed practically adopting the risk-based approach proclaimed by the GDPR (van Dijk

et al., 2016). In short, the business case for investing in data protection becomes stronger, the more complex the project is. This is interesting to note as this relation apparently even holds in the current climate of 'weak enforcement' by data protection authorities EU-wide (Lancieri, 2021), i.e. in absence of the so-called stick.

Second, we showed that investing in data protection could indeed yield benefits apart from increasing data protection levels in the form of boosting both internal capabilities and organizational reputation. In addition, these benefits seem to grow as investment size increases. This finding can be utilized to demonstrate to the private sector that there is indeed a concrete interest in approaching data protection in a diligent way, too often tenderers still view data protection law compliance as a mere cost hurdle. Also, relatedly, it was found that these benefits are more prone to produce themselves in the context of a competitive dialogue. Thus, arguably, public procurement procedures which are more conducive of inter-organization learning, are to be preferred for SCS tenders when incentives for private sector data protection investment are to be optimized.

Last, and most notably, we have found indications that investing in data protection does not increase the probability of winning SCS tenders. Seeing that the size of our sample of tenders is restricted, it is important to mark this finding as explorative. Nonetheless, in our sample, the potential for data protection levels to be a competitive advantage in the smart city market does not seem to be present. Furthermore, it seems that the private sector is aware of this fact. Our results show that increased competition for tenders does not induce tenderers to invest more in data protection of SCSs, i.e. data protection is not considered a (key) field for competition. All of this adds insult to injury as the perceived expected compliance cost might have made companies exit or not enter the market as was alluded to in previous research (Gal & Aviv, 2020; Vandercruysse, Buts, and Dooms, 2021). Our research suggests that the onus is on the public sector to rectify this problematic situation and to create an environment in which data protection can flourish. It points to a need for the evaluation scope of SCS tender bids to go beyond mere core functionality and price, and include data protection elements. Likely, this will necessitate increasing tendering organizations' resources and data protection expertise as well as wide-spread sharing of best practices. However, our exploration hints that the suggested broadened evaluation is an important condition for using competition as a lever for increasing data protection levels.

7. Conclusion

This chapter constitutes the first investigation into data protection related ex-ante transaction costs borne by private sector actors. It should be noted that its aims are explorative in nature.

We focus on the specific context of tenders for SCSs issued in the EU since the introduction of the GDPR. Using a slightly adapted version of the three-level framework of De Schepper et al. (2015), an econometric analysis of 72 bids was conducted. Sample size is thus limited, and any results should be interpreted with due caution. On the first level of the framework, it was found that the historic relationship between tendering organization and tenderer as well as the level of data protection outsourcing positively influence the reported level of ex-ante transaction costs related to data protection. Also, project complexity increases reported costs. In contrast, the number of bidders, a proxy for the level of competition, did not affect the data protection investment levels. On the second level, it was observed that the level of ex-ante data protection investment positively impacted the level of spill-over benefits. Additionally, the competitive dialogue procurement procedure was found to be particularly conducive to the realization of these benefits. On the third level, it was established that ex-ante transaction costs related to data protection levels do not explain variability in the probabilities of winning an SCS tender in our sample.

Most interestingly, the combined analysis of levels one and three suggests that tendering organizations' bid evaluation procedures might be unduly narrow. By the private sector, data protection is arguably not seen as an SCS feature which lends itself to producing a competitive advantage. By the public sector, at least in our explorative sample, data protection is not evaluated and scored in a way such that SCSs with better data protection are more likely to win a tender, ceteris paribus. To incentivize the private sector to ameliorate data protection levels, it could be an important step that the public sector first shows it commitment concerning the matter. In that regard, investments in additional resources and expertise are probably indispensable.

The research also has a number of limitations.

The first limitation has to do with the absence of a comparison between ex-ante transaction costs related to data protection before the introduction of the GDPR and those after its introduction. In order to truly measure the cost effect of the GDPR such an analysis would be the gold standard. We were not able to collect the necessary data to do this analysis. Nonetheless, this study offers useful insight into the current situation. Further research could employ more qualitative methodologies to contrast the before and after period.

The second limitation concerns the limited number of observations. Because of the relative novelty of the GDPR and the fact that data protection expertise is often very concentrated organizationally, finding respondents who possess all necessary information to complete our survey was extremely challenging (cfr. the difference between the number of contacted organizations and the respondents, and the attrition rate during the survey). Nonetheless, 72 observations constitute a sufficient number

to exploratively analyze the issue at hand and lay the groundwork for further study. We note that our sample might lack the representativeness to allow for strong general conclusions. However, the results can indicate points of interest for both policy and academia. Preliminary exploration is necessary to allow for prompt policy intervention and to induce deepening research. Moreover, value also lies in the chapter constituting the first research on the topic at hand, and the contribution in terms of the application of the transaction costs economics framework to the realm of data protection.

Further research could look into the variability of the identified correlations over time. For example, it would be very interesting to monitor whether data protection investment levels will become a determinant of SCS tender success as data protection awareness grows and/ or the scope of bid evaluations is broadened.

Another avenue for further research concerns specific transaction cost levels. A holistic analysis of transaction costs in the context of SCS tenders could shed some light on the relative importance of those costs specifically related to data protection. Alternatively, an analysis of data protection transaction costs covering the entire contract life-cycle would also offer valuable additional insights.

Chapter 8. Data protection in smart cities: Pre-commercial procurement as a silver bullet?[19,20]

Abstract

Globally, cities are adopting smart services at a rapidly increasing pace. Such services may benefit the public interest, yet they also bring risks to fundamental rights of city-dwellers. The ubiquity of available technology applications and lack of expertise within public administrations present a potential danger to rights such as privacy, equality, and in particular, data protection.

As custodians of the public interest, public spaces and fundamental rights, cities should consider the need to protect rights and enable democratic oversight and accountability when procuring smart services. These peculiarities vis-à-vis private service provision complicate utilizing classic public procurement procedures as off-the-shelf IT-applications rarely cater to these requirements.

To enable public sector innovation, the European Union (EU) supported a series of public procurement procedures aimed to offer more leeway for negotiation between public and private partners than a pure sales relationship. The exponent of these is pre-commercial procurement. Allowing public sector administrators to be closely involved in the product development stage and to really co-create with private partners, prevents mismatches between private sector offerings and public sector needs. At the same time, the procedure offers a learning opportunity for multiple private partners and can induce these to offer more transparency, oversight and accountability by-default.

This chapter contrasts data protection governance in the context of classic and pre-commercial procurement of smart city services. Through case studies, opportunities and pitfalls for public administrations will be distilled. Our findings are especially valuable for administrations investing in sustainable human-centric smart city development.

[19] This chapter was presented at the First Interdisciplinary Utrecht University Centre for Public Procurement PhD Forum, we thank the conference attendees for their useful comments. Please cite as: "Vandercruysse, L., & Christofi, A. (Nov. 30, 2021). Data Protection in the Smart City: Pre-Commercial Procurement as a Silver Bullet? [Conference paper]. *First Interdisciplinary Utrecht University Centre for Public Procurement PhD Forum.*"

[20] **Author contributions** - **Laurens Vandercruysse**: Conceptualization, Methodology, Formal Analysis, Investigation, Visualization, Writing - Original Draft; **Athena Christofi**: Conceptualization, Investigation, Writing - Original Draft; **Caroline Buts**: Validation, Writing - Review & Editing; **Michaël Dooms**: Supervision.

1. Introduction

Numerous cities strive to become smart trough the implementation of smart city services (SCSs). SCSs can be defined as data-intensive, public interest services for which data collection entails the use of sensors (Vandercruysse, Buts & Dooms, 2020). Information technologies (ITs), algorithms and data are leveraged inter alia to improve security, optimize mobility and transport, and render public services more responsive.

However, the implementation of SCSs can also affect the enjoyment of fundamental rights in cities, especially the right to data protection (Charter of Fundamental Rights of the European Union, 2012). There is a need to balance the public interest objectives with the need to protect citizens' rights. European data protection law provides a legal infrastructure that enables such balancing by placing extensive obligations on "*controllers*," i.e. the entities which determine the purposes and means of the processing of personal data, in casu the local authorities. As SCSs often process personal data, data protection law becomes increasingly relevant for smart city development.

SCS development is often costly and highly complex (Edwards, 2016). Since most local authorities lack the expertise to create SCSs in-house (Myeong, Jung & Lee, 2018), services are regularly acquired through formal public procurement procedures. This calls for links between data protection and public procurement laws and practices. Smart city-related public procurement processes need to embed and ensure respect for data protection. Nevertheless, how the desired nexus between procurement and substantive compliance with data protection is to be achieved is far from straightforward.

Most classic public procurement[21] is modeled after a sales relationship whereby a tendering organization acquires a ready-made product or service from a provider (Hoppe & Schmitz, 2013). However, it can be argued that for the procurement of SCSs such a relationship is impractical and even undesirable. Ready-made services might simply not be suitable for public sector use. As guardians of the public interest, local authorities are subject to other demands than the private sector (e.g. accountability, democratic oversight) (Stentoft Arlbjørn & Vagn Freytag, 2012; Ranchordas & Goanta, 2020). The public sector has more robust fundamental rights obligations, and when it comes to data protection, it "*should lead by example*" (European Data Protection Board, 2019). The tension in SCSs between public interest objectives and fundamental rights protection, and the ensuing balancing act, are tasks attributed to the public authorities. A balancing in flux demands a level of flexibility that a contract based on an existing SCS might not offer. In addition, it would be more appropriate to bake this balancing into the service by design rather than retrofit an existing service with a series of values.

[21] In the context of this chapter "Classic public procurement" has to be understood as all procurement of products or services which are available on the market (both in large and in small quantities).

For these reasons, desired data protection might transcend typical private sector offerings available through classic procurement.

At the same time, with an eye on fostering innovation, the EU supports a series of special public procurement procedures that arguably have more potential to ensure high levels of data protection (European Commission, n.d.b). Pre-commercial procurement (PCP), a process enabling the procurement of research and development (R&D), is one such procedure. In theory, PCP should be a good fit for SCS procurement as close involvement of public sector administrators in the service development should prevent the presented mismatches between private sector offerings and public sector needs. This chapter sets out to test this hypothesis, and essentially, to determine the extent to which PCP could contribute to the establishment of smart cities that respect the right to data protection. In view of the proliferation of SCSs and the growing importance of data protection in the EU, the research is highly topical.

The chapter is structured as follows: Section two presents the methodology. Section three addresses the legal fundamentals of data protection in public procurement for SCSs. It explains why in a smart city context it is essential to create links between these two different fields of law and practice. Section four lays out some key challenges in embedding data protection considerations in classic procurement processes, and contrasts these with the theory of PCP. Section five focuses on PCP empirics, discussing the insights gained from the interviews on the potential and limitations of PCP to ensure data protection in SCSs. Section six provides a discussion of useful takeaways for procurement of innovative solutions in general. Section seven concludes.

2. Methodology

The chapter will make use of a case study methodology. The case study is built on semi-structured interviews with procurement and data protection experts working both in the public and the private sectors in Belgium (BE) and the Netherlands (NL). It is important to note that by design, both the working environments and the experience levels of interviewees varied widely. Common methodological guidelines for expert interviews were followed (Bogner, Littig & Menz, 2009).

20 interviews were conducted with experts who have experience with classic procurement of SCSs. Nine experts are active in city administrations (5 BE & 4 NL), one expert is active in a regional administration (1 BE), three experts are from city umbrella organizations (2 BE & 1 NL), and seven experts work in the private sector (6 BE & 1 NL). Also, four interviews concerned PCP of SCSs specifically. Three experts were active in national projects, whereas one was involved in an EU-wide project. These interviews were conducted after the interviews on classic procurement were finalized.

Analysis of this first series of interviews pointed to the PCP as a research area of interest, and insights from the earlier interviews aided in determining the PCP interview questions.

Through combining the insights of the interviews on classic public procurement, on the one hand, and on PCP, on the other hand, two archetypical cases are constructed and subsequently contrasted (Ritala et al., 2013). While this approach is necessarily less concrete than a single case study, we believe the archetypical approach offers the most useful appreciation of the subject. Generalizability of theoretical insights is increased while the analysis is not rendered unduly abstract (Öjehag-Pettersson & Granberg, 2019). General opportunities and pitfalls for local authorities can thus be distilled.

The study is interdisciplinary, combining a legal analysis focused on the EU legal order with a managerial exploration. The value of mixing legal analysis with the management discipline is in the increased practical relevance. Legal notions are confronted with managerial concepts in a way that can offer guidance to various stakeholders.

3. Data protection responsibility in smart cities

As SCSs often process personal data, data protection law codified in the EU in the General Data Protection Regulation (GDPR) is highly relevant for SCSs. The GDPR aims to protect all fundamental rights and freedoms of individuals by laying out rules with regard to the processing of personal data (Regulation (EU) 2016/679 (GDPR), 2016). Such rules are mainly addressed to controllers. It is beyond the scope of the chapter to refer to all GDPR obligations. Rather, we focus on two that well illustrate the legislator's desire to achieve substantive and ex-ante protection of rights, and are thus highly relevant in the smart-city context where multiple rights and interests are at stake and often in conflict: data protection by design and by default (DPbDD), and data protection impact assessment (DPIA).

DPbDD requires controllers to implement "*appropriate technical and organisational measures*" to ensure that data protection principles and all necessary safeguards to meet the GDPR requirements and protect individuals' rights are effectively integrated into the processing, both by design and by default (Regulation (EU) 2016/679 (GDPR), 2016). Guidelines from European data protection authorities provide examples on "*key design and default elements*" enabling respect of data protection principles (European Data Protection Board, 2019). For instance, to respect the lawfulness principle design choices should limit the processing's scope to what is necessary to achieve a specified purpose (European Data Protection Board, 2019). The fairness principle calls for fair algorithms and for mitigating possible biases, as well as informing individuals on algorithmic personal data processing that analyses or makes predictions about their behaviours (European Data Protection Board, 2019). Technical measures, such as hashing and encryption, limit the possibilities to reuse personal data, thereby respecting the purpose limitation principle (European Data Protection Board, 2019). Reliable

datasets and measures that reduce false positives and/or negatives in automated decisions can be necessary to comply with the data accuracy principle (European Data Protection Board, 2019). Overall, DPbDD has been aptly described as "*the technological and organisational hardwiring*" of interests relating to the protection of individuals' rights (Bygrave, 2017).

Where processing "*is likely to result in a high risk to the rights and freedoms of natural persons*," controllers are required to conduct a DPIA (Regulation (EU) 2016/679 (GDPR), 2016). The DPIA is a process meant to function as an early warning system by identifying, analysing and mitigating possible negative consequences of a processing (Kosta, 2020). A DPIA must include a description of the envisaged processing and its purposes; an analysis of its necessity and proportionality; an assessment of the risks to the rights and freedoms of individuals; and, measures envisaged to address the identified risks.

The DPbDD and the DPIA obligations are not about paper-based compliance. They aim to ensure that data protection requirements are considered early on, possible risks (not only to data security but to citizens' rights more broadly) are understood, and decisions that enable compliance are then embedded in the design of a processing operation and throughout its implementation.

In GDPR terms, local authorities in SCSs are often the controllers, or joint-controllers along with other entities, as it is them who set the purposes and means of the public interest-related processing. Since they lack technological know-how and equipment, they contract private entities to provide services and/or products. Nevertheless, the contracting does not absolve local authorities of their responsibilities under data protection law. Recital 78 GDPR clarifies that the principles of DPbDD "*should […] be taken into consideration in the context of public tenders*." DPbDD guidelines from European data protection authorities note that even though all controllers, public and private, have to implement DPbDD, "*public administrations should lead by example*" (European Data Protection Board, 2019). When contracting with software developers, hardware providers, processors and sub-processors, local authorities should thus be mindful that they as controllers are responsible to fulfil DPbDD, conduct DPIAs, and respect all GDPR requirements.

4. Bridging data protection and public procurement

4.1. A void

In view of the above, bridging data protection and public procurement law is highly pertinent for SCSs. Yet, bridges may not be easy to build neither conceptually nor practically. While data protection law aims for substantive protection of citizens' rights, procurement revolves around ensuring transparency, equal treatment and competition among bidders via highly regulated procurement processes. The GDPR acknowledges a link in Recital 78, but not a particularly firm one: The principles

of DPbDD *"should be"* taken into consideration in public tenders, which hardly suggests a categorical obligation. The provision is silent on the weight of these principles in a procurement process vis-à-vis other criteria and interests procurers may want to achieve (Bygrave, 2017). In addition, the day-to-day workings of local authorities make collaboration difficult as procurement officials and data protection officers (DPOs) belong to different organisational units, have different expertise, and may have limited interactions. Even the lack of academic research on the need and feasibility of embedding data protection considerations in procurement processes suggests that fragmentation also exists among scholars, and data protection and public procurement are viewed as markedly distinct fields of scholarship.

4.2. Classic procurement: A tightrope

Existing literature exploring the fundamental rights/ public procurement conundrum is scarce (Mulligan & Bamberger, 2019; Crump, 2016; Brauneis & Goodman, 2018). It concerns the United States (US) legal system and challenges of procuring machine learning systems that respect privacy, equality, good administration principles and public values via classic off-the-shelf procurement. US scholars have noted how government authorities have no influence on the design of these systems, and thus lack the ability to steer and align machine learning systems with public values (Mulligan & Bamberger, 2019). Because of trade secrecy and confidentiality claims raised by private vendors (Brauneis & Goodman, 2018), and/or the lack of algorithmic literacy within public authorities –especially procurement departments-, the latter are often unable to exercise any meaningful oversight. They buy complex systems off-the-shelf as if they were any "*old usual*" product, via a bureaucratic procurement process that values price and fairness in the bidding process, and yet ignores that unlike other products and services, these complex technological systems can impact governance, public values and citizens' rights (Mulligan & Bamberger, 2019).

Arguably, the existence of a comprehensive EU data protection framework that aims to protect various rights makes it harder for public authorities in the EU to renounce their responsibilities by resorting to procurement. Are the abovementioned challenges then irrelevant in the EU context? What other challenges, more specific to the nature of EU public procurement and EU data protection law, can be observed?

To understand current practices we conducted a series of interviews with experts in data protection and classic procurement of SCSs, what follows is a description of an archetypical classic procurement procedure for an SCS in the region.

When a department of a local authority decides to procure an SCS, the dossier is allocated to a public procurement expert (City 8, personal communication, 25/03/2021). This expert then focuses on the

formal legal requirements and the administrative side of the procurement, while the functional needs-based analysis remains the prerogative of the first department (Regional Organization 1, personal communication, 29/03/2021a). Often, time constraints and lack of awareness lead to the non-involvement of subject experts like sustainability experts or DPOs (City 9, personal communication, 16/04/2021). Lack of thematic expertise beyond public procurement from the part of the procurement experts means that data protection requirements are typically limited to the integration of a series of standard GDPR-clauses in the tender documents (City 1, personal communication, 26/05/2020; Company 1, personal communication, 19/06/2020; Company 5, personal communication, 13/07/2020). Bidders are presumed to have read and complied with these clauses at bid submission (City 4, personal communication, 10/06/2020; City 7, personal communication, 5/06/2020). In practice, GDPR thus comes down to checking-the-boxes compliance.

The evaluation criteria of the received bids tend to center on price and core functionality (City 1, personal communication, 26/05/2020). While data protection features might yield bonus points (City 2, personal communication, 4/06/2020), they often do not. Thorough integration of DPOs in the evaluation process of bids is rare because either they are not made aware of the procurement or the data protection department lacks the necessary resources (City 9, personal communication, 22/04/2021; Regional Organization 1, personal communication, 29/03/2021b). Seeing the low flexibility of inherently rigid classic public procurement, local authorities are to abide by a strict timeline as well. Evaluation periods are necessarily restricted. Even when DPOs are involved, bidders are wary to offer access to proprietary information to a mere potential buyer (City 3, personal communication, 8/06/2020; City 4, personal communication, 10/06/2020). An additional difficulty presents itself in several markets for SCSs that are characterized by low competition. In procurement procedures where only two or three bids are received, the local authority's choice of action is regularly reduced to accepting a non-ideal solution, also with regard to data protection, or having a failed public procurement process (City 3, personal communication, 8/06/2020; City 5, personal communication, 3/07/2020).

The contract conclusion with the winning bidder follows the evaluation stage. Regarding data protection, the contract includes a repetition of the standard GDPR-clauses in the tender as well as a standard non-tailored data processing agreement as an annex (City 2, personal communication, 4/06/2020; City 6, personal communication, 21/08/2020; Company 3, personal communication, 2/07/2020).

The sketched case effectively backloads all data protection considerations, in stark contrast to the spirit of the GDPR. Vendors' compliance statements with data protection law are accepted without much –

or any– scrutiny. Obligations preoccupied with substantive and ex-ante protection, such as DPbDD and DPIAs become extremely difficult to meet in this classic procurement setting. Since data protection has not been thoroughly addressed during the procurement procedure, it has a propensity to come up only once problems arise, e.g. data breaches or data protection authority investigations (City 5, personal communication, 3/07/2020; City 8, personal communication, 20/05/2021). Furthermore, as local authorities are adamant about remaining the "*owner*" of the data collected in the public space (City 2, personal communication, 4/06/2020; City 4, personal communication, 10/06/2020; City 7, personal communication, 5/06/2020; City Organization 1, personal communication, 29/05/2020), they regularly demand controllership. With an eye on the DPIA, which is the responsibility of the (joint) controller(s), this situation is problematic in the sense that local authorities might not dispose of all required information to effectively conduct a DPIA and the private partner might at this stage lack the incentives to aid in the process (City Organization 3, personal communication, 10/07/2020).

From the above, it is clear that the archetypical case of classic procurement is problematic for diligent data protection in smart cities. The next section outlines the theoretical benefits that the PCP can offer.

4.3. PCP in theory: A bridge

To strategically support public sector innovation the EU has provided support to various new procurement procedures, among which PCP. In short, PCP concerns the procurement of R&D services (Commission of the European Communities, 2007). PCP is exempted from the EU directives on public procurement and the extensive regulation of procurement processes that these contain (Directive 2014/24 (EU), 2014). This exemption makes it a low-bureaucracy, flexible process, whereby public authorities can co-create novel services together with various private partners (European Commission, n.d.c). The procedure consists of three phases: i) a design phase, ii) a prototyping phase, and iii) a test phase (European Commission, n.d.c). A PCP starts off with a number of private partners, and after each consecutive step the least suitable candidates are dropped. It is thus a competitive process. PCP stops short of the large production of the novel service, but shares R&D risk with the private partners – private partners receive an amount of public funding in a staggered manner to complete the three steps (Iossa, Biagi & Valbonesi, 2018). The co-creation process allows for steering as well as flexibility and knowledge sharing.

The high level of innovation that SCSs should entail is what brings PCP and smart cities closer. Innovative solutions to urban challenges often do not exist already, or need to be tested and proven in the urban context. As local authorities need to invest in ideas that are still subject to R&D, there is ample ground to use the PCP process in a smart city context.

Theoretically, PCP could offer a series of advantages regarding data protection in SCSs compared to classic procurement. First, public sector involvement in the R&D phase of SCS development should assure a level of access and impact that is impossible through classic procurement. PCP allows insights into the inner workings, and thus also data protection philosophy, of the private organizations. Contacts between a variety of employees and collaborators of the contracting authority and the tenderers highlight commonalities and differences (Brogaard, 2017). In addition, public administrators can steer the private sector partners through dialogue or through setting certain evaluation criteria for the various PCP stages (Iossa, Biagi & Valbonesi, 2018). This is an advantage in terms of data protection in the sense that there is a strong argument that data protection can for a large part be safeguarded through system design (Romanou, 2018), a reasoning that is endorsed in the GDPR, and obligations such as DPbDD and DPIA discussed in Section three.

Second, R&D demands interdisciplinary involvement from the very beginning. Where classic public procurement often suffers from a silo mentality, due to the seeming emphasis on the formalistic complexity of public sector buying (Kristensen, Mosgaard & Remmen, 2021), the emphasis of the PCP remains on the level of the desired service (Edquist & Zabala-Iturriagagoitia, 2015). A service-centered approach more easily lends itself to a broad involvement of specialties. In many ways, collaboration between silos is a crucial necessity for successful PCP (Brogaard, 2017). Consequently, it is not an option to overlook certain auxiliary functions within the organization, e.g. data protection officers. The PCP thus fosters horizontal intra-organizational collaboration.

Third, the PCP does not entail an obligation to procure the winning service at the end of the procedure (Delina, Gróf & Dráb, 2021). In that sense, the procedure allows for non-committal testing and an extensive review and evaluation phase (European Commission, 2016). This cooling-off period has the advantage that it allows for public administrators to look at the process with some distance before a final deployment decision is made (Iossa, Biagi & Valbonesi, 2018). It follows that separating the R&D and deployment phases should lead to better thought-out data protection strategy as well. At the end of the PCP the tendering organization is free to use the acquired insights in any desired fashion for the set-up of a tender (barring intellectual property), key learnings can then be translated into formal requirements or evaluation criteria.

5. PCP in practice: A bridge indeed?

Aiming to go beyond the theoretical, this section zooms in on the implementation of the PCP. The aim of this empirical investigation, consisting of an analysis of four interviews with experts having experience in PCPs, is to determine to what extent the abovementioned advantages hold up in

practice. Confronting theory with practical experience allows for distillation of concrete best practices and pitfalls.

Interviewees indeed pointed to the theoretical benefits of PCP outlined above as important opportunities for data protection. First, early involvement in the service/ product development process provides extensive potential for tailoring the desired product/service (PCP Expert 2, personal communication, 29/07/2021), as well as a level of access to private partners' inner workings that is unattainable in classic procurement (PCP Expert 1, personal communication, 27/07/2021). Second, PCP was propagated as a "*change management tool*" (PCP Expert 4, personal communication, 3/08/2021). Public administrations are mentioned to work in a siloed way, i.e. cross-departmental communication and collaboration are rare (PCP Expert 4, personal communication, 3/08/2021). As the PCP process forces interdisciplinary teams to be set up, it offers a good opportunity for fostering data protection awareness and close DPO-involvement throughout the specific PCP process, but also beyond the particular PCP (PCP Expert 1, personal communication, 27/07/2021; PCP Expert 4, personal communication, 3/08/2021). Third, the fact that the PCP includes a testing phase disconnected from a purchase obligation leaves room for testing and low-risk failure. It is emphasized that PCP concerns R&D explicitly excluding final deployment, by consequence data protection learning can be evaluated and integrated in any follow-up tender (PCP Expert 1, personal communication, 27/07/2021; PCP Expert 2, personal communication, 29/07/2021).

Key factors for successful data protection in PCP can be broken down into PCP process preconditions, on the one hand, and specific data protection elements, on the other hand.

PCP process preconditions do not have a direct effect on data protection levels, but they ensure that a climate is created which allows data protection to be tackled at all. First, it needs to be clear why the PCP process for an SCS is commenced – "*innovation for the sake of innovation is really counterproductive*" (PCP Expert 1, personal communication, 27/07/2021). This entails: analyzing the current procurement practices, analyzing the current public service that the SCS is aimed to replace, and analyzing the public organization (PCP Expert 1, personal communication, 27/07/2021; PCP Expert 4, personal communication, 3/08/2021). Understanding the laws and regulations of the sector the PCP is dealing with before the drafting of the tender documents is also crucial for the PCP (PCP Expert 1, personal communication, 27/07/2021). It is as part of this legal requirements analysis that data protection may often emerge in SCS projects, and accorded the necessary importance within the PCP. To properly analyze all these aspects, there is a need for an interdisciplinary team (PCP Expert 1, personal communication, 27/07/2021; PCP Expert 3, personal communication, 3/08/2021). Where a lack of in-house (evaluation) expertise is identified, external experts need to be consulted (PCP Expert

2, personal communication, 29/07/2021; PCP Expert 4, personal communication, 3/08/2021). Second, PCP demands a clear predefined strategy (PCP Expert 3, personal communication, 3/08/2021). As the procurement workflow is reversed in PCP, i.e. requirements are predefined and adapted as the process proceeds in contrast to a catalogue of final products being evaluated, there is a need to induce a mindset shift within the public organization (PCP Expert 4, personal communication, 3/08/2021). PCP being a sui generis procurement procedure comes with a set of particularities that need to be taken into account. There is a strong need for expectation management (PCP Expert 3, personal communication, 3/08/2021): the process concerns R&D and not final deployment (PCP Expert 1, personal communication, 27/07/2021), there are no guarantees for success (PCP Expert 4, personal communication, 3/08/2021), the process is comparatively quite time intensive (PCP Expert 3, personal communication, 3/08/2021), and the process is comparatively very complex (PCP Expert 2, personal communication, 29/07/2021). In view of the potential for intra- as well as inter-organizational expectation mismatches and the level of risky upfront investment, top-level management support is crucial (PCP Expert 4, personal communication, 3/08/2021).

Turning to specific data protection success factors, it is important to differentiate between: a need for a data protection strategy, a need for technology push management, and a need for flexibility.

Having a carefully considered data protection strategy is a necessary requirement for diligent data protection, arguably more so when the environment in which the strategy is to be applied is more complex. Interviewees mentioned that complexity of the PCP process itself has in practice led to complexities related to data protection in the service under design remaining unaddressed: as one interviewee recalled, it was not possible to put more emphasis on privacy "*because everything else was already so complicated*" (PCP Expert 3, personal communication, 3/08/2021). Therefore, it is key that data protection is top-of-mind of both top-level management and PCP project management (PCP Expert 1, personal communication, 27/07/2021; PCP Expert 3, personal communication, 3/08/2021). In addition, the strategy should include raising data protection awareness throughout the public organization. Completing a PCP demands involvement of a plethora of subject experts, for a data protection strategy to be implemented effectively all involved should at least be aware of the basics (PCP Expert 4, personal communication, 3/08/2021). Related, there is a need for breaking down the discipline silos that have formed inside the public organization (PCP Expert 4, personal communication, 3/08/2021). PCP fosters but also demands horizontal intra-organizational collaboration from the very beginning (PCP Expert 1, personal communication, 27/07/2021). Broad data protection awareness is good, but that also entails that for more complex issues collaborators need to involve data protection experts/ DPOs.

DPOs involvement should be continuous throughout the PCP, and start from a very early stage (pre-publication of the tender documents) to the evaluation and negotiations with private partners (PCP Expert 4, personal communication, 3/08/2021). Compliance with even complex GDPR obligations, such as DPbDD and DPIAs then becomes truly possible. As one interviewee explained, the beauty of the PCP is that DPOs and vendors have a very close working relationship during the execution of the phases. So already in the design study they can challenge the vendors, by asking questions on the possible risks of the designed solutions and the measures to be taken to tackle those (PCP Expert 1, personal communication, 27/07/2021). Even though often, a formal DPIA can only be conducted during the final PCP phase, it is important to look into data protection and risks much earlier on: otherwise it can "*cost you too much time, too much money, and it's not going to work*" (PCP Expert 1, personal communication, 27/07/2021).

PCP entails close collaboration between public and private sector actors (PCP Expert 1, personal communication, 27/07/2021). Often SCSs are procured rather than developed in-house because public organizations lack the necessary technological know-how. However, it is important that the necessary expertise to evaluate SCSs is present on the side of the public organization, in particular in the context of PCP (PCP Expert 3, personal communication, 3/08/2021). One interviewee put it strikingly as:

> "*If you do a PCP, you need to understand that you need to be a counterpart for the technology vendors on the technology stuff*" (PCP Expert 1, personal communication, 27/07/2021).

The necessity of having public sector expertise stems from a need to preserve a level of independence vis-à-vis the private sector. If public organizations were to trust blindly private PCP competitors' information, it is clear they are susceptible to misinformation and manipulation. In short, there is a need to manage the technology push. Interviewees again pointed to the essential prerequisite of having a multidisciplinary team (PCP Expert 4, personal communication, 3/08/2021), especially in the evaluations that take place at the end of every PCP phase (PCP Expert 3, personal communication, 3/08/2021). In case the necessary expertise is not available in-house, external experts should be involved (PCP Expert 1, personal communication, 27/07/2021). Interviewees implicitly underscored the relevance of hiring external expertise:

> "*It's the companies that are really the specialists on how to make sure that these [data protection] questions can be answered and that the data is protected. The specialists will probably not be in the public entities*" (PCP Expert 2, personal communication, 29/07/2021).

Additionally, there is a considerable need for flexibility and a solution-oriented approach throughout. Inevitably this then entails a change of mind-set, not only in procurement departments but also in thematic experts, such as DPOs. While DPOs are seemingly used to examine solutions, approving or

sanctioning them, they now have the chance –and challenge- of working together with colleagues and private partners, and participating in the solution:

> *"… now [the DPO] should say upfront how [he or she] will judge [the SCS], how [he or she will] compare those [data protection features]. That is a completely different mindset"* (PCP Expert 4, personal communication, 3/08/2021).

Seeing inherent PCP features, collaborators should be comfortable working with an abstract idea of data protection (PCP Expert 4, personal communication, 3/08/2021). An abstract idea would then mean one based on central GDPR principles as opposed to on the technical and practical. As only in the test phase physical end products are evaluated, in the previous phases evaluations concern plans and works-in-progress. Consequently, any data protection approach would follow a funnel-system (PCP Expert 4, personal communication, 3/08/2021), i.e. requirements and recommendations would only become more specific as the PCP moves through the different stages. Also, as PCP is an open process in which the emphasis is on the sought solution rather than the technology used, proposed alternatives might not be easily comparable (PCP Expert 1, personal communication, 27/07/2021; PCP Expert 3, personal communication, 3/08/2021). This holds true in general as well as specifically with regard to data protection. Herein also lies a pitfall in the sense that this opens up the possibility for eliminated PCP participants to make the case that the terms for competition were not fair and open (PCP Expert 2, personal communication, 29/07/2021), a considerable legal risk.

While it was possible to distill certain best practices from the interviews, the latter have also revealed significant challenges in embedding meaningful data protection in PCP. This is especially true when it comes to complex requirements such as DPIA and DPbDD. For instance, an interviewee attested that when discussing the need to conduct a Privacy Impact Assessment in a PCP project,[22] complex questions emerged as to who and how would do such assessment: the tenderers or the contracting authorities?

> "*Practically, procedurally, it was difficult to say how this could be done in a really good and proper way, and so it was not done"* (PCP Expert 3, personal communication, 3/08/2021).

Even where privacy and data protection are a main preoccupation in a PCP project, setting the right selection/ evaluation criteria is still a learning process, with an interviewee admitting that "*we will just have to see how it works*" (PCP Expert 4, personal communication, 3/08/2021). The technical review of proposals - which closely links to the DPbDD obligation - is regarded particularly challenging (PCP

[22] Privacy Impact Assessments (PIAs) are essentially the predecessors of DPIAs. Experts have sometimes used the terms "*PIA"* and "*DPIA"*, or "*privacy"* and "*data protection"* interchangeably.

Expert 4, personal communication, 3/08/2021). If private vendors offer something very technical, and something very different from one another, the contracting authority can only hope (rather than be confident) that it will be possible to properly evaluate solutions.

Finally, an interesting message is the belief that PCP is a "*regulatory sandbox"* (PCP Expert 1, personal communication, 27/07/2021), or a "*learning process*" (PCP Expert 4, personal communication, 3/08/2021). For SCS projects, a significant aspect of such experimentation concerns data protection, and the limits that data protection law places vis-à-vis ever-ambitious and innovative technologies. The dilemma local authorities may be called to face when developing innovative projects has broadly been described by an interviewee as follows:

> "*For privacy, [you can say] two things: 'it's a complex privacy issue, so we don't do this [project]'; or, 'it's a complex privacy issue, so we are going to test it and do innovation projects to see what is possible and also of course what is not possible'"* (PCP Expert 4, personal communication, 3/08/2021).

PCP arguably gives local authorities more leverage to opt for the second - often more challenging - choice. For SCSs, where privacy and data protection need to be finely balanced with public interest objectives, this possibility to experiment and learn can be particularly valuable.

Table 31 summarizes in a schematic way how the practice of PCP compares to its theory as well as how it compares to classic procurement, in essence the table constitutes the succinct review of Section four and Section five.

Practice	**Theory**	**Practice**
Classic procurement	**PCP**	**PCP**
Focus on formal legal public procurement requirements • Time constraints • Lack of awareness	Focus on R&D and service requirements a.o. data protection	Yes, but need to: • Map status quo • Define process strategy • Have top-level support
Limited involvement of data protection experts • Non-tailored GDPR-clauses in tender • Standard data processing agreement in annex	Early involvement in of data protection experts in multidisciplinary team • Co-creation and steering • Deep access	Yes, but need to: • Define data protection strategy, incl. evaluation • Have flexible, principle-based understanding of data protection • Manage technology push
Outright purchase of solution	Test phase of solution followed by cooling off period	
Backload data protection considerations	Frontload data protection considerations	
Enable 'tick the box' data protection compliance	Enable substantive data protection	Potentially enable substantive data protection

Table 31. Schematic overview of Section four and Section five.

6. Discussion

While our findings primarily underline the potential value for smart city data protection of procurement by PCP specifically, managerial implications can be derived that could hold more broadly. This is important for two reasons. In the first place, it should be noted that PCPs currently only constitute a small part of all tenders in the EU (OpenTender.eu, n.d.). Also, the format of the PCP might not be suitable for the procurement of more mundane SCSs.

There are three central managerial takeaways: (i) reconciliation of public procurement and data protection demands active effort, (ii) procurement process management influences data protection outcomes, and (iii) broad as well as deep data protection awareness is crucial.

First, it cannot be assumed that strictly abiding by the formalistic legal and administrative approach of tender issuance, will lead to procurement of SCSs that thoroughly respect the fundamental right to data protection of city dwellers. The inclusion of standard GDPR-clauses and non-tailored data processing agreements enables tick-the-box compliance, especially in view of a lack of monitoring, and complicates substantive data protection. The procurement practice in general would benefit from closer involvement of thematic experts, and the establishment of multidisciplinary SCS- or IT-procurement working groups.

Second, process management matters. Having a clear line of command – e.g. in terms of determining the why and how of the procurement –, following a sound process strategy, and having management support arguably render comprehensively tending to data protection more attainable. As PCP is a relatively more complex procurement procedure, the effects might be more pronounced in that context, but arguably this holds true in general as well.

Last, in any case substantive data protection will demand a broader intra-organizational data protection awareness, including but not limited to the public procurement department, and an influx of data protection expertise. Awareness throughout the organization aids in timely signaling potential issues or points of interest, and also leads to administrators knowing when the involvement of thematic experts is desirable. Furthermore, most local authorities also require a considerable influx of data protection expertise to be able to objectively evaluate SCS-tender features. Whether that expertise should be available in-house or external consultants can be relied upon, can be evaluated on a case-by-case basis, but the interviews demonstrated that a lack of data protection resources is an inhibiting factor. Moreover, the inability to independently audit SCSs can endanger the protection of public values in a broad sense.

It can be concluded that PCP offers a potential for substantive data protection over and above what classic procurement currently provides. But by no means do we argue that local authorities should employ PCP for the sole end of upgrading data protection levels. However, best practices of successful PCPs can, and should, inform the classic procurement practice. To that end, this chapter gave guidance on how to make the most of the specific data protection opportunities that PCP offers in the event such a procedure is launched, and distilled more general managerial takeaways that can offer key learnings for classic procurement.

7. Conclusion

This chapter explored the extent to which PCP can facilitate and ultimately improve data protection in SCSs, especially when contrasted with classic procurement processes. Combining insights from the literature and empirical research consisting of expert interviews, it has outlined the challenges of embedding data protection considerations in classic procurement on the one hand, and the potential advantages of the PCP process to ensure more robust data protection in SCSs on the other hand.

We conclude that resorting to PCP is not a sufficient condition for achieving a more elevated level of data protection in SCSs than through classic procurement. Difficulties need to be managed both on a strategic process level as well as specifically related to data protection. Nonetheless, if managed correctly, theoretical PCP benefits vis-à-vis classic procurement can hold up in practice. It is important to note that PCP might not be the appropriate procedure for a range of SCSs, however key learnings from past successful PCPs can inform and reinforce data protection approaches in classic procurement.

Chapter 9. Conclusion

The collection of research articles contained in this dissertation investigates smart city data protection from an economic and managerial perspective. Adding to a body of literature largely formed by technology and legal scholars, the work demonstrated the importance of multi- and interdisciplinary research to grasp contemporary issues in a holistic manner. In addition, it highlighted the potential of using business and economics insights to formulate concrete interventions that might aid in attaining technological or compliance objectives.

Constituting the end of the dissertation, this concluding chapter brings together the various individual chapters. It sequentially recapitulates key findings, summarizes theoretical contributions, highlights practical implications, addresses limitations, and suggests avenues for further research.

1. Key findings

Chapter 2 produced a typology of SCSs based on DPIA-costs. A series of nine interviews with experts active in the Flemish smart city, demonstrated that costs of a DPIA vary along eight factors: i) city size, ii) diversity of urban stakeholders, iii) total of SCSs in the urban region, iv) number of different data streams, v) clarity of data controllership, vi) amount of use-cases, vii) privacy invasiveness, and viii) visibility of the SCS. These factors can be considered distinct layers of two prime complexities underlying DPIA-cost variations, i.e. the urban environment in which an SCS is provided and the SCS itself.

Chapter 3 showed that three SCS data controllership set-ups are potentially problematic for DPIA-obligation compliance and diligent data protection. In particular, these set-ups are: a joint data controller taking the role of data processor, joint data controllership, and a data controller outsourcing processing to a data processor. Problems spring from a tendency to avoid data protection responsibilities, a lack of information sharing, and a deficiency of data protection literacy among smart city actors. Data processing and joint controller agreements outlining information provision obligations could be integrated in SCS tenders, and data protection awareness, both internally and externally, should be raised, to somewhat alleviate the identified problems.

Chapter 4 mapped the various stakeholder interests to be balanced in the context of a DPIA on an SCS. For this exercise, following A29WP guidance, five stakeholder groups were taken into account, namely (joint) data controllers, data (sub-)processors, specialized consultants/ researchers, citizens, and data protection authorities. The completion of 16 data protection expert interviews led to the identification of eleven distinct interests spanning four themes: i) compliance, ii) cost control, iii) data management, iv) efficiency, v) generation of trust, vi) income acquisition, vii) limiting impact on service performance, viii) reputation building, ix) risk management, x) safeguarding competition, and xi) safeguarding data

security. The AHP method revealed that the generation of trust, risk management, and data security feature most prominently during the DPIA.

Chapter 5 investigated the role of hardware and technology providers in the DPIA. It was shown that although this stakeholder group is often overlooked in guidelines by regulators as well as in literature, there are considerable advantages that spring from their more extensive DPIA-involvement. In particular, requiring hardware and technology providers to prepare a generic DPIA based on technical SCS aspects could force a responsibilisation on the stakeholder group in terms of taking ownership of privacy-by-design and privacy-by-default. Additionally, the avoidance of unnecessary duplication of data protection costs downstream and the scope for uniformization of data protection risks provided further economic benefits.

Chapter 6 focused on the (lack of) competitive effects of the practical elaboration of the EU Digital Strategy on the market for SCSs. Seeing the proposed large size-related cutoffs to be eligible for gatekeeper status under the DMA and the largely facultative nature of the DGA, a more proactive approach with regard to safeguarding competition by public procurement requirement setting would add value. Building on insights gathered through 19 expert interviews, it was suggested to embed tailored data protection clauses, i.e. require the submission of a data protection report and the signature of an SCS-specific data processing agreement, as well as data sharing requirements in SCS tenders.

Chapter 7 zoomed in on data protection related ex-ante transaction costs borne by bidders in the context of public procurement of SCSs. An empirical study of 72 SCS tender bids showed that these particular costs amount to between 4 % and 5 % of the total tender value. Furthermore, the cost level positively correlated with the strength of the relationship with the tendering authority, i.e. there was a tendency to invest more in data protection when a good relationship between tender issuer and tenderer existed. However, it did not correlate significantly with the probability of winning a tender for an SCS. Additionally, increased competition in the form of a higher number of bidders for an SCS tender did not affect ex-ante data protection investment levels.

Chapter 8 highlighted that the theoretical data protection governance benefits of PCP in comparison with traditional procurement can indeed occur in practice. Concretely these benefits concerned: the opportunity to frontload data protection due to co-creation inherent to the PCP process, the possibility to use the PCP as a lever to transcend departmental silos for the purposes of data protection, and the freedom to utilize the third phase of the PCP purely as a test phase before integrating data protection insights into a tender for final deployment. However, a list of important necessary conditions was identified as well. First, a clear strategy both regarding the PCP as well as data protection needs to be

formulated. Second, there is need for extensive technical and data protection expertise in the public sector, either internal or external, to manage the technology push. Last, it is important that there is awareness concerning the particularities of PCP, particularly the need for flexibility.

2. Theoretical contributions

As a scholarly work, the dissertation set out to make a series of contributions to theory. It can be concluded that there are four overarching theoretical contributions.

Theoretical contribution 1: DPIA and issue-focused stakeholder management.

Comprising a few of the earlier works on the DPIA in smart cities, this dissertation aids in grounding theory in practice, and adjusting relevant theoretical lenses. Chapter 2 builds a conceptual model on the topic of DPIA-cost variation. In essence, the model offers a lever for (non-)economists and (non-)data protection experts to effectively communicate on DPIAs, and data protection risks more broadly. The various theories underlying data protection impact, and related mitigation costs, were derived from the literature and subsequently refined to suit the context of SCSs. Also, Chapter 4 offers a contribution to the field of issue-focused stakeholder management (Roloff, 2008). First, we derived a role-based stakeholder framework suitable to analyze data interactions at the base level. This is significant since any actor-based framework necessarily overlooks intricacies with regard to the data (protection) layer of smart cities. Second, we built theory, and offered empirics, on data protection interests beyond the traditional duality between private sector and public sector as in e.g. Galic & Schuilenburg (2020). The result is a more nuanced picture on which more accurate theory can be constructed. Third, we offered a baseline on the balancing of various interests in the DPIA on SCSs. This finding can be a steppingstone for more dynamic stakeholder research.

Theoretical contribution 2: Data protection and public procurement of innovation.

Chapter 6 and Chapter 8 constitute additions to theory on public procurement of innovation. Both chapters refine views on procurement processes involving SCSs in particular, as well as innovation in general, in the sense that data governance success factors are mapped. Moreover, important limitations concerning the potential of innovation procurement emerging from managerial or economic dynamics are pinpointed. The integration of these insights into theory could aid in research on congruence between high-level policy goals and procurement processes (Ranchordas & Goanta, 2020), cfr. green procurement.

Theoretical contribution 3: Data protection and competition.

The chapters on competition add to the emerging literature on the nexus of competition and data protection. In particular, we add to the ideas that data is a key asset – not just an input – in the new

economy (Gal & Aviv, 2020), and that data control in essence offers a type of horizontal power (Kerber, 2019), i.e. data collected in one market can be equally valuable in other markets. We pinpoint the managerial and economic dynamics producing sustainable market power from data in the market for SCSs specifically, but we are confident that these dynamics hold more broadly. By squarely embedding the concept of data controllership into the discussion on the management and economics, the combination of the various chapters forms a much-needed bridge between the disciplines of law and data economics. Moreover, on the topic of data protection, this dissertation produces notable avenues for theory building. In contrast to the legal works following the doctrinal tradition of the legal discipline, this work performs a true deep-dive into the realities on the ground. Especially with regard to the study of data protection law compliance and incentive management, the chapters offer novel insights.

Theoretical contribution 4: Data protection and transaction cost economics.

Building on the seminal works by Coase (1937) and Williamson (1975), we made use of the transaction cost economics lense in Chapter 7. As the first application of this theoretical framework to the realm of data protection, we extended its range by finetuning the operationalization by De Schepper, Haezendonck, and Dooms (2015). In addition, even though explorative in nature, we performed an empirical analysis which suggests high potential pertinence of the framework with an eye on explaining data protection outcomes.

3. Practical implications

The research results in the various chapters of this dissertation can also be combined into a number of takeaways for practice and policy.

Takeaway 1: broad data protection literacy is a crucial success factor for sustainable smart city development.

In line with extant literature, this dissertation found that citizen trust is the prime concern of most smart city actors (Khan et al., 2017; Yeh, 2017). An AHP demonstrated that even in the specific context of the DPIA, generation of trust outranked risk management and data security as most important stakeholder interest. It is reasonable to assume that active generation of trust forms part of an organization's communication/ participation efforts. Evidently, the DPO does not usually form part of the communication/ participation department. To correctly identify data protection matters of interest and to communicate clearly and comprehensively on the subject, a certain level of data protection literacy of communication department staff is primordial. More generally, in principle any interaction with a citizen can necessitate a referral to the DPO. The ability to timely gather the necessary information and to make a succinct risk assessment will further demonstrate seriousness with regard to data protection matters and transmit trust to the public. In the form of an adage, one

could say: “It is an organization-wide effort to build trust, but it only takes a single person to destroy it.”

The above also holds for contact between organizations. The problems that were identified regarding three specific data controllership set-ups for SCS were in hindsight indeed a symptom of a wider issue concerning low data protection literacy. Data protection discussions are often backloaded because of lack of knowledge and awareness, and tend to impose themselves when problems arise. Problem-based ad-hoc retrofitted data protection arrangements are detrimental to the public image of all actors involved but also to inter-organizational trust levels. Clearly outlining data protection aspects in the tender and discussing potential functional implications with project managers, or, alternatively, making data protection part of the co-creation effort in for example a PCP process, can keep the scope for unpleasant surprises to a minimum.

If a smart city is to develop in a manner that is sustainable, garnering trust will be key. Making sure administrators are well-informed, and informing the public and partners in a clear way, are important drivers to that end.

Takeaway 2: the DPIA process holds the potential to be a powerful lever for smart city data protection, if managed correctly.

It cannot be assumed that all actors will take up their tasks regarding the DPIA as laid out in the GDPR. Including tailored clauses in tender documents could offer an additional big stick. Data processors can be asked to provide a data protection report, including a generic DPIA outlining technical risks, while (joint) data controllers can be asked to sign tailored joint controller agreements at bid submission. Assuming good agreements do indeed make good friends, clear lines of control and responsibility should induce partners to do their part. And, if not, with an eye on nullifying the SCS contract, the non-compliance with tender requirements might be easier and quicker to establish than non-compliance with the GDPR.

Furthermore, it was found that DPIAs can vary widely in terms of costs and as regards methodological emphasis. Therefore, it is important to manage expectations. A DPIA on a city-wide camera shield will demand more resources than a DPIA on a more mundane data processing operation. In the same vein, a DPIA in which many actors with differing interests are involved will likely be more challenging than a DPIA on a strictly internal processing. In any case, allocated time and resources should be adapted accordingly.

As a collaborative exercise, the DPIA accords well with the spirit of co-creation underlying PCP. This dissertation showed that PCP can foster substantive data protection through a.o. breaking down

departmental silos. It could prove beneficial for the public sector to employ PCP as a change management tool: by learning to transcend departmental and organizational borders in the particular context of a project, this might indeed open the door to do it more regularly.

In conclusion, Article 35 of the GDPR presents an opportunity. Embedding the balancing of public interest pursuit and safeguarding of rights and freedoms of individuals in the general procedure for introducing a "*high risk*" data processing operation, makes sure data protection is at least reflected upon. However, whether the DPIA will decay into a merely administrative procedure or become a strong precedent for a new genus of fundamental rights protection measures, depends largely on process management and on the stakeholders involved. Even more so, since GDPR enforcement is rather slow (Satariano, 2020; Stolton, 2020).

Takeaway 3: the fundamental right to data protection merits safeguarding but the legal instruments that constitute its practical translation likely require pro-competitive flanking measures. Regulation of data protection might thus hurt competition.

Concretely, it was demonstrated that the introduction of the GDPR has the potential to substantially affect competition in public procurement of SCSs. Gathered empirics suggest that its introduction raised data protection-related ex-ante transaction costs to a level that is at 4 % to 5 % of total tender value on average. To make matters worse, it was shown that the data protection investments made up to tender submission are not a significant factor in tender award processes.

Therefore, likely a number of tenderers exited the SCS market, or did not enter it, in the aftermath of GDPR introduction, and the remaining tenderers are faced with considerable additional costs with which no real competitive advantage can be gained. Arguably, such a situation will foster tick-the-box compliance, if not a race to the bottom, over the longer term, as there are no direct financial incentives to go beyond. The introduction of a regulation to safeguard data protection might hence end up worsening data protection levels, not unlike how a tightening of safety management rules for maritime transportation led to an increase in ship accidents in Norway (Størkersen, Antonsen & Kongsvik, 2017).

To avoid that the SCS market structure evolves towards that of online search engines or social media (Lynskey, 2019), it is important to boost competition on data protection levels. In essence, this will demand efforts on two fronts: stimulating competition in general, and turning data protection levels into a competitive field of interest for SCSPs.

With an eye on encouraging competition in digital markets, the DMA and DGA proposals are steps in the right direction. However, the European Commission initiatives still focus mostly on rectifying rather than preventing problems. Elevated cutoffs in terms of revenue largely preclude private actors

acquiring dominance in non-mature markets, such as the SCS market, from being subject to DMA gatekeeper obligations (European Commission, 2020b). Also, the DGA is mostly concerned with voluntary data sharing (European Commission, 2020c). This dissertation proposed a shift towards a more ex-ante approach by embedding data sharing requirements as hard conditions in SCS tender documents and by propagating a data protection strategy which requires public sector data controllership over all SCS data.

Rendering data protection levels an important competitive factor in SCS tenders will demand a large influx of data (protection) expertise in the public sector. This dissertation has shown that by most standards data protection knowledge and maturity in Belgian (local) public authorities is relatively low on average. To effectively convey to SCSPs that the public sector is serious about data protection, and to consequently induce a shift in mindset (and actions) on the part of SCSPs, it is a necessary condition that public administrators are able to assess data protection aspects of SCSs both on a legal and on a technical level. Data protection assessment can be made more graspable through measures such as demanding a data protection report in a desired template format and/ or requiring the submission of a generic DPIA by hardware and technology providers. However, the public sector should be able to independently verify the veracity of the data protection claims made. Whether it is practically feasible and desirable to demand individual (local) public authorities to set up their own data (protection) teams, or it is preferred that a more central authority, e.g. a city umbrella organization or a branch of the DPA, take on a larger role, remains an open question.

4. Limitations

The limitations of this dissertation can be divided along methodological lines. Concerning the qualitative investigations, limited data can be considered a caveat for generalization. The innovative nature of the research subject naturally leads to a compact target group of potential interviewees, i.e. the GDPR has entered into applicability on 25. May 2018 while smart city transitions in many respects are still in their early stages. Also, the limited maturity with regard to data (protection) of both public and private actors in the region under investigation complicates compiling a large interview set. However, this lack of maturity constitutes a finding in itself. In addition, the limitation of the geographical scope to Belgium and the Netherlands constitutes a strength as well as a weakness. This dissertation provides a more in-depth look at the SCS market in the two countries, but as such somewhat foregoes an EU-wide analysis. Throughout the research it became clear that Flanders, Belgium as a whole, and the Netherlands, are plagued by similar challenges. This allowed us to confidently enlarge the region under investigation without losing too much context-dependent depth related to the analyses. It should be noted that the findings can most confidently be generalized to Belgium and the Netherlands, but the explorative nature of various research designs point to the need

for cautious interpretation. The geographical focus of chapters also varies as a result of the challenges related to the search for suitable interview subjects. Initially, expertise on smart city data protection was scarcer, and potential respondents were weary of being involved in the research process. As awareness grew, absolute response numbers improved, allowing for broader and deeper investigation.

With regard to the quantitative studies, the lack of an SCSP directory at EU level, and often at national level, complicated the search for survey respondents. Nonetheless, during the course of the research contained in this dissertation, a proprietary database containing over 1 200 SCSPs was compiled. The limited response rate can mostly be attributed to the low data (protection) maturity and lack of awareness among smart city actors. Contrary to the approach of the qualitative research, it was opted to enlarge the geographical scope to include the whole of the EU. Especially the specific nature of the transaction cost survey in terms of required width of expertise of respondents, demanded such enlargement. It should be noted that the investigation contained in this dissertation is the first of its kind, and its aims are explorative. Though there is thus not a perfect match with the geographic scope of the qualitative analyses, it can still suggest points of attention, and provide a steppingstone for more regionally focused research.

5. Avenues for further research

This dissertation contributes to the literature on the economics of data protection in smart cities, nonetheless several questions remain unanswered. This chapter ends with some ideas for further research.

A first set of proposals concerns DPIA-research in particular. The typology of SCSs included in this dissertation is based on relative DPIA-costs. However, the research leaves absolute costs largely unexplored. Shedding light in concrete cost levels could aid smart city actors in rationalizing data protection efforts. Moreover, the evolution of DPIA-cost variations over time could allow us to draw inferences concerning the equilibrium state of the DPIA as an instrument, i.e. mere administrative hurdle or in-depth fundamental rights analysis.

Also, further research into stakeholder dynamics in the context of the DPIA imposes itself. This dissertation did not specifically zoom in on power differences between stakeholders, while this might in practice be an important element to take into account (Mitchell, Agle and Wood, 1997). In addition, studying the dynamic nature of stakeholder interests as the DPIA progresses, might be highly insightful with regard to stakeholder management. Finally, international research could pinpoint variations in practices, interests and emphases of stakeholders in different geographic contexts.

A second series of suggestions builds on the insights concerning competition in the SCS market. Several chapters elaborate on the assumption and theoretical consensus that opening up data will stimulate

competition (Kerber, 2019). However, empirical evidence for the size of such an effect is mostly missing. In particular in view of the DMA and DGA proposals, more research in that direction is needed. Going beyond open data, the competitive effects of using certain data standards and requiring specific interoperability measures should also be investigated (Gal & Rubinfield, 2019). In essence, necessary conditions for open data to truly boost competition should be researched, and then diligently mapped.

Concerning data protection related ex-ante transaction costs, more in-depth research is needed. To arrive at general conclusions, a substantially larger sample will be needed. More regionally-focused research could pinpoint geographic differences. In the near future these types of investigations might become feasible. Moreover, monitoring the competitive relevance of data protection related ex-ante transaction costs over time would be important to assess the feasibility of creating a race to the top on data protection levels. Furthermore, additional in-depth research on complete life-cycle transaction costs related to data protection could provide important insights.

References

Acquisti, A., Taylor, C., & Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature*, *54*(2), 442–492. https://doi.org/10.1257/jel.54.2.442

Agoria. (n.d.). *Waarom Agoria?* Retrieved on 25 May 2019 from https://www.agoria.be/nl/Waarom-Agoria

Akbar, Y. H., & Tracogna, A. (2018). The sharing economy and the future of the hotel industry: Transaction cost theory and platform economics. *International Journal of Hospitality Management*, *71*, 91–101. https://doi.org/10.1016/j.ijhm.2017.12.004

Albrecht, J. P. (2016). How the GDPR Will Change the World. *European Data Protection Law Review, 2*(3), 287–289. https://doi.org/10.21552/EDPL/2016/3/4

Allison, P. D. (2014). Measures of fit for logistic regression. *Proceedings of the SAS Global Forum 2014 Conference*, 1-13.

Al Nuaimi, E., Al Neyadi, H., Mohamed, N., & Al-Jaroodi, J. (2015). Applications of big data to smart cities. *Journal of Internet Services and Applications*, *6*(1), 25. https://doi.org/10.1186/s13174-015-0041-5

Amponsah, C. T. (2011). Application of multi-criteria decision making process to determine critical success factors for procurement of capital projects under public-private partnerships. *International Journal of the Analytic Hierarchy Process*, *3*(2). https://doi.org/10.13033/ijahp.v3i2.121

Anand, P. B., & Navío-Marco, J. (2018). Governance and economics of smart cities: Opportunities and challenges. *Telecommunications Policy*, *42*(10), 795–799. https://doi.org/10.1016/j.telpol.2018.10.001

Andreani, S., Kalchschmidt, M., Pinto, R., & Sayegh, A. (2019). Reframing technologically enhanced urban scenarios: A design research model towards human centered smart cities. *Technological Forecasting and Social Change*, *142*, 15–25. https://doi.org/10.1016/j.techfore.2018.09.028

Anthopoulos, L. G. (2015). Understanding the Smart City Domain: A Literature Review. In Rodríguez-Bolívar M. P. (Ed.), *Transforming City Governments for Successful Smart Cities* (pp. 9–21). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-03167-5_2

Article 29 Working party. (2016). *Guidelines on Data Protection Officers ('DPOs') (WP 243)*. [Article 29 Working party's guideline]. Retrieved on 5 November 2021 from https://ec.europa.eu/newsroom/article29/items/612048

Article 29 Working party. (2017). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248).* [Article 29 Working party's guideline]. Retrieved on 8

October 2019 from https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Aull-Hyde, R., Erdogan, S., & Duke, J. (2006). An experiment on the consistency of aggregated comparison matrices in AHP. *European Journal of Operational Research, 171*(1), 290–295. https://doi.org/10.1016/j.ejor.2004.06.037

Axelsson, K., & Granath, M. (2018). Stakeholders' stake and relation to smartness in smart city development: Insights from a Swedish city planning project. *Government Information Quarterly*, *35*(4), 693–702. https://doi.org/10.1016/j.giq.2018.09.001

Bartoli, A., Hernandez-Serrano, J., Soriano, M., Dohler, M., Kountouris, A., & Barthel, D. (2011). *Security and Privacy in your Smart City*. Proceedings of Barcelona Smart Cities Congress 2011. Retrieved on 16 April 2019 from https://pdfs.semanticscholar.org/a8eb/00601cdb94ff6bbfc03118f3fcb7575ba07a.pdf

Baruch, Y. (1999). Response Rate in Academic Studies - A Comparative Analysis. *Human Relations*, *52*(4), 421–438. https://doi.org/10.1177/001872679905200401

Beiragh, R. G., Alizadeh, R., Kaleibari, S. S., Cavallaro, F., Zolfani, S. H., Bausys, R., & Mardani, A. (2020). An integrated Multi-Criteria Decision Making Model for Sustainability Performance Assessment for Insurance Companies. *Sustainability*, *12*(3), 789. https://doi.org/10.3390/su12030789

Belgian Data Protection Authority. (2018). *Aanbeveling nr. 01/2018 van 28 februari 2018.* [Belgian data protection authority's recommendation]. Retrieved on 5 November 2019 from https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanbeveling_01_2018.pdf

Belgian Data Protection Authority. (2020). *Beslissing ten gronde 25/2020 van 14 mei 2020: Rechtsgrondslag van verwerkingen van persoonsgegevens door sociale media platform* [Data protection authority decision]. Retrieved on 26 January 2021 from https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-25-2020.pdf

Belgian Data Protection Authority (DPA). (n.d.). *Meer informatie over de Autoriteit.* [Website] Retrieved on 15 October 2019 from https://www.gegevensbeschermingsautoriteit.be/meer-informatie-over-de-autoriteit

Bell, D. and Jayne, M. (2009). Small Cities? Towards a Research Agenda. *International Journal of Urban and Regional Research, 33*, 683-699. https://doi.org/10.1111/j.1468-2427.2009.00886.x

Bergkamp, L. (2002). EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy. *Computer Law & Security Review, 18*(1), 31-47. https://doi.org/10.1016/S0267-3649(02)00106-1

Berry, W. D., & Feldman, S. (1985). *Multiple Regression in Practice*. Thousand Oaks, CA: SAGE.

Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., & Rost, M. (2016). A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation. In Schiffner S., Serna J., Ikonomou D., Rannenberg K. (Eds.), *Privacy Technologies and Policy* (pp. 21-37). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-44760-5_2

Binns, R. (2017). Data protection impact assessments: a meta-regulatory approach. *International Data Privacy Law*, *7*(1), 22–35. https://doi.org/10.1093/idpl/ipw027

Bisztray, T., & Gruschka, N. (2019). Privacy Impact Assessment: Comparing Methodologies with a Focus on Practicality. In A. Askarov, R. R. Hansen, & W. Rafnsson (Eds.), *Secure IT Systems* (pp. 3–19). Springer International Publishing. https://doi.org/10.1007/978-3-030-35055-0_1

Blandford, A. E. (2013). Semi-structured qualitative studies. In Soegaard, M., & Dam, R. (Eds.), *The Encyclopedia of Human-Computer Interaction*. Aarhus, Denmark: Interaction Design Foundation.

Blume, J. (2018). A Contextual Extraterritoriality Analysis of the DPIA and DPO Provisions in the GDPR Notes. *Georgetown Journal of International Law*, *49*(4), 1425–1460.

Bogner, A., Littig, B., & Menz, W. (Eds.). (2009). *Interviewing experts*. Basingstoke [England] ; New York: Palgrave Macmillan. https://doi.org/10.1057/9780230244276

Bojanc, R., & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management, 28*(5), 413-422. https://doi.org/10.1016/j.ijinfomgt.2008.02.002

Bonneau, J., & Preibusch, S. (2010). The Privacy Jungle: On the Market for Data Protection in Social Networks. In T. Moore, D. Pym, & C. Ioannidis (Eds.), *Economics of Information Security and Privacy* (pp. 121–167). Springer US. https://doi.org/10.1007/978-1-4419-6967-5_8

Boral, S., Howard, I., Chaturvedi, S. K., McKee, K., & Naikan, V. N. A. (2020). An integrated approach for fuzzy failure modes and effects analysis using fuzzy AHP and fuzzy MAIRCA. *Engineering Failure Analysis, 108*, 104195. https://doi.org/10.1016/j.engfailanal.2019.104195

Bouranta, N., Chitiris, L., & Paravantis, J. (2009). The relationship between internal and external service quality. *International Journal of Contemporary Hospitality Management*, *21*(3), 275–293. https://doi.org/10.1108/09596110910948297

Boussauw, K., Van Meeteren, M., Sansen, J., Meijers, E., Storme, T., Louw, E., Derudder, B. & Witlox, F. (2018). Planning for agglomeration economies in a polycentric region: Envisioning an

efficient metropolitan core area in Flanders. *European Journal of Spatial Development, 69*, 1-26. http://doi.org/10.30689/EJSD2018:69.1650-9544

Bovis, C. (2005). *Public Procurement in the European Union*. London, England: Palgrave Macmillan UK.

Braun, T., Fung, B. C. M., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. *Sustainable Cities and Society*, *39*, 499–507. https://doi.org/10.1016/j.scs.2018.02.039

Brauneis, R., & Goodman, E. P. (2018). Algorithmic transparency for the smart city. *Yale Journal of Law & Technology, 20*, 103. http://doi.org/10.2139/ssrn.3012499

Bresciani, S., Ferraris, A., & Del Giudice, M. (2018). The management of organizational ambidexterity through alliances in a new context of analysis: Internet of Things (IoT) smart city projects. *Technological Forecasting and Social Change*, *136*, 331–338. https://doi.org/10.1016/j.techfore.2017.03.002

Breuer, J., & Pierson, J. (2021). The Right to the City and Data Protection for Developing Citizen-Centric Digital Cities. *Information, Communication & Society, 24*(6), 797–812. https://doi.org/10.1080/1369118X.2021.1909095

Brodley, J. F. (1987). The Economic Goals of Antitrust: Efficiency, Consumer Welfare, and Technological Progress Papers Presented at the Airlie House Conference on the Antitrust Alternative. *New York University Law Review*, *62*(5), 1020–1053.

Brogaard, L. (2017). Innovation and value in pre-commercial procurement: A systematic evaluation of national experiences. *Journal of Strategic Contracting and Negotiation*, *3*(3), 137–156. https://doi.org/10.1177/2055563618799065

Brown, L. D. (1985). People-Centered Development and Participatory Research. *Harvard Educational Review, 55*(1), 69-76. https://doi.org/10.17763/haer.55.1.r07478n215287101

Buccino, G., Iossa, E., Raganelli, B., & Vincze, M. (2020). Competitive dialogue: An economic and legal assessment. *Journal of Public Procurement*, *20*(2), 163–185. https://doi.org/10.1108/JOPP-09-2019-0059

Budzinski, O. (2008). Monoculture versus diversity in competition economics. *Cambridge Journal of Economics*, *32*(2), 295–324. https://doi.org/10.1093/cje/bem031

Buiten, M. C. (2019). Regulating Data Giants: Between Competition Law and Data Protection Law. In K. Mathis & A. Tor (Eds.), *New Developments in Competition Law and Economics* (pp. 265–294). Springer International Publishing. https://doi.org/10.1007/978-3-030-11611-8_13

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-548. https://doi.org/10.2307/25750690

Buocz, T., Ehrke-Rabel, T., Hödl, E., & Eisenberger, I. (2019). Bitcoin and the GDPR: Allocating responsibility in distributed networks. *Computer Law & Security Review*, *35*(2), 182–198. https://doi.org/10.1016/j.clsr.2018.12.003

Bu-Pasha, S.-. (2020). The controller's role in determining 'high risk' and data protection impact assessment (DPIA) in developing digital smart city. *Information & Communications Technology Law, 29*(3), 391–402. https://doi.org/10.1080/13600834.2020.1790092

Bygrave, L. A. (2017). Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. *Oslo Law Review*, *4*(02), 105–120. https://doi.org/10.18261/issn.2387-3299-2017-02-03

Callegaro, M., Manfreda, K. L., & Vehovar, V. (2015). *Web Survey Methodology*. London, England: SAGE.

Calzada, I. (2018). Smart Citizens from Data Providers to Decision-Makers? The Case Study of Barcelona. *Sustainability*, *10*(9), 3252. https://doi.org/10.3390/su10093252

Camero, A., & Alba, E. (2019). Smart City and information technology: A review. Cities, 93, 84–94. https://doi.org/10.1016/j.cities.2019.04.014

Cameron, A. C., & Trivedi, P. K. (2005). *Microeconometrics: Methods and applications*. New York, NY: Cambridge University Press.

Capdevila, I., & Zarlenga, M. I. (2015). Smart city or smart citizens? The Barcelona case. *Journal of Strategy and Management, 8*(3), 266-282. https://doi.org/10.1108/JSMA-03-2015-0030

Capgemini. (2019). *Championing Data Protection and Privacy: a source of competitive advantage in the digital century* [report]. Retrieved on 10 January 2020 from https://www.capgemini.com/championing-data-protection-and-privacy/

Capobianco, A., & Nyeso, A. (2018). Challenges for Competition Law Enforcement and Policy in the Digital Economy. *Journal of European Competition Law & Practice*, *9*(1), 19–27. https://doi.org/10.1093/jeclap/lpx082

Caragliu, A., Del Bo, C., & Nijkamp, P. (2011). Smart Cities in Europe. *Journal of Urban Technology*, *18*(2), 65–82. https://doi.org/10.1080/10630732.2011.601117

Carbonara, N., Costantino, N., & Pellegrino, R. (2016). A transaction costs-based model to choose PPP procurement procedures. Engineering, Construction and Architectural Management, 23(4), 491–510. https://doi.org/10.1108/ECAM-07-2014-0099

Carlsson, B. (2004). The Digital Economy: What is new and what is not? *Structural Change and Economic Dynamics*, *15*(3), 245–264. https://doi.org/10.1016/j.strueco.2004.02.001

Casaló, L., Flavián, C., & Guinalíu, M. (2007). The role of security, privacy, usability and reputation in the development of online banking. *Online Information Review, 31*(5), 583-603. https://doi.org/10.1108/14684520710832315

Cecco, L. (2020, 7 May). Google affiliate Sidewalk Labs abruptly abandons Toronto smart city project. *The Guardian*. Retrieved on 8 December 2021 from https://www.theguardian.com/technology/2020/may/07/google-sidewalk-labs-toronto-smart-city-abandoned

Cennamo, C. (2019). *Competing in Digital Markets: a Platform-Based Perspective* [Academy of Management Perspectives]. Retrieved on 25 January 2021 from https://doi.org/10.5465/amp.2016.0048

Chamoso, P., González-Briones, A., Rodríguez, S., & Corchado, J. M. (2018). Tendencies of Technologies and Platforms in Smart Cities: A State-of-the-Art Review. *Wireless Communications and Mobile Computing, 2018*, 3086854. https://doi.org/10.1155/2018/3086854

Charter of Fundamental Rights of the European Union. Official Journal of the European Union, Vol. C326 (26 October 2012), pp. 391-407. Retrieved on 8 April 2019 from https://eur-lex.europa.eu/eli/treaty/char_2012/oj

Chen, M. K., & Wang, S.-C. (2010). The critical factors of success for information service industry in developing international market: Using analytic hierarchy process (AHP) approach. *Expert Systems with Applications 37(*1), 694-704. https://doi.org/10.1016/j.eswa.2009.06.012

Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J. R., Mellouli, S., Nahon, K., Pardo, T. A., Scholl, H. J. (2012). Understanding Smart Cities: An Integrative Framework. *2012 45th Hawaii International Conference on System Sciences*, 2289–2297. https://doi.org/10.1109/HICSS.2012.615

Christensen, L. , Colciago, A., Etro, F., & Rafert, G. (2013). The Impact of the Data Protection Regulation in the E.U. [Intertic Policy Paper]. Retrieved on 18 March 2020 from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.657.138&rep=rep1&type=pdf

Christofi, A., Breuer, J., von Grafenstein, M., Kritikos, M., Groothuizen, R., van Zeeland, I., & Pierson J. (2021). *Where are the Missing Data Subjects? Data Protection, Control and Public Participation.* [SMIT Policy Brief #45]. Retrieved on 11 June 2021 from https://smit.vub.ac.be/policy-brief-45-where-are-the-missing-data-subjects

Cinelli, M., Coles, S., & Kirwan, K. (2014). Analysis of the Potentials of Multi Criteria Decision Analysis Methods to Conduct Sustainability Assessment. *Ecological Indicators, 46*, 138–148. https://doi.org/10.1016/j.ecolind.2014.06.011

Clarivate. (2021). *Web of Science* [Database]. Retrieved on 7 December 2021 from https://www.webofscience.com/wos/woscc/basic-search

Clarke, R. (2009). Privacy impact assessment: Its origins and development. *Computer Law & Security Review, 25*(2), 123-135. https://doi.org/10.1016/j.clsr.2009.02.002

Clemons, E. K., & Madhani, N. (2010). Regulation of Digital Businesses with Natural Monopolies or Third-Party Payment Business Models: Antitrust Lessons from the Analysis of Google. *Journal of Management Information Systems*, *27*(3), 43–80. https://doi.org/10.2753/MIS0742-1222270303

Clifford, D., & Ausloos, J. (2018). Data Protection and the Role of Fairness. *Yearbook of European Law*, *37*, 130–187. https://doi.org/10.1093/yel/yey004

Coase, R. H. (1937). The Nature of the Firm. *Economica, 4*(16), 386–405. https://doi.org/10.1111/j.1468-0335.1937.tb00002.x

Colangelo, G., & Maggiolino, M. (2017). Data Protection in Attention Markets: Protecting Privacy through Competition? *Journal of European Competition Law & Practice*, *8*(6), 363–369. https://doi.org/10.1093/jeclap/lpx037

Cornwall, A., & Jewkes, R. (1995). What is participatory research? *Social Science & Medicine, 41*(12), 1667-1676. https://doi.org/10.1016/0277-9536(95)00127-S

Court of Justice of the European Union. (2014). Case C-293/12, Digital Rights Ireland, ECLI:EU:C:2014:238.

Crump, C. (2016). Surveillance policy making by procurement. *Washington Law Review*, *91*, 1595. http://doi.org/10.2139/ssrn.2737006

Dameri, R. P. (2012). Searching for Smart City definition: a comprehensive proposal. *International Journal of Computers & Technology*, *11*(5), 2544–2551. https://doi.org/10.24297/ijct.v11i5.1142

Dameri, R. P. (2017). Smart City Definition, Goals and Performance. In R. P. Dameri (Ed.), *Smart City Implementation: Creating Economic and Public Value in Innovative Urban Systems* (pp. 1–22). Springer International Publishing. https://doi.org/10.1007/978-3-319-45766-6_1

Dameri, R. P., & Rosenthal-Sabroux, C. (2014). Smart City and Value Creation. In R. P. Dameri & C. Rosenthal-Sabroux (Eds.), *Smart City: How to Create Public and Economic Value with High Technology in Urban Space* (pp. 1–12). Springer International Publishing. https://doi.org/10.1007/978-3-319-06160-3_1

Data Protection Commission. (2019). *Guide to Data Protection Impact Assessments (DPIAs) of September 2019.* [Guidance Note by the Data Protection Commission]. Retrieved on 27 February 2020 from https://www.dataprotection.ie/sites/default/files/uploads/2019-09/190926%20Guide%20to%20Data%20Protection%20Impact%20Assessments%20%28DPIAs%29.pdf

Data Protection Commission. (2020). *Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act 2018 in the matter of Twitter International Company*

[Data protection authority decision]. Retrieved on 26 January 2021 from https://edpb.europa.eu/sites/edpb/files/decisions/final_decision_-_in-19-1-1_9.12.2020.pdf

Delina, R., Gróf, M., & Dráb, R. (2021). Understanding the Determinants and Specifics of Pre-Commercial Procurement. *Journal of Theoretical and Applied Electronic Commerce Research*, *16*(2), 80–100. https://doi.org/10.4067/S0718-18762021000200106

Demetzou, K. (2019). Data Protection Impact Assessment: A Tool for Accountability and the Unclarified Concept of 'High Risk' in the General Data Protection Regulation. *Computer Law & Security Review, 35*(6), 105342. https://doi.org/10.1016/j.clsr.2019.105342

De Schepper, S., Haezendonck, E., & Dooms, M. (2015). Understanding pre-contractual transaction costs for Public–Private Partnership infrastructure projects. *International Journal of Project Management*, *33*(4), 932–946. https://doi.org/10.1016/j.ijproman.2014.10.015

Desdemoustier, J., & Crutzen, N. (2017). *Etat des lieux sur la dynamique « Smart City » en Belgique : Un baromètre quantitatif* [Report]. Retrieved on 12 February 2019 from https://orbi.uliege.be/handle/2268/220415

Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC Official Journal of the European Union, Vol. L94 (28 March 2014), pp. 65–242. Retrieved on 14 September 2020 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0024

DLA Piper. (2019). *Data protection laws of the world* [Legal guide]. Retrieved on 7 January 2020 from https://www.dlapiperdataprotection.com

Dudkin, G., & Välilä, T. (2005). *Transaction Costs in Public Private Partnerships: A First Look at the Evidence* [European Investment Bank Economic and Financial Report 2005/03]. Retrieved on 23 April 2020 from https://www.eib.org/attachments/efs/efr_2005_v03_en.pdf

Duflo, E., Glennerster, R., & Kremer, M. (2007). Using Randomization in Development Economics Research: A Toolkit. In P. T. Schults, & J. Strauss (Eds.), *Handbook of Development Economics* (pp. 3895-62). Elsevier Science Ltd.: North Holland.

Dugger, W. M. (1983). The Transaction Cost Analysis of Oliver E. Williamson: A New Synthesis? *Journal of Economic Issues*, *17*(1), 95–114. https://doi.org/10.1080/00213624.1983.11504090

Dweiri, F., Kumar, S., Khan, S. A., & Jain, V. (2016). Designing an integrated AHP based decision support system for supplier selection in automotive industry. *Expert Systems with Applications, 62*, 273–283. https://doi.org/10.1016/j.eswa.2016.06.030

Edquist, C., & Zabala-Iturriagagoitia, J. M. (2015). Pre-commercial procurement: A demand or supply policy instrument in relation to innovation? *R&D Management*, *45*(2), 147–160. https://doi.org/10.1111/radm.12057

Edwards, L. (2016). Privacy, Security and Data Protection in Smart Cities: *European Data Protection Law Review*, *2*(1), 28–58. https://doi.org/10.21552/EDPL/2016/1/6

Engels, B. (2016). Data portability among online platforms. *Internet Policy Review*, *5*(2), 1–17. https://doi.org/10.14763/2016.2.408

Eskerod, P., Huemann, M., & Savage, G. (2015). Project Stakeholder Management—Past and Present. *Project Management Journal, 46*(6), 6–14. https://doi.org/10.1002/pmj.21555

European Commission. (2007). *Pre-Commercial Procurement: Driving Innovation to Ensure Sustainable High Quality Public Services in Europe* [European Commission communication]. Retrieved on 20 October 2021 from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0799:FIN:EN:PDF

European Commission. (2012). *Impact assessment /* SEC/2012/0072 final */* [European Commission staff working paper]. Retrieved on 27 August 2019 from http://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf

European Commission. (2016). *Innovation Partnerships Keep Public Services up to Date* [Website]. Retrieved on 29 July 2021 https://ec.europa.eu/growth/content/8699-innovation-partnerships-keep-public-services-date_en

European Commission. (2018a). *Impact Assessment on the Review of the Directive 2003/98/EC on the Reuse of Public Sector Information* [Impact Assessment]. Retrieved on 25 January 2021 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:127:FIN

European Commission. (2018b). *When is a Data Protection Impact Assessment (DPIA) required?* [Website]. Retrieved on 13 March 2019 from https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/when-data-protection-impact-assessment-dpia-required_en

European Commission. (2019). *Types of EU law* [Website]. Retrieved on 30 August 2019 from https://ec.europa.eu/info/law/law-making-process/types-eu-law_en

European Commission. (2020a). *Data protection in the EU* [Website]. Retrieved on 19 August 2020 from https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_nl

European Commission. (2020b). *Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)* [European Commission communication]. Retrieved on 20 October 2021 from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN

European Commission. (2020c). *Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)* [European Commission

communication]. Retrieved on 20 October 2021 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0767

European Commission. (2020d). *Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC* [European Commission communication]. Retrieved on 20 October 2021 from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN

European Commission. (2020e). *Public tendering rules* [Website]. Retrieved on 26 October 2021 from https://europa.eu/youreurope/business/selling-in-eu/public-contracts/public-tendering-rules/index_en.htm

European Commission. (2020f). *Shaping Europe's Digital Future* [European Commission communication]. Retrieved on 25 January 2021 from https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

European Commission. (n.d.a). *Fundamental rights* [Website]. Retrieved on 28 July 2021 from https://ec.europa.eu/home-affairs/pages/glossary/fundamental-rights_en

European Commission. (n.d.b). *Innovation Procurement* [Website]. Retrieved on 28 July 2021 from https://ec.europa.eu/info/policies/public-procurement/tools-public-buyers/innovation-procurement_en

European Commission. (n.d.c). *Pre-Commercial Procurement* [Website]. Retrieved on 28 July 2021 from https://digital-strategy.ec.europa.eu/en/policies/pre-commercial-procurement

European Data Protection Board. (2019). *EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.* [Guideline]. Retrieved on 2 January 2020 from https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_nl

European Data Protection Supervisor. (2019). *The History of the General Data Protection Regulation* [Website]. Retrieved on 30 August 2019 from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

European Data Protection Supervisor. (n.d.a). *Data Protection Officer (DPO)* [Website]. Retrieved on 18 December 2019 from https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

European Data Protection Supervisor. (n.d.b). *Information security* [Website]. Retrieved on 18 December 2019 from https://edps.europa.eu/data-protection/data-protection/reference-library/information-security_en

European Smart Cities. (n.d.). *The ranking* [Website]. Retrieved on 10 June 2021 from http://www.smart-cities.eu/ranking.html

Eurostat. (2016). *Urban Europe — statistics on cities, towns and suburbs — patterns of urban and city developments* [Website]. Retrieved on 24 May 2019 from https://ec.europa.eu/eurostat/statistics-explained/index.php/Urban_Europe_%E2%80%94_statistics_on_cities,_towns_and_suburbs_%E2%80%94_patterns_of_urban_and_city_developments#Patterns_of_urban_and_city_developments_in_the_EU

Evans, D. S., & Schmalensee, R. (2012). *The Antitrust Analysis of Multi-Sided Platform Businesses* [Coase-Sandor Institute for Law & Economics Working Paper]. Retrieved on 23 April 2020 from https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1482&context=law_and_economics

Fagnant, D. J., & Kockelman, K. (2015). Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations. *Transportation Research Part A: Policy and Practice*, *77*, 167–181. https://doi.org/10.1016/j.tra.2015.04.003

Fernandez-Anez, V., Fernández-Güell, J. M., & Giffinger, R. (2018). Smart City implementation and discourses: An integrated conceptual model. The case of Vienna. *Cities*, *78*, 4–16. https://doi.org/10.1016/j.cities.2017.12.004

Fernández-Güell, J.-M., Collado-Lara, M., Guzmán-Araña, S., & Fernández-Añez, V. (2016). Incorporating a Systemic and Foresight Approach into Smart City Initiatives: The Case of Spanish Cities. *Journal of Urban Technology*, *23*(3), 43–67. https://doi.org/10.1080/10630732.2016.1164441

Finch, K., & Tene, O. (2018). Smart Cities: Privacy, Transparency, and Community. In Selinger, E., Polonetsky, J., & Tene, O. (Eds.), *The Cambridge Handbook of Consumer Privacy* (pp. 125–148). Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316831960.007

Flemish Agency for Innovation and Entrepreneurship. (2018). *Ontdek 21 smart city-toepassingen* [Website]. Retrieved on 20 November 2019 from https://www.vlaio.be/nl/nieuws/ontdek-21-smart-city-toepassingen

Flemish Government. (n.d.). *Bewustmaking* [Website]. Retrieved on 10 December 2019 from https://overheid.vlaanderen.be/bewustmaking

Flemish Institute for Biotechnology. (n.d.). *Living in Flanders, the heart of Europe* [Website]. Retrieved on 24 May 2019 from http://www.vib.be/en/about-vib/Pages/Living-in-Flanders.aspx

Fombrun, C., & Shanley, M. (1990). What's in a name? Reputation building and corporate strategy. *Academy of Management Journal, 33*(2), 233-248. https://doi.org/10.5465/256324

Fontana, F. (2014). The Smart City and the Creation of Local Public Value. In R. P. Dameri & C. Rosenthal-Sabroux (Eds.), *Smart City: How to Create Public and Economic Value with High Technology in Urban Space* (pp. 117–137). Springer International Publishing. https://doi.org/10.1007/978-3-319-06160-3_6

Forman, E., & Peniwati, K. (1998). Aggregating individual judgments and priorities with the analytic hierarchy process. *European Journal of Operational Research*, *108*(1), 165–169. https://doi.org/10.1016/S0377-2217(97)00244-0

Fossey, E., Harvey, C., McDermott, F., & Davidson, L. (2002). Understanding and evaluating qualitative research. *Australian and New Zealand Journal of Psychiatry, 36*, 717–732. https://doi.org/10.1046/j.1440-1614.2002.01100.x

French Data Protection Authority (DPA). (2020). *Délibération SAN-2020-012 du 7 décembre 2020* [Data protection authority decision]. Retrieved on 26 January 2021 from https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042635706

Frooman, J. (2010). The issue network: Reshaping the stakeholder model. *Canadian Journal of Administrative Sciences / Revue Canadienne Des Sciences de l'Administration, 27*(2), 161–173. https://doi.org/10.1002/cjas.150

Frow, P., & Payne, A. (2011). A stakeholder perspective of the value proposition concept. *European Journal of Marketing, 45*(1/2), 223–240. https://doi.org/10.1108/03090561111095676

Fung, B. C. M., Trojer, T., Hung, P. C. K., Xiong, L., Al-Hussaeni, K., & Dssouli, R. (2012). Service-Oriented Architecture for High-Dimensional Private Data Mashup. *IEEE Transactions on Services Computing*, *5*(3), 373–386. https://doi.org/10.1109/TSC.2011.13

Gal, M. S., & Aviv, O. (2020). The Competitive Effects of the GDPR. *Journal of Competition Law & Economics*, *16*(3), 349–391. https://doi.org/10.1093/joclec/nhaa012

Gal, M., & Petit, N. (2020). *Radical Restorative Remedies for Digital Markets* [SSRN Scholarly Paper]. Retrieved on 25 January 2021 from https://papers.ssrn.com/abstract=3687604

Gal, M. S., & Rubinfeld, D. L. (2019). Data standardization. *New York University Law Review, 94*(4), 737-770. http://dx.doi.org/10.2139/ssrn.3326377

Galič, M., & Schuilenburg, M. (2020). Reclaiming the Smart City: Toward a New Right to the City. In J. C. Augusto (Ed.), *Handbook of Smart Cities* (pp. 1–18). Springer International Publishing. https://doi.org/10.1007/978-3-030-15145-4_59-1

Galletta, A. (2013). *Mastering the semi-structured interview and beyond: From research design to analysis and publication.* New York, NY: New York University Press. https://doi.org/10.18574/nyu/9780814732939.001.0001

Gellert, R. (2018). Understanding the Notion of Risk in the General Data Protection Regulation. *Computer Law & Security Review, 34*(2), 279–288. https://doi.org/10.1016/j.clsr.2017.12.003

Georghiou, L., Edler, J., Uyarra, E., & Yeow, J. (2014). Policy instruments for public procurement of innovation: Choice, design and assessment. *Technological Forecasting and Social Change*, *86*, 1–12. https://doi.org/10.1016/j.techfore.2013.09.018

Georgiou, D., & Lambrinoudakis, C. (2021). Data Protection Impact Assessment (DPIA) for Cloud-Based Health Organizations. *Future Internet, 13*(3), 66. https://doi.org/10.3390/fi13030066

Gharizadeh Beiragh, R., Alizadeh, R., Shafiei Kaleibari, S., Cavallaro, F., Zolfani, S., Bausys, R., & Mardani, A. (2020). An integrated Multi-Criteria Decision Making Model for Sustainability Performance Assessment for Insurance Companies. *Sustainability*, *12*(3), 789. http://dx.doi.org/10.3390/su12030789

Giffinger, R., Fertner, C., Kramar, H., & Meijers, E. (2007). *City-ranking of European Medium-Sized Cities* [Website]. Retrieved on 7 January 2020 from http://www.smartcity-ranking.eu/download/city_ranking_final.pdf

Gleeson, N., & Walden, I. (2016). Placing the state in the cloud: Issues of data governance and public procurement. *Computer Law & Security Review*, *32*(5), 683–695. https://doi.org/10.1016/j.clsr.2016.07.004

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research*, *59*(6), 703–705. https://doi.org/10.2501/IJMR-2017-050

Golany, B., & Kress, M. (1993). A multicriteria evaluation of methods for obtaining weights from ratio-scale matrices. *European Journal of Operational Research*, *69*(2), 210–220. https://doi.org/10.1016/0377-2217(93)90165-J

Graef, I. (2015). Mandating portability and interoperability in online social networks: Regulatory and competition law issues in the European Union. *Telecommunications Policy*, *39*(6), 502–514. https://doi.org/10.1016/j.telpol.2015.04.001

Grand View Research. (2020). *Smart Cities Market Size, Share & Trends Analysis Report By Application, By Region, And Segment Forecasts, 2020 – 2027* [Market analysis report]. Retrieved on 25 January 2021 from https://www.grandviewresearch.com/industry-analysis/smart-cities-market#:~:text=Report%20Overview,24.7%25%20from%202020%20to%202027

Grossi, G., & Pianezzi, D. (2017). Smart cities: Utopia or neoliberal ideology? *Cities*, *69*, 79–85. https://doi.org/10.1016/j.cities.2017.07.012

Haase, D., Larondelle, N., Andersson, E. et al. (2014). A Quantitative Review of Urban Ecosystem Service Assessments: Concepts, Models, and Implementation. *AMBIO, 43*, 413–433. https://doi.org/10.1007/s13280-014-0504-0

Haber, N., Fargnoli, M., & Sakao, T. (2020). Integrating QFD for product-service systems with the Kano model and fuzzy AHP. *Total Quality Management & Business Excellence, 31*(9–10), 929–954. https://doi.org/10.1080/14783363.2018.1470897

Hallinan, D., & Martin, N. (2020). Fundamental Rights, the Normative Keystone of DPIA. *European Data Protection Law Review, 6*(2), 178 – 193. https://doi.org/10.21552/edpl/2020/2/6

Hart, S., Ferrara, A. L., & Paci, F. (2020). Fuzzy-Based Approach to Assess and Prioritize Privacy Risks. *Soft Computing, 24*(3), 1553–63. https://doi.org/10.1007/s00500-019-03986-5

Härting, R.-C., Kaim, R., & Ruch, D. (2020). Impacts of the Implementation of the General Data Protection Regulations (GDPR) in SME Business Models—An Empirical Study with a Quantitative Design. In G. Jezic, J. Chen-Burger, M. Kusek, R. Sperka, R. J. Howlett, & L. C. Jain (Eds.), *Agents and Multi-Agent Systems: Technologies and Applications 2020* (pp. 295–303). Springer. https://doi.org/10.1007/978-981-15-5764-4_27

Hartmann, P. (1995). Response Behavior in Interview Settings of Limited Privacy. *International Journal of Public Opinion Research, 7*(4), 383–390. https://doi.org/10.1093/ijpor/7.4.383

Hashem, I. A. T., Chang, V., Anuar, N. B., Adewole, K., Yaqoob, I., Gani, A., Ahmed, E., & Chiroma, H. (2016). The role of big data in smart city. *International Journal of Information Management*, *36*(5), 748–758. https://doi.org/10.1016/j.ijinfomgt.2016.05.002

HeinOnline. (2022). *Law Journal Library* [Database]. Retrieved on 23 March 2022 from https://home.heinonline.org/content/law-journal-library/

Herrschel, T., Dierwechter, Y., & Dierwechter, Y. (2018). *Smart Transitions in City Regionalism : Territory, Politics and the Quest for Competitiveness and Sustainability*. London, England: Routledge.

Ho, D., Newell, G., & Walker, A. (2005). The importance of property-specific attributes in assessing CBD office building quality. *Journal of Property Investment & Finance, 23*(5), 424-444. https://doi.org/10.1108/14635780510616025

Hoppe, E. I., & Schmitz, P. W. (2013). Public-private partnerships versus traditional procurement: Innovation incentives and information gathering. *The RAND Journal of Economics*, *44*(1), 56–74. https://doi.org/10.1111/1756-2171.12010

Horák, M., Stupka, V., & Husák, M. (2019). GDPR Compliance in Cybersecurity Software: A Case Study of DPIA in Information Sharing Platform. *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 1–8. https://doi.org/10.1145/3339252.3340516

Hosmer, D.W., & Lemeshow, S. (1980). Goodness of fit tests for the multiple logistic regression model. *Communications in Statistics - Theory and Methods, 9*, 1043- 1069.

Hsieh, Y.-C., Hsieh, J.-K., & Feng Y.-C. (2011). Switching between Social Media: The Role of Motivation and Cost. *Second International Conference on Economics, Business and Management*.

Retrieved on 26 January 2021 from http://www.ipedr.com/vol22/18-ICEBM2011-M00032.pdf

Hueskes, M., Verhoest, K., & Block, T. (2017). Governing public–private partnerships for sustainability: An analysis of procurement and governance practices of PPP infrastructure projects. *International Journal of Project Management*, *35*(6), 1184–1195. https://doi.org/10.1016/j.ijproman.2017.02.020

IMD Smart City Observatory. (2020). *Smart city index 2020* [Website]. Retrieved on 9 June 2021 from https://www.imd.org/smart-city-observatory/smart-city-index/

imec-SMIT-VUB & imec.Living.Labs. (2019). *imec.smartcitymeter 2019* [Report]. Retrieved on 17 October from https://www.imeccityofthings.be/drupal/sites/default/files/inline-files/SCM2019_Rapport_Finaal_NL_1.pdf

Iossa, E., Biagi, F., & Valbonesi, P. (2018). Pre-commercial procurement, procurement of innovative solutions and innovation partnerships in the EU: Rationale and strategy. *Economics of Innovation and New Technology*, *27*(8), 730–749. https://doi.org/10.1080/10438599.2017.1402431

Janssen, M., Luthra, S., Mangla, S., Rana, N. P., & Dwivedi, Y. K. (2019). Challenges for adopting and implementing IoT in smart cities: An integrated MICMAC-ISM approach. *Internet Research*, *29*(6), 1589–1616. https://doi.org/10.1108/INTR-06-2018-0252

Jia, J., Jin, G. Z., & Wagman, L. (2019). *The Short-Run Effects of GDPR on Technology Venture Investment* [SSRN Scholarly Paper]. Retrieved on 5 November 2020 from https://papers.ssrn.com/abstract=3278912

Johnson, G., Shriver, S, & Goldberg, S. (2021). *Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR* [SSRN Scholarly Paper]. Retrieved on 20 April 2021 from https://papers.ssrn.com/abstract=3477686

Johnston, R. (2008). Internal service – barriers, flows and assessment. *International Journal of Service Industry Management*, *19*(2), 210–231. https://doi.org/10.1108/09564230810869748

Kang, M.-P., Mahoney, J. T., & Tan, D. (2009). Why firms make unilateral investments specific to other firms: The case of OEM suppliers. *Strategic Management Journal*, *30*(2), 117–135. https://doi.org/10.1002/smj.730

Karvonen, A., Cugurullo, F., & Caprotti, F. (2018). *Inside Smart Cities: Place, Politics and Urban Innovation*. London, England: Routledge. https://doi.org/10.4324/9781351166201

Kayali, L., & Scott, M. (2021, 18 January). Brussels Eclipsed as EU Countries Roll Out Their Own Tech Rules. *POLITICO.* Retrieved on 19 January 2021 from https://www.politico.eu/article/eu-dsa-tech-rules-france-national-regulation/

Kerber, W. (2019). *Data-Sharing in IoT Ecosystems From a Competition Law Perspective: The Example of Connected Cars* [SSRN Scholarly Paper]. Retrieved on 16 April 2020 from https://www.ssrn.com/abstract=3445422

Kerr, C., Farrukh, C., Phaal, R., & Probert, D. (2013). Key principles for developing industrially relevant strategic technology management toolkits. *Technology Forecasting and Social Change, 80*(6), 1050–1070. https://doi.org/10.1016/j.techfore.2012.09.006

Kersting, N., & Vetter, A. (2013). *Reforming Local Government in Europe: Closing the Gap between Democracy and Efficiency*. Berlin, Germany: Springer Science & Business Media.

Khan, H. H., Malik, M. N., Zafar, R., Goni, F. A., Chofreh, A. G., Klemeš, J. J., & Alotaibi, Y. (2020). Challenges for sustainable smart city development: A conceptual framework. *Sustainable Development*, *28*(5), 1507–1518. https://doi.org/10.1002/sd.2090

Khan, Z., Pervez, Z., & Abbasi, A. G. (2017). Towards a secure service provisioning framework in a Smart city environment. *Future Generation Computer Systems*, *77*, 112–135. https://doi.org/10.1016/j.future.2017.06.031

Kitchin, R. (2016). *Getting smarter about smart cities: Improving data privacy and data security* [Data Protection Unit of the department of the Taoiseach technical report]. Retrieved on 7 August 2019 from http://www.taoiseach.gov.ie/eng/Publications/Publications_2016/Smart_Cities_Report_January_2016.pdf

Kitchin, R., Coletta, C., Evans, L., & Heaphy, L. (2018). Creating smart cities: Introduction. In Coletta, C., Evans, L., Heaphy, L., & Kitchin, R. (Eds.), *Creating Smart Cities* (pp. 1-18). London, England: Routledge. https://doi.org/10.4324/9781351182409

Kloza, D., Calvi, A., Casiraghi, S., Maymir, S. V., Ioannidis, N., Tanas, A., & van Dijk, N. (2020). *Data protection impact assessment in the European Union: developing a template for a report from the assessment process* [Report]. Retrieved on 14 December 2020 from https://osf.io/preprints/lawarxiv/7qrfp/

Kong, L., & Woods, O. (2018). The ideological alignment of smart urbanism in Singapore: Critical reflections on a political paradox. *Urban Studies, 55*(4), 679–701. https://doi.org/10.1177/0042098017746528

Kosta, E. (2020). Article 35. Data Protection Impact Assessment. In C. Kuner, L. A. Bygrave, & C. Docksey (Eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (pp. 669). Oxford University Press.

Kristensen, H. S., Mosgaard, M. A., & Remmen, A. (2021). Circular public procurement practices in Danish municipalities. *Journal of Cleaner Production*, *281*, 124962. https://doi.org/10.1016/j.jclepro.2020.124962

Kummitha, R. K. R., & Crutzen, N. (2017). How do we understand smart cities? An evolutionary perspective. *Cities*, *67*, 43–52. https://doi.org/10.1016/j.cities.2017.04.010

Kuss, O. (2002). Global goodness-of-fit tests in logistic regression with sparse data. *Statistics in Medicine*, *21*(24), 3789–3801. https://doi.org/10.1002/sim.1421

Kutlina-Dimitrova, Z., & Lakatos, C. (2016). Determinants of direct cross-border public procurement in EU Member States. *Review of World Economics*, *152*(3), 501–528. https://doi.org/10.1007/s10290-016-0251-3

Kwon, J., & Johnson, E. (2014). Health-Care Security Strategies for Data Protection and Regulatory Compliance. *Journal of Management Information Systems, 30*(2), 41-66. https://doi.org/10.2753/MIS0742-1222300202

Lancieri, F. (2021). *Narrowing Data Protection's Enforcement Gap* [SSRN Scholarly Paper]. Retrieved on 20 October 2020 from https://doi.org/10.2139/ssrn.3806880

Landes, W. M., & Posner, R. A. (1981). Market Power in Antitrust Cases. *Harvard Law Review*, *94*(5), 937–996. https://doi.org/10.2307/1340687

Laurer, M., & Seidl, T. (2021). Regulating the European Data-Driven Economy: A Case Study on the General Data Protection Regulation. *Policy & Internet*, *13*(2), 257–277. https://doi.org/10.1002/poi3.246

Lavrakas, P. (2008). *Encyclopedia of Survey Research Methods*. Sage Publications, Inc. https://doi.org/10.4135/9781412963947

Lee, J. H., Phaal, R., & Lee, S.-H. (2013). An integrated service-device-technology roadmap for smart city development. *Technological Forecasting and Social Change*, *80*(2), 286–306. https://doi.org/10.1016/j.techfore.2012.09.020

Lee, J., & Lee, H. (2014). Developing and validating a citizen-centric typology for smart city services. *Government Information Quarterly*, *31*(1), 93–105. https://doi.org/10.1016/j.giq.2014.01.010

Leinfelder, H., & Allaert, G. (2010). Increasing Societal Discomfort About a Dominant Restrictive Planning Discourse on Open Space in Flanders, Belgium. *European Planning Studies, 18*(11), 1787-1804. https://doi.org/10.1080/09654313.2010.512164

Lenard, T. M., & Rubin, P. H. (2010). In Defense of Data: Information and the Costs of Privacy. *Policy & Internet*, *2*(1), 143–177. https://doi.org/10.2202/1944-2866.1035

Lim, C., Kim, K.-J., & Maglio, P. P. (2018). Smart cities with big data: Reference models, challenges, and considerations. *Cities*, *82*, 86–99. https://doi.org/10.1016/j.cities.2018.04.011

Lindqvist, J. (2018). New challenges to personal data processing agreements: Is the GDPR fit to deal with contract, accountability and liability in a world of the Internet of Things? *International Journal of Law and Information Technology*, *26*(1), 45–63. https://doi.org/10.1093/ijlit/eax024

Lingard, H., Hughes, W., & Chinyio, E.A. (1998). The impact of contractor selection method on transaction costs: a review. J*ournal of Construction Procurement, 4*(2), 89-102.

Lipczynski, J., Wilson, J. O., & Goddard, J. A. (2005). *Industrial organization: competition, strategy, policy.* London, England: Pearson Education.

Liu, Z., & Liu, S. (2018). Polycentric Development and the Role of Urban Polycentric Planning in China's Mega Cities: An Examination of Beijing's Metropolitan Area. *Sustainability, 10*(5), 1588. https://doi.org/10.3390/su10051588

Loertscher, S., & Marx, L. M. (2020). Digital monopolies: Privacy protection or price regulation? *International Journal of Industrial Organization*, *71*, 102623. https://doi.org/10.1016/j.ijindorg.2020.102623

Lopes, N.V. (2017). Smart governance: A key factor for smart cities implementation. *Proceedings of the 2017 IEEE International Conference on Smart Grid and Smart Cities, ICSGSC 2017*, 277–282. Retrieved on 26 January 2021 from https://ieeexplore.ieee.org/document/8038591

Lowe, A. (2005). The real life guide to accounting research — A behind-the-scenes view of using qualitative research methods. *The International Journal of Accounting*, *40*(3), 294–298. https://doi.org/10.1016/j.intacc.2005.06.011

Lynskey, O. (2019). Grappling with "Data Power": Normative Nudges from Data Protection and Privacy. *Theoretical Inquiries in Law*, *20*(1), 189–220. https://doi.org/10.1515/til-2019-0007

MacDonald, C. (2012). Understanding participatory action research: A qualitative research methodology option. *Canadian Journal of Action Research, 13*(2), 34–50. https://doi.org/10.33524/cjar.v13i2.37

Marelli, L., & Testa, G. (2018). Scrutinizing the EU General Data Protection Regulation. *Science*, *360*(6388), 496–498. https://doi.org/10.1126/science.aar5419

Marrone, M., & Hammerle, M. (2018). Smart Cities: A Review and Analysis of Stakeholders' Literature. *Business & Information Systems Engineering*, *60*(3), 197–213. https://doi.org/10.1007/s12599-018-0535-3

Martinez-Balleste, A., Perez-martinez, P., & Solanas, A. (2013). The pursuit of citizens' privacy: a privacy-aware smart city is possible. *IEEE Communications Magazine*, *51*(6), 136–141. https://doi.org/10.1109/MCOM.2013.6525606

McCrudden, C. (2004). Using public procurement to achieve social outcomes. *Natural Resources Forum*, *28*(4), 257–267. https://doi.org/10.1111/j.1477-8947.2004.00099.x

Mehregan, M., Jamporazmey, M., Hosseinzadeh, M., & Mehrafrouz, M.. (2011). Application of Fuzzy Analytic Hierarchy Process in Ranking Modern Educational Systems' Success Criteria. *International Journal of E-Education, e-Business, e-Management and e-Learning, 1*(4), 299–304. https://doi.org/10.7763/IJEEEE.2011.V1.49

Meijer, A., & Bolívar, M. P. R. (2016). Governing the smart city: a review of the literature on smart urban governance. *International Review of Administrative Sciences*, *82*(2), 392–408. https://doi.org/10.1177/0020852314564308

Mele, D. (2002). *Not only Stakeholder Interests. The Firm Oriented toward the Common Good*. Notre Dame, IN: University of Notre Dame Press.

Mellahi, K., & Harris, L. C. (2015). Response Rates in Business and Management Research: An Overview of Current Practice and Suggestions for Future Direction. *British Journal of Management, 27*(2), 426-437. https://doi.org/10.1111/1467-8551.12154

Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts. *Academy of management review, 22*(4), 853-886. http://dx.doi.org/10.2307/259247

Moura, H. L., & Teixeira, J. C. (2009). Managing Stakeholders Conflicts. In Chinyio, E., & Olomolaiye, P. (Eds.), *Construction Stakeholder Management*. Hoboken: Blackwell Publishing Ltd. https://doi.org/10.1002/9781444315349.ch17

Mulligan, D. K., & Bamberger, K. A. (2019). Procurement as policy: Administrative process for machine learning. *Berkeley Technology Law Journal*, *34*, 773. http://doi.org/10.2139/ssrn.3464203

Myeong, S., Jung, Y., & Lee, E. (2018). A Study on Determinant Factors in Smart City Development: An Analytic Hierarchy Process Analysis. *Sustainability*, *10*(8), 2606. https://doi.org/10.3390/su10082606

Narayanan, A., Huey, J., & Felten, E. W. (2016). A Precautionary Approach to Big Data Privacy. In S. Gutwirth, R. Leenes, & P. De Hert (Eds.), *Data Protection on the Move* (Vol. 24, pp. 357–385). Springer Netherlands. https://doi.org/10.1007/978-94-017-7376-8_13

Neirotti, P., De Marco, A., Cagliano, A. C., Mangano, G., & Scorrano, F. (2014). Current trends in Smart City initiatives: Some stylised facts. *Cities*, *38*, 25–36. https://doi.org/10.1016/j.cities.2013.12.010

Nikou, S., & Mezei, J. (2013). Evaluation of mobile services and substantial adoption factors with Analytic Hierarchy Process (AHP). *Telecommunications Policy, 37*(10), 915-929. https://doi.org/10.1016/j.telpol.2012.09.007

Ni Loideain, N. (2018). *A Port in the Data-Sharing Storm: The GDPR and the Internet of Things* [King's College London Law School Research Paper No. 2018-27]. Retrieved on 10 April 2019 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3264265

Ni Loideain, N. (2019). A port in the data-sharing storm: the GDPR and the Internet of things. *Journal of Cyber Policy, 4*(2), 178-196. https://doi.org/10.1080/23738871.2019.1635176

Nuccio, M., & Guerzoni, M. (2019). Big data: Hell or heaven? Digital platforms and market power in the data-driven economy. *Competition & Change*, *23*(3), 312–328. https://doi.org/10.1177/1024529418816525

Oderkirk, J., Ronchi, E., & Klazinga, N. (2013). International comparisons of health system performance among OECD countries: Opportunities and data privacy protection challenges. *Health Policy, 112*(1-2), 9-18. https://doi.org/10.1016/j.healthpol.2013.06.006

Oetzel, M. C., & Spiekermann, S. (2014). A systematic methodology for privacy impact assessments: a design science approach. *European Journal of Information Systems*, *23*(2), 126–150. https://doi.org/10.1057/ejis.2013.18

Öjehag-Pettersson, A., & Granberg, M. (2019). Public Procurement as Marketisation: Impacts on Civil Servants and Public Administration in Sweden. *Scandinavian Journal of Public Administration*, *23*(3–4), 43–59.

Onur, I., & Tas, B. K. O. (2019). Optimal bidder participation in public procurement auctions. *International Tax and Public Finance*, *26*(3), 595–617. https://doi.org/10.1007/s10797-018-9515-2

OpenTender.eu (n.d.). *Open Tender All Data – Market Analysis* [Data Portal]. Retrieved on 11 March 2022 from https://opentender.eu/all/dashboards/market-analysis

Organisation for Economic Co-operation and Development. (2010). *Public Procurement in EU Member States – The Regulation of Contract below the EU Thresholds and in Areas Not Covered by the Detailed Rules of The EU Directives* [Sigma Paper 45] Retrieved on 26 January 2021 from https://www.oecd-ilibrary.org/docserver/5km91p7s1mxv-en.pdf?expires=1611649542&id=id&accname=guest&checksum=A3BFD1DFB36505050627F5D93A6CAF9E

Organisation for Economic Co-operation and Development. (2011). *Public procurement: Below threshold contracts* [Brief]. Retrieved on 4 December 2020 from https://www.oecd-ilibrary.org/docserver/5js4vmp1xxd3-en.pdf?expires=1607071841&id=id&accname=oid006084&checksum=536A7D0F9D143D84113988120D4E1A83

Ørngreen, R., & Levinsen, K. T. (2017). Workshops as a Research Methodology. *Electronic Journal of ELearning, 15*(1), 70-81. Retrieved on 27 May 2019 from www.ejel.org/issue/download.html?idArticle=569

Ossadnik, W., Schinke, S., & Kaspar, R. H. (2016). Group Aggregation Techniques for Analytic Hierarchy Process and Analytic Network Process: A Comparative Analysis. *Group Decision and Negotiation*, *25*(2), 421–457. https://doi.org/10.1007/s10726-015-9448-4

Otuoze, A. O., Mustafa, M. W., & Larik, R. M. (2018). Smart grids security challenges: Classification by sources of threats. *Journal of Electrical Systems and Information Technology*, *5*(3), 468–483. https://doi.org/10.1016/j.jesit.2018.01.001

Parker, D., & Hartley, K. (2003). Transaction costs, relational contracting and public private partnerships: A case study of UK defence. *Journal of Purchasing and Supply Management*, *9*(3), 97–108. https://doi.org/10.1016/S0969-7012(02)00035-7

Petersen, O. H., Baekkeskov, E., Potoski, M., & Brown, T. L. (2019). Measuring and Managing Ex Ante Transaction Costs in Public Sector Contracting. *Public Administration Review*, *79*(5), 641–650. https://doi.org/10.1111/puar.13048

Phaal, R., Kerr, C., Ilevabre, I., Farrukh, C., Routley, M., & Athanassopoulou, N. (2016). *On 'self-facilitating' templates for technology and innovation strategy workshops* [Centre for Technology Management working paper No. 8]. Retrieved on 26 August 2019 from https://www.repository.cam.ac.uk/handle/1810/268001

Pöyhönen, M., Hämäläinen, R. P., & Salo, A. A. (1997). An experiment on the numerical modeling of verbal ratio statements. *Journal of Multi-Criteria Decision Analysis*, *6*, 1–10. https://doi.org/10.1002/(SICI)1099-1360(199701)6:1<1::AID-MCDA111>3.0.CO;2-W

Puiu, D., Barnaghi, P., Tönjes, R., Kümper, D., Ali, M. I., Mileo, A., Parreira, J. X., Fischer, M., Kolozali, S., Farajidavar, N., Gao, F., Iggena, T., Pham, T., Nechifor, C., Puschmann, D., & Fernandes, J. (2016). CityPulse: Large Scale Data Analytics Framework for Smart Cities. *IEEE Access*, *4*, 1086–1108. https://doi.org/10.1109/ACCESS.2016.2541999

Ramanathan, R., & Ganesh, L. S. (1995). Energy resource allocation incorporating qualitative and quantitative criteria: An integrated model using goal programming and AHP. *Socio-Economic Planning Sciences*, *29*(3), 197–218. https://doi.org/10.1016/0038-0121(95)00013-C

Ranchordas, S., & Goanta, C. (2020). The New City Regulators: Platform and Public Values in Smart and Sharing Cities. *Computer Law & Security Review*, *36*, 105375. https://doi.org/10.1016/j.clsr.2019.105375

Ritala, P., Agouridas, V., Assimakopoulos, D., & Gies, O. (2013). Value creation and capture mechanisms in innovation ecosystems: A comparative case study. *International Journal of Technology Management*, *63*(3/4), 244. https://doi.org/10.1504/IJTM.2013.056900

Romanou, A. (2018). The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. *Computer Law & Security Review*, *34*(1), 99–110. https://doi.org/10.1016/j.clsr.2017.05.021

Regulation (EU) 2016/679 of the European Parliament and of the Council 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, Vol. L119 (4 May 2016), pp. 1-88. Retrieved on 8 April 2019 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

Reynaert, I. (2018). *Belgian providers of smart cities technologies and services* [Slideshow]. Retrieved on 16 January 2019 from https://www.agoria.be/upload/enewsv7/Agoria%20Belgian%20providers%20smart%20cities%2010-2018.pdf

Robert, J., Kubler, S., Kolbe, N., Cerioni, A., Gastaud, E., & Främling, K. (2017). Open IoT Ecosystem for Enhanced Interoperability in Smart Cities—Example of Métropole De Lyon. *Sensors*, *17*(12), 2849. https://doi.org/10.3390/s17122849

Roloff, J. (2008). Learning from Multi-Stakeholder Networks: Issue-Focussed Stakeholder Management. *Journal of Business Ethics*, *82*(1), 233–250. https://doi.org/10.1007/s10551-007-9573-3

Ruhlandt, R. W. S. (2018). The governance of smart cities: A systematic literature review. *Cities*, *81*, 1–23. https://doi.org/10.1016/j.cities.2018.02.014

Ruijer, E., Grimmelikhuijsen, S., & Meijer, A. (2017). Open data for democracy: Developing a theoretical framework for open data use. *Government Information Quarterly*, *34*(1), 45–52. https://doi.org/10.1016/j.giq.2017.01.001

Ryz, L., & Grest, L. (2016). A new era in data protection. *Computer Fraud & Security*, *2016*(3), 18–20. https://doi.org/10.1016/S1361-3723(16)30028-8

Saaty, T. (1980). *The Analytic Hierarchy Process.* New York, NY: McGraw-Hill.

Saaty, T. (2008). Decision Making with the Analytic Hierarchy Process. *International Journal of Services Sciences, 1*(1), 83. https://doi.org/10.1504/IJSSCI.2008.017590.

Saaty, T., & Tran, L. (2007). On the Invalidity of Fuzzifying Numerical Judgments in the Analytic Hierarchy Process. *Mathematical and Computer Modelling, 46*(7), 962–975. https://doi.org/10.1016/j.mcm.2007.03.022.

Sambasivan, M., & Fei, N. Y. (2008). Evaluation of critical success factors of implementation of ISO 14001 using analytic hierarchy process (AHP): a case study from Malaysia. *Journal of Cleaner Production, 16*(13), 1424-1433. https://doi.org/10.1016/j.jclepro.2007.08.003.

Satariano, A. (2020, 27 April). Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates. *The New York Times*. Retrieved on 11 January 2021 from https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html

Scott, J. (2014). Extraterritoriality and Territorial Extension in EU Law. *The American Journal of Comparative Law, 62*(1), 87–126. https://doi.org/10.5131/AJCL.2013.0009

Screen Flanders. (n.d.). *The Flanders region* [Website]. Retrieved on 25 May 2019 from https://www.screenflanders.be/en/film-commission/production-guide/facts-and-figures/the-flanders-region

Seawright, J., & Gerring, J. (2008). Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options. *Political Research Quarterly, 61*(2) 294–308. https://doi.org/10.1177/1065912907313077.

Seo, J., Kim, K., Park, M., Park, M., & Lee, K. (2018). An Analysis of Economic Impact on IoT Industry under GDPR. *Mobile Information Systems, 2018*. https://doi.org/10.1155/2018/6792028

Shahin, A., & Mahbod, A. (2007). Prioritization of Key Performance Indicators: An Integration of Analytical Hierarchy Process and Goal Setting. *International Journal of Productivity and Performance Management, 56*(3), 226–240. https://doi.org/10.1108/17410400710731437.

Shelton, T., Zook, M., & Wiig, A. (2015). The 'actually existing smart city'. *Cambridge Journal of Regions, Economy and Society, 8*(1), 13–25. https://doi.org/10.1093/cjres/rsu026

Smart Cities Flanders. (n.d.). *Over Smart Cities Vlaanderen* [Website]. Retrieved on 13 December 2018 from https://www.smartcities.vlaanderen/over/

Smart City Institute. (2018). *Barometer 2018: Smart Cities in België* [report]. Retrieved on 9 January 2019 from https://orbi.uliege.be/bitstream/2268/225025/1/Belgische%20Barometer%202018%20Smart%20Cities%20NL.pdf

Smith, V., & Walker, J. (1993). Monetary Rewards and Decision Cost in Experimental Economics. *Economic Inquiry, 31*(2), 245–261. https://doi.org/10.1111/j.1465-7295.1993.tb00881.x

Song, D., Shi, E., Fischer, I., & Shankar, U. (2012). Cloud Data Protection for the Masses. *Computer, 45*(1), 39-45. https://doi.org/10.1109/MC.2012.1

Statacorp. (2009). Stata IC: Data Analysis and Statistical Software, Release 16.

Statbel. (2019). *Structuur van de bevolking* [Website]. Retrieved on 25 May 2019 from https://statbel.fgov.be/nl/themas/bevolking/structuur-van-de-bevolking#figures

Stentoft Arlbjørn, J., & Vagn Freytag, P. (2012). Public procurement vs private purchasing: Is there any foundation for comparing and learning across the sectors? *International Journal of Public Sector Management*, *25*(3), 203–220. https://doi.org/10.1108/09513551211226539

Stolton, S. (2020, 25 May). GDPR enforcement held back by lack of resources, report says. *EURACTIV.* Retrieved on 11 January 2021 from https://www.euractiv.com/section/data-protection/news/gdpr-enforcement-held-back-by-lack-of-resources-report-says/

Størkersen, K. V., Antonsen, S., & Kongsvik, T. (2017). One size fits all? Safety management regulation of ship accidents and personal injuries. *Journal of Risk Research*, *20*(9), 1154–1172. https://doi.org/10.1080/13669877.2016.1147487

Stucke, M. E., & Ezrachi, A. (2016). When Competition Fails to Optimize Quality: A Look at Search Engines. *Yale Journal of Law and Technology*, *18*, 70–110.

Sustainable Development Flanders. (n.d.). *Smart Cities Barometer* [Website]. Retrieved on 11 June 2021 from https://do.vlaanderen.be/smart-cities-barometer

Talari, S., Shafie-khah, M., Siano, P., Loia, V., Tommasetti, A., & Catalão, J. P. S. (2017). A Review of Smart Cities Based on the Internet of Things Concept. *Energies*, *10*(4), 421. https://doi.org/10.3390/en10040421

Tancock, D., Pearson, S., & Charlesworth, A. (2010). Analysis of Privacy Impact Assessments within Major jurisdictions. *2010 Eighth International Conference on Privacy, Security and Trust*, 118–125. https://doi.org/10.1109/PST.2010.5593260

Telgen, J., Harland, C., & Knight, L. (2007). Public procurement in perspective. In L. Knight, C. Harland, J. Telgen, K. V. Thai, G. Callender, & K. McKen (Eds.), *Public Procurement: International cases and commentary* (pp. 16-24). Routledge. https://doi.org/10.4324/9780203815250-9

Tempels, B., Verbeek, T., Pisman, A., & Allaert, G. (2012). *Verstedelijking in de Vlaamse open ruimte: een vergelijkende studie naar vijf transformaties.* Heverlee, Belgium: Steunpunt Ruimte en Wonen.

Thompson, N., Ravindran, R., & Nicosia, S. (2015). Government data does not mean data governance: Lessons learned from a public sector application audit. *Government Information Quarterly*, *32*(3), 316–322. https://doi.org/10.1016/j.giq.2015.05.001

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134–153. https://doi.org/10.1016/j.clsr.2017.05.015

Todde, M., Beltrame, M., Marceglia, S., & Spagno, C. (2020). Methodology and workflow to perform the Data Protection Impact Assessment in healthcare information systems. *Informatics in Medicine Unlocked*, *19*, 100361. https://doi.org/10.1016/j.imu.2020.100361

Tombal, T. (2020). *GDPR as shield to a data sharing remedy* [SSRN Scholarly Paper]. Retrieved on 9 October 2020 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3516718

Trudel, P. (2009). Privacy Protection on the Internet: Risk Management and Networked Normativity. In Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (Eds.), *Reinventing Data Protection?* Dordrecht, The Netherlands: Springer. https://doi.org/10.1007/978-1-4020-9498-9_19

Tucker, C. (2019). Digital Data, Platforms and the Usual [Antitrust] Suspects: Network Effects, Switching Costs, Essential Facility. *Review of Industrial Organization*, *54*(4), 683–694. https://doi.org/10.1007/s11151-019-09693-7

Urquhart, L., Lodge, T., & Crabtree, A. (2019). Demonstrably doing accountability in the Internet of Things. *International Journal of Law and Information Technology*, *27*(1), 1–27. https://doi.org/10.1093/ijlit/eay015

Van Alsenoy, B. (2019). *Data protection law in the EU : roles, responsibilities and liability*. Cambridge, United Kingdom: Intersentia.

Van der Haak, M., Wolff, A. C., Brandner, R., Drings, P.,Wannenmacher, M., & Wetter, T. (2003). Data Security and Protection in Cross-Institutional Electronic Patient Records. *International Journal of Medical Informatics, 70*(2), 117–130. https://doi.org/10.1016/S1386-5056(03)00033-9

Vandercruysse, L., Buts, C., & Dooms, M. (2019). Data Control in Smart City Services: Pitfalls and How to Resolve Them. *European Data Protection Law Review, 5*(4), 554–560. https://doi.org/10.21552/edpl/2019/4/16

Vandercruysse, L., Buts, C., & Dooms, M. (2020). A Typology of Smart City Services: The Case of Data Protection Impact Assessment. *Cities, 104*, 102731. https://doi.org/10.1016/j.cities.2020.102731

Vandercruysse, L., Buts, C., & Dooms, M. (Sep. 4, 2021). Public procurement of smart city services: The anticompetitive effect of the GDPR [Conference paper]. *15th International Conference on Competition and Regulation (CRESSE): Advances in the Analysis of Competition Policy and Regulation.*

van Dijk, N., Gellert, R., & Rommetveit, K. (2016). A risk to a right? Beyond data protection risk assessments. *Computer Law & Security Review*, *32*(2), 286–306. https://doi.org/10.1016/j.clsr.2015.12.017

van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3), 472–480. https://doi.org/10.1016/j.giq.2016.06.004

Veale, M., Binns, R., & Ausloos, J. (2018). When data protection by design and data subject rights clash. *International Data Privacy Law*, *8*(2), 105–123. https://doi.org/10.1093/idpl/ipy002

Voss, W. G. (2016). European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting. *The Business Lawyer*, *72*(1), 221–234.

Walravens, N., & Ballon, P. (2013). Platform business models for smart cities: from control and value to governance and public value. *IEEE Communications Magazine*, *51*(6), 72–79. https://doi.org/10.1109/MCOM.2013.6525598

Wang, Y.-M., & Luo, Y. (2009). On rank reversal in decision analysis. *Mathematical and Computer Modelling*, *49*(5), 1221–1229. https://doi.org/10.1016/j.mcm.2008.06.019

Wedley, W. C. (1993). Consistency prediction for incomplete AHP matrices. *Mathematical and Computer Modelling*, *17*(4), 151–161. https://doi.org/10.1016/0895-7177(93)90183-Y

Williamson, O. E. (1975). *Markets and hierarchies: Analysis and antitrust implications: A study in the economics of internal organization*. New York, NY: Free press.

Williamson, O. E. (2007). *Transaction Cost Economics: An Introduction* [SSRN Scholarly Paper]. Retrieved on 20 April 2021 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1691869

Wooldridge, J. M. (2015). *Introductory Econometrics: A Modern Approach*. Mason, OH: Cengage Learning.

Wright, D. (2012). The state of the art in privacy impact assessment. *Computer Law & Security Review*, *28*(1), 54–61. https://doi.org/10.1016/j.clsr.2011.11.007

Wright, D. (2013). Making Privacy Impact Assessment More Effective. *The Information Society*, *29*(5), 307–315. https://doi.org/10.1080/01972243.2013.825687

Wright, D., Finn, R., & Rodrigues, R. (2013). A Comparative Analysis of Privacy Impact Assessment in Six Countries. *Journal of Contemporary European Research*, *9*(1), Article 1. https://www.jcer.net/index.php/jcer/article/view/513

Wright, D., & Raab, C. D. (2012). Constructing a surveillance impact assessment. *Computer Law & Security Review*, *28*(6), 613–626. https://doi.org/10.1016/j.clsr.2012.09.003

Yeh, H. (2017). The effects of successful ICT-based smart city services: From citizens' perspectives. *Government Information Quarterly*, *34*(3), 556–565. https://doi.org/10.1016/j.giq.2017.05.001

Zerlang, J. (2017). GDPR: A milestone in convergence for cyber-security and compliance. *Network Security*, *2017*(6), 8–11. https://doi.org/10.1016/S1353-4858(17)30060-0

Appendices

Appendix 1

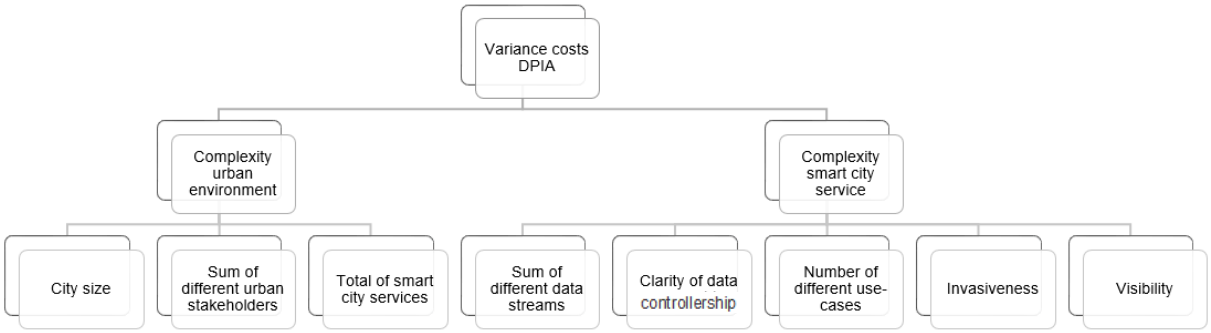

Figure A.1. Code tree. Source: own creation based on the interviews.

Appendix 2

Question #	Formulation
1	How many and which SC services are provided in your city/ do you provide?
2	How much experience do you have with performing DPIAs?
3	How is decided whether or not a data processing activity will be subject to a DPIA?
4	How is decided whether to perform the DPIA in-house or to outsource it to an external partner?
5	What is the scope of the DPIA that is performed?
6	Is the DPIA process adapted to the actual SC service (e.g. extended Vs. succinct)?
7	How confident are you that if you perform a DPIA on a certain SC service, the SC service will eventually be implemented (and thus the residual risks will not be found too large)?
8	What are in your opinion the most important criteria for a DPIA?
9	Can you rank these criteria from more important to less important and explain why?

Table A.2. Semi-structured interview guide. Source: own creation.

Score AHP	Meaning
1	You attribute equal weight to the choice on the left and the choice on the right
3	You slightly prefer the choice on the right over the choice on the left
5	You prefer the choice on the right over the choice on the left
7	You strongly prefer the choice on the right over the choice on the left
9	You very strongly prefer the choice on the right over the choice on the left
Note: these score were recalibrated from an originally balanced scale. Balanced scales are preferred for the purposes of directly comparing two alternatives (Pöyhönen, Hämäläinen & Salo, 1997).	

Table A.3. Explanation scoring AHP-survey. Source: own creation based on Saaty (1980).

Appendix 3

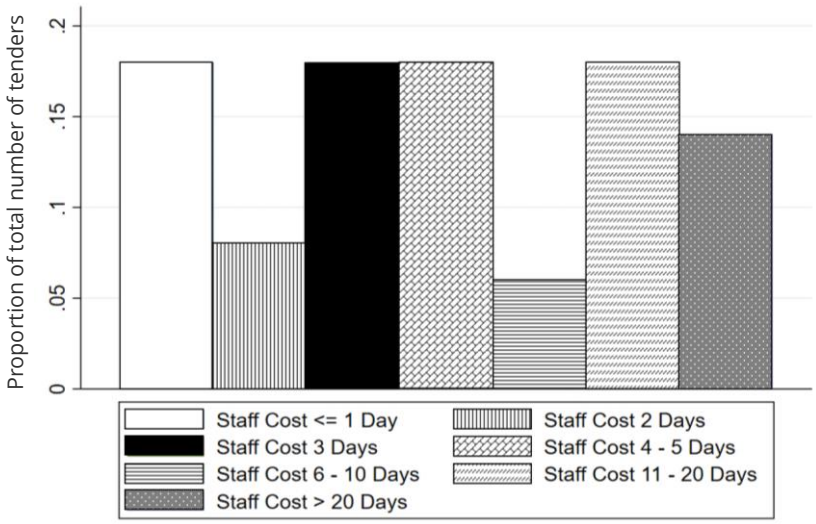

Figure A.4. Overview size of SCS tender data protection staff cost (n=50).

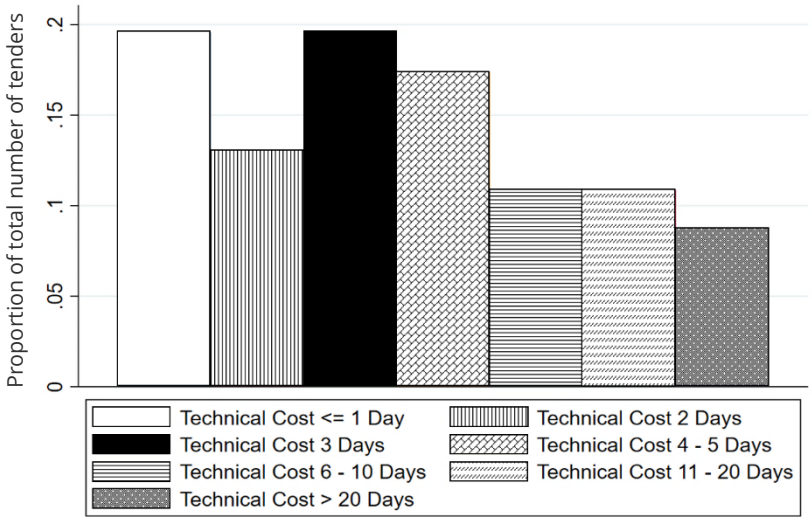

Figure A.5. Overview size of SCS tender data protection technical cost (n=46).

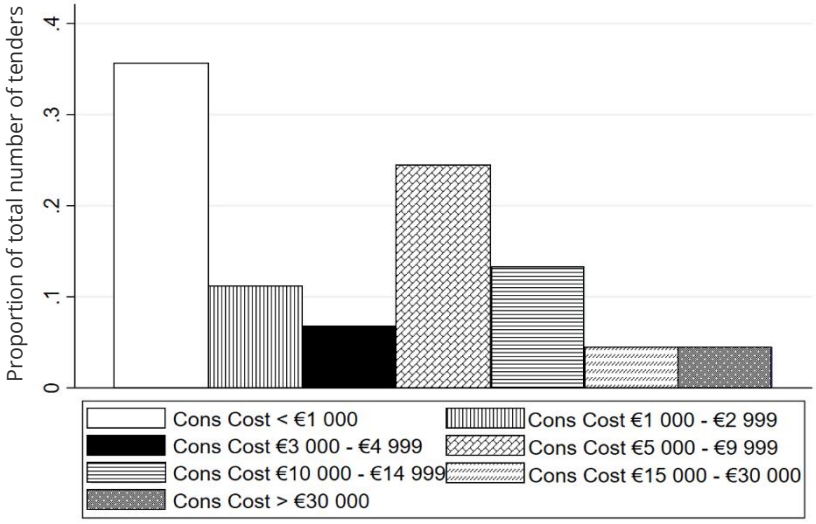

Figure A.6. Overview size of SCS tender data protection consulting cost (n=45).


VUB
VRIJE
UNIVERSITEIT
BRUSSEL


SPECTRE