The Perceived Impact of GDPR Readiness, Privacy Protection Tools, and Control Mechanisms on the Evolution of European Urban Data Platforms

Master thesis
Business Information Management
RSM – Erasmus Universiteit

Daniel Bos
374806

Supervisors RSM:
Coach: E. van Heck
Co-reader: Zike Cao

Supervisor organization:
Municipality of Rotterdam
Point of Contact: Jaap Dekker

Point of contact KPN:
Roland van Ravenstein

Date: 15-06-2018

Preface

The copyright of the master thesis rests with the author. The author is responsible for its contents. RSM is only responsible for the educational coaching and cannot be held liable for the content.

Acknowledgements

With the writing of this master thesis, the final chapter of my six years of studies at the Rotterdam School of Management has started. I have developed myself both academically as personally via the various courses, extra-curricular activities, an exchange, an internship and various side-jobs. This all together gave me the inspiration to write my thesis in the field of smart cities. The thesis trajectory was something that I did not look forward to, but in the end, I can say that is has been a valuable project for me. I have learned many things while writing this thesis and I could not have done this without certain people. Therefore, I would like to thank those persons:

First of all, I would like to thank my coach, Prof. van Heck, for guiding me through this trajectory. The knowledge that you shared with me on the topic of platform ecosystems steered me in the right direction while writing this thesis. The multiple meetings that we had when I got stuck in the amount of work helped me to gain confidence and work harder to be able to make this thesis something that is of academic value. Furthermore, I would like to thank Prof. van Oosterhout for providing me with this topic and the continuous guidance throughout the trajectory. With the meetings regarding the questionnaire and developments you made it possible to stay on schedule and to gain valuable insights. Zike Cao as my co-reader gave me the freedom to write my thesis and assisted when needed with some interesting perspectives that I had not thought of.

Finding the right cases for this study was not the easiest part. Therefore, I would like to thank Jaap Dekker from the city of Rotterdam for connecting me to the participating cities and interviewees. Moreover, I would like to thank the interviewees for their time and contributions.

Lastly, I would like to thank my parents for providing me with the opportunity to study at this university. Without your inspiration, the finalizing of my studies might not have been possible. My respect for your academic and work achievements is immense.

Executive Summary

Rotterdam is part of the European smart city project Ruggedised. This project is meant to accelerate the path towards a sustainable future by creating model urban areas. Within those urban areas, data will be collected and shared with data from third parties via an urban data platform. With those platforms, ICT, e-mobility and energy solutions can be combined to design smart and resilient cities. Focus will be the perceived impact of the new GDPR regulations on such an urban data platform. The goal is to guide the city of Rotterdam in their choices regarding the governance and privacy of the platform in order to create a positive effect on the evolution of the platform.

Tiwana's book (2014) on platform ecosystems has been used as the guidebook for this study and several variables from his work have been adopted. There is not much literature available on smart cities and GDPR. However, all over Europe smart cities are popping up and they are all facing the upcoming GDPR regulations. Therefore, a questionnaire and a multiple-case study have been performed, as that would fit an exploratory study. With the usage of the variables GDPR readiness, privacy protection tools, and control mechanisms, the effect on the dependent variable, the short-term evolution of a platform, has been studied. The metrics that are part of the short-term evolution are resilience, scalability, and composability. Propositions regarding these variables have been scrutinized and resulting findings have been presented.

Firstly, a high level of GDPR readiness positively influences the evolution of a platform. During the interviews, it became clear that the general opinion was that GDPR compliancy will help a platform flourish. This is both for the reason that it prevents smart cities of getting fines from the AP, but it also makes sure that they obtain a certain level of trust from the citizens which allows them to let their platform evolve.

Secondly, the use of privacy protection tools ensures a certain level of trust from citizens, which in the end leads to a positive effect on the evolution of a platform. When people feel that the city and its platform are to be trusted, they are more eager to join the platform. Eventually this will lead to a higher scalability and therefore has a positive effect on the short-term evolution of a platform.

Lastly, the use of control mechanisms has proven to create a higher degree of privacy and GDPR readiness and therefore, they positively moderate the effect between one of those and the short-term evolution of a platform. What came out of the interviews, was the fact that they often used gatekeeping to ensure a certain level of GDPR compliancy and privacy.

These findings bring relevant contributions to existing theory, as they not only validate existing research but also show new findings which give directions for future research and give valuable insights to the platform owners of urban data platforms. They can compare their platforms to the other urban data platforms that have been discussed so that they can critically assess, and where needed adapt, their own management and governance. In the end this should lead to a positive evolution of their urban data platform.

Inhoudsopgave

List of figures

List of Tables

1. Introduction

1.1. Social relevance

In the time that we currently live in, technology has become a main part of our lives. Most of the people have a smartphone, tablet, smartwatch, laptop or otherwise. Even our household attributes are being made with more and more technology. This means that there is an increasing number of connected devices. Combined with that, the world population keeps growing and it is expected that there will be 9,8 billion people on earth in 2050 (UN News Centre, 2017). With that growing population, cities have also been growing fast in the 21st century, due to the opportunities for working people and availability of good resources. Those cities can be productive, but on the other hand, it presents challenges for governments to keep up with the growing population. The demand for services has increased and there is a new form of competition between cities due to of globalization (Harrison, 2011). These developments lead to experiments with new ideas in terms of governance, infrastructure, sustainability etc. This means that governments need to design new strategies to prevail city performance. What results from this is the idea of a smart city that makes use of all these before mentioned connected devices and becomes more sustainable whilst being more efficient. A smart city can be described as a city that integrates and monitors conditions of all the critical infrastructures, organizes the resources in the city better, monitors the security aspects and maximizes services for its citizens (Giffinger et al., 2007).

All the data that comes available from those connected devices will be analysed and monitored. This will allow the city to increase efficiency, improve healthcare services, implement smart energy management and develop new business models for transportation (Berrone, 2016). There are already some cities that have been implementing these new ways of running the city. Some of them, like San Diego and San Francisco can be seen as forerunners. These examples give other cities guidelines on how to build their urban data platforms and thereby become smarter. Most cities and companies however, struggle to realize economic benefits from all the data that is gathered. This can partially be explained because there has never been a general framework to guide the implementation of an open data strategy. Berrone (2016) discusses the example of Barcelona where the initiative of an open data strategy has been implemented which can be seen as a success story that can offer lessons for governments and companies in the process of the implementation of open data initiatives.

1.2. Platform ecosystems

The architecture of a smart city can be compared with the architecture of a platform ecosystem, and there are many aspects that can be copied from a platform ecosystem when building a smart city. Therefore, it is good to study the key principles of a platform. A platform consists of two major elements: the platform and its complementary apps. Other core elements are its ecosystem, the interfaces, and the architecture (Tiwana, 2014, p. 7). With the implementation of an urban data platform, you would like to know if the platform is a success. To be able to measure that level of success, it is wise to take a look at the evolution of the platform. The evolution can be divided into three phases: short-term, mid-term, and long-term. In this study, the focus will be on the short-term evolution. Furthermore, the governance of a platform is of great importance. Platform governance encompasses three dimensions of which one of them will be discussed thoroughly: control mechanisms. The platform owner creates control through mechanisms so that he is able to implement and enforce certain rules that will reward desirable behaviour, promulgate standard behaviour, and punish bad behaviour (Evans et al. 2007). These mechanisms can play a part in the GDPR readiness of the urban data platform, which will be discussed later on.

1.3. Privacy

Whilst developing those smart city models, there are several aspects that need to be taken into consideration. These include costs, the sustainability of certain ideas, the ease of usage and the security of the businesses and citizens and their data. Data security and data privacy are topics that have gained more attention over the last couple of years. The more connected devices we have, the more data there will be available. This data needs to be secured, but it could also harm the privacy of citizens and businesses. The danger in all these connected devices lies in the fact that the government or private businesses can follow every movement of citizens and use it for various purposes. The reason could be to help people get more out of their lives, but not everyone might be willing to share everything and they have the right to decide that for themselves.

1.4. GDPR

This is one of the reasons that the new GDPR regulations have been drawn up. The GDPR, which will be discussed thoroughly later on, are the regulations from the EU that have been designed to protect and empower the data privacy of all EU citizens (GDPR Portal, 2017). This leads back to the smart cities. As discussed before there will be lots of data that needs to be analysed and monitored. That data will be floating around freely available for various stakeholders. This can be public data, but can also cover personal, sensitive data. This causes certain risks that need to be taken care of. Citizens need to know that their data is well protected and secured and that not everyone can easily get access to that data. A Data Protection Officer need to be installed at organisations that have processing operations that require regular monitoring of data subjects on a large scale (GDPR Portal, 2017). Furthermore, topics as privacy by design, breach notification, data registers, and Privacy Impact Assessments are part of GDPR. Only if these new regulations have been taken care of, the implementation of a smart city business model can be possible.

Therefore, it would be smart to take a closer look at the impact of GDPR on the previously mentioned evolution of a platform ecosystem. The degree of GDPR readiness could influence that evolution and it would be wise to take that into account.

1.5. Thesis structure

To be able to study the abovementioned scope, there needs to be a research object that falls under the GDPR regulations and can be seen as a smart city project. This will be the Ruggedised project, which is a smart city lighthouse project under the European Union’s Horizon 2020 research and innovation program. We will take a closer look at the Ruggedised project in chapter 2. Rotterdam is one of those lighthouse cities in the project, and will be used as a research object in this study. In chapter 3, existing literature about smart cities, platform ecosystems, privacy, and GDPR will be discussed in order to shape a conceptual framework. Following from that comes chapter 4, which consists of the methodology that will be used in this study. This methodology will consist of a survey that has been sent out to smart city projects all over Europe and a multiple in-depth case study.

In the end, this study will have done exploratory research about the GDPR readiness of parties within an urban data platform to be able to find out if that influences the short-term evolution of that urban data platform. and the relevance of GDPR in the implementation of an urban data platform. With those findings, recommendations will be given to the municipality of Rotterdam in order to provide them with some guidelines on how to get the most out of their urban data platform without harming its citizens. This will include managerial implications, limitations of this study, and directions for future research on this topic.

2. Ruggedised project

The topic of this thesis is the subtopic of a project in collaboration with the 'Gemeente Rotterdam': The Ruggedised EU project. This is a smart city project that brings together three lighthouse cities: Rotterdam, Glasgow and Umeå. The European Commission defines a smart city as: "*A place where the traditional networks and services are made more efficient with the use of digital and telecommunication technologies, for the benefit of its inhabitants and businesses*" (Ruggedised, 2017). There are three other cities which can be seen as the follower cities. These are Brno, Gdansk and Parma. If the implemented models in the lighthouse cities work well, they can be implemented in the follower cities or they can be reshaped because some aspects were not needed or needed alteration. The Ruggedised project will test and implement smart solutions which include: ICT, E-mobility and Energy solutions. These smart solutions are meant to improve the quality of life for citizens, reduce the environmental consequences of certain activities and to create a stimulating environment for a sustainable economic. In the end, the goal is to create urban data platforms.

This thesis will be focusing on the city of Rotterdam and will discuss one out of eight subtopics that have been designed around the Ruggedised project. These subjects are designed by the municipality of Rotterdam in collaboration with companies that can play a role in certain parts of the project. The general topic will be: the perceived impact of GDPR on urban data platforms. If Rotterdam wants to become a smart city and respond to changes like big data, robotics and sensor techniques, data security and data privacy are important aspects in making this project work. Not every piece of information can be available for the businesses and/or government that are building this smart city model. Without a good plan and risk analysis, the AP could fine the city of Rotterdam and slow down the implementation of the urban data platform. Furthermore, the citizens of Rotterdam could feel like their privacy will be breached and therefore might not support the initiative of the Ruggedised project, which gives the city of Rotterdam a bad image.

That relates to the main reason why this is such an upcoming and important topic. This year, on the 25th of May, the EU General Data Protection Regulation will be implemented. This is the biggest change in data privacy regulation over the last 20 years and the aim of the GDPR is to protect the privacy of EU all citizens and contain data breaches in an increasingly data-driven world. This includes that breach notification will become mandatory when a breach is likely to result in a risk for the rights of individuals (GDPR Portal, 2017).

Smart city initiatives like the Ruggedised project might not be as well prepared for GDPR as they should be. This could hinder the implementation of the urban data platform. Think about all the data that is being gathered from citizens right now like cameras above highways etc. These concepts should all be reconsidered to check if they are compliant with the new regulations. That level of GDPR readiness could influence the evolution of an urban data platform as this could stand in the way of implementing certain aspects of the urban data platform.

3. Research Question and Objective

3.1. Research Question and Objective

The overall goal regarding data security and privacy in the Ruggedised project is to find out how all the data of businesses, the municipality, and the citizens can be safeguarded when it can be used as open data to be analysed and monitored (Berrone, 2016). However though, this would be too big of a scope for this study. Therefore, we will scope it down to the later on designed research question. Data security and data privacy are uprising topics and citizens and businesses are worried about what will happen with all their personal and company data. For that reason, the European Union has designed the GDPR to protect and empower all EU citizens' data privacy. The implementation of the GDPR will have great consequences for companies and initiatives of smart cities, as the GDPR determines how personal data has to be collected, processed and saved (GDPR, 2017). With the addition of the GDPR, the goal of this study can be redefined to: the perceived impact of GDPR on an urban data platform. To link this to academic work and to further scope it down, Platform Ecosystems by Tiwana (2014) will be used. He describes three phases to measure the evolution of a platform: short-term, mid-term, and long-term. As the GDPR still has to be implemented when writing this thesis, the short-term metrics will be used to measure the evolution of an urban data platform.

These findings are necessary to be able to proceed with the project, because if you want to have a more efficient urban governance, the adoption of a data management scheme including the protection of the data which is in line with EU rules, is necessary (Green Digital Chapter, 2017). The implemented GDPR will make sure that the privacy of European citizens is protected, but it is not sure what the impact will be on an urban data platform. Concluding out of that comes the research question:

"What is the perceived impact of GDPR on the short-term evolution of an urban data platform?"

This study will look into the new GDPR regulations that will be implemented in May 2018. It will also take a closer look at certain privacy concerns and challenges those smart cities will be facing. The question that has risen in previous privacy studies is which data is for public usage and what would be a right privacy framework for that? This involves the concerns of citizens about their privacy in smart cities that Van Zoonen et al. (2016) wrote about. Those concerns are related to the pace of evolution of an urban data platform as privacy concerns from citizens can influence the pace of implementation of certain aspects from the urban data platform. Therefore, it would be good to study the effect of the GDPR on the short-term evolution of an urban data platform. Furthermore, the moderating effect of control mechanisms on the relationship between GDPR readiness and the short-term evolution will be researched. By doing this, conclusions can be drawn on the kind of effect those two have and what possible recommendations would be.

3.2. Relevance

The concept of platform ecosystems and smart cities are still quite new subjects in academic literature. There are various articles about the different aspects of a smart city and there are also some cases available about cities that have already implemented smart urban data platforms, but it is not extensive. The relevance of this subject is that the GDPR will be implemented in May 2018 and therefore, data security and privacy have become important aspects of the smart city. This is due to the fact that there could be regulations that smart cities initiatives did not foresee when starting their projects, which could cause difficulties in the implementation of an urban data platform. Some data might be available for the public, but critical personal information is not to be seen by everyone. As the number of connected devices is increasing, there is more data being shared. This data also includes personal data, and according to the new GDPR, this cannot be handled like it used to be. This is something, that combined with a better data security, is an uprising topic in current literature but also in the corporate world.

4. Theoretical background

This chapter will describe the fundamental concepts of the research objective. To get a clear image what will be discussed as the research object, the concept of smart cities will first be reviewed. Thereafter, the concept of platform ecosystems will be discussed and the reason why smart cities fit in that concept. Subjects like governance, the evolution of platform ecosystems, privacy, and GDPR will all be reviewed. Furthermore, a conceptual framework for this study will be designed and discussed.

4.1. Smart cities

The need to balance the social development, the economic growth and the sustainability of the world is the main reason that governments all over the world are interested in the concept of smart cities. The main focus within those projects is to improve the energy use, healthcare, education and transportation. For those services, a strategy needs to be designed in order to integrate them into an urban model (Letaifa, 2015).

It is hard to distinguish the difference between a creative, intelligent, wired or smart city. Smart cities are both creative and intelligent. It offers a balanced centricity among institutions, people and technology (Letaifa, 2015). There has been a shift that went from wired to smart-er cities. With wired cities, the idea exists that technology should be the main focus and that that can automatically transform and improve cities (Allwinkle et al, 2011). The idea of a smart city however, is that cities should always start with its people and the human capital, rather than blindly believing in technology. For Hollands, the critical factor in a smart city is the citizens and how they interact (Hollands, 2008). Hollands says in his article that the key elements of a smart city relate to networked infrastructures as a means to enable economic, social, environmental, and cultural development.

Then there is the difference between intelligent and smart cities. Intelligent cities have been around for a while already and are now transforming into smart cities (Allwinkle et al, 2011). With intelligent cities, the focus lies on innovation and the promotion of services, while the focus in smart cities lies on application and serving as a platform for the community which is in line with the thoughts of Hollands.

An example of serving as a platform for the community can be found in the agriculture sector. The connected cow is an Internet of Things example where sensors are placed on certain parts of cows’ bodies (Fildes, 2017). The goal here is to help increase the productivity of the herd. Birth-related complications can be prevented as the sensors tell the farmer for example if the cow is walking too much or too little.

There have been several approaches to implement those platforms for smart cities. They are generally designed with efficiency in mind though. This means that the implemented technologies will displace jobs, while it should be the purpose to create jobs and thereby even new industries. Furthermore, the purpose should be to improve the quality of life of citizens. There is some lack of sensitivity which causes one big issue: a city is nothing without its citizens (Mulligan, 2013).

Those citizens should not be left out, because in the end they decide what happens with the city. In Rotterdam, a lot of data is already being monitored and analysed. This includes data from city registers, data from government and data from social media. Local governments make these data available to the public sometimes. With this comes the question who has legitimate access, which data is for public usage and what would be the right privacy framework. This is part of the debate that people’s concerns about their privacy in those smart cities should not be forgotten because this involves their support and participation (van Zoonen, 2016).

4.2. Platform ecosystems

The architecture of platform ecosystems can be compared with the architecture of modern cities (Tiwana, 2014, p. 94). Therefore, the concept of platform ecosystems will be discussed and the way that Rotterdam as a smart city can act as a platform ecosystem. Tiwana describes the concept of a platform ecosystem in his book and covers important areas of research which makes it a good guidebook for this study.

The focus of this study will be software based platform ecosystems, as the overarching goal of the previously mentioned Ruggedised project is to make Rotterdam a smarter city. A software platform is a platform that will serve as a foundation on which other parties can build their complementary products or services. The party that is responsible for the platform, is called the platform owner. In this case, that will be a sort of co-ownership between the city of Rotterdam and KPN. But that ownership can also be solely held by one person.

Platform ecosystems consist of two major elements: the platform and the complementary apps. The platform consists of the enabling core technologies and shared infrastructure, which the apps can leverage. Companies build on those functionalities of the platform through a set of interfaces which allows them to communicate and interoperate with the platform (Tiwana, 2014, p. 6). The platform can also be divided into two parts: the upstream and the downstream part. The upstream part is what goes into the platform, such as hardware suppliers, manufacturing partners and network connectivity partners. The downstream part consists of the platform complement producers. These are the app developers and end-users. That makes the apps downstream complements for the platform. The downstream part of the platform is the most important part. This is because the attractiveness of the platform does not come from the platform itself, but from what end-users can do with it. The fate and survival of a platform therefore depend on the downstream ecosystem (Tiwana, 2014, p. 7). This is the reason that the focus lies on the downstream part of the platform.

Platforms have been uprising over the last couple of years. The main reason for that are five drivers which enable the migration towards platforms. Those drivers are: deepening specialization within industries, the packetization of products, services, software embedding, Internet of Things, and ubiquity. These five drivers can be found in the figure below.

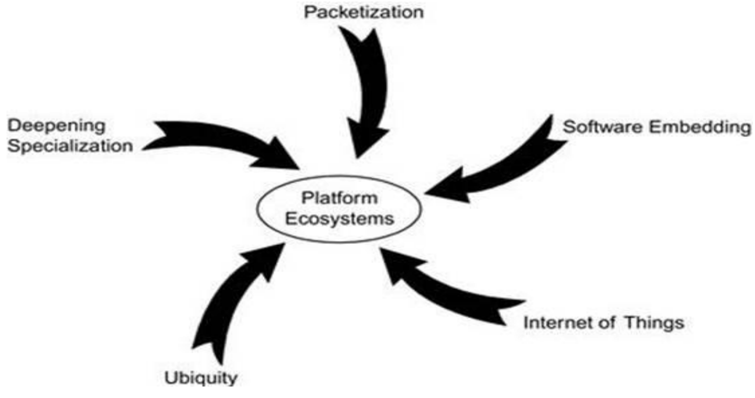


Figure 1: five drivers of the migration towards platform ecosystems (Source: Tirwana, 2013)

The Internet of Things is the one that relates the most to smart cities. As discussed before, there is an increased number of connected devices. This is what can be seen as the Internet of Things and with that it is meant that cities can make use of connected devices, sensors etc. The usage of the data that flows out of all those connected devices will therefore become more important and can enable a platform ecosystem model.

This can be aligned with the focus of the Ruggedised project. As stated before, the main focus of the project will be to improve the quality of life of its citizens. This means that the end-users are important stakeholders. Community engagement is key here. The project should for instance be inclusive, social, and participatory (Jadoul, 2017). To make it a success, the valuation that comes from the end-users is important. That value mainly depends on the ease of use of a platform and the availability of applications. The availability of applications depends upon app developers whether they would like to participate on the platform or not. It is therefore essential for the municipality of Rotterdam to find ways to get them on board. The size of the end-user group and the size of the app developers can be increased via positive cross-side network effects (Tiwana, 2014, p. 33) which is something to keep in mind.

As this study will mainly focus on data security/privacy and the involvement of GDPR compliancy in the smart city concept, the related topics that come from platform ecosystems will be discussed thoroughly to get a clear view on what is involved in a platform ecosystem and how to fit GDPR compliancy into that.

4.2.1. Platform Management

Managing a platform requires a whole different kind of mindset for strategy. The fundamental, structural difference with products and services is that several assumptions on how those are managed do not hold for platforms. The shift goes to control without ownership, orchestration without authority, and direction without enough expertise by the platform owner (Tiwana, 2014, p. 52). These shifts violate the assumptions that most managers are used to make, in particular about ownership and control. One of the main reasons for that is that organizational boundaries are blurring. With a platform, it becomes more important to draw a line where the boundary of the platform's owner ends and where the boundary of the ecosystems' partners begins. The governing of a platform requires a delicate balance of the control from a platform owner and the autonomy of the independent app developers. This is a topic that will be discussed more thoroughly throughout this study.

4.3. Platform evolution

The evolution of a platform can be seen as a key factor to determine the success of a platform ecosystem. For that evolution, there have been developed some metrics to assess the evolution of a platform. These metrics serve three purposes: They steer evolution in a way that will enhance its fitness in the competitive environment the platform finds itself in, they help with avoiding dead ends and take on good opportunities, and they manage trade-offs in design choices along the way (Tiwana, 2014, p. 156). There are three different phases: short-term, mid-term, and long-term, and they all have three metrics which can be divided in operational and strategic metrics.

This study will focus its attention on the short-term, as the GDPR will be implemented in the end of May and we are looking into the perceived impact of GDPR readiness. This would not make sense if the GDPR has already been implemented. Furthermore, the short term is as important as the long term. Tiwana (2014, p. 158) makes the comparison between orchestrating a platform without short-term metrics and driving a car without a speedometer. The underlying theme in all the metrics, whether they are short-term or long-term, is the speed of evolution. Evolvability is the ability of a subsystem within a platform to change when new requirements, needs, and possibilities emerge (Tiwana, 2014, p. 161). That evolvability can be influenced by architectural choices about the platform. However, whether that evolutionary potential is being reached depends on how well the governance reinforces its architectural properties. This is what is being called the architecture-governance alignment. These two aspects of a platform will be discussed later on. The metrics that fall under the scope of the short-term phase are: resilience, scalability, and composability. Those metrics will be discussed to get a clear view of what needs to be assessed in the short-term.

4.3.1. Resilience

Resilience can be explained as the degree to which a subsystem in the platform can maintain a certain level of service when something happens in another subsystem or there is disruption in an external service. It shows the degree to which the subsystem is immune for uncontrollable external factors that are difficult for the developer to directly control (de Weck et al., 2011, p. 71). An important attribute here is that it has a fast recovery, the capacity to bounce back, rather than failure avoidance. At a platform level, this means that the platform needs to be capable of bouncing back when an app in the platform malfunctions. In the figure below, two different levels of resilience are shown.

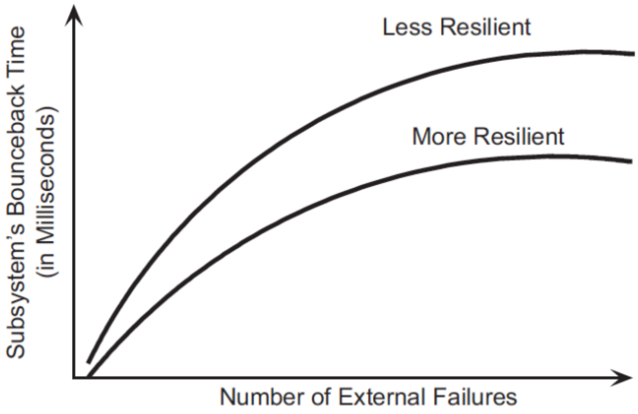


Figure 2: resilience

4.3.2. Scalability

Scalability can be defined as the degree to which the functional and financial performance of a subsystem is size agnostic. De Wecke et al. (2011) define scalability as "*the degree to which a subsystem can maintain its performance and function, and retain all its desired properties without a corresponding increase in its internal complexity".* There is an important difference between scalability in a platform and scalability in another software system. Normally you would only think of scaling upwards, but in a platform, the capacity to scale downward is just as important. Furthermore, performance can mean both financial performance and technical performance. Scalability for technical performance can be assessed as the change in latency, responsiveness, error rates for additional or fewer end-users, and changes in the amount of end-users or external services at the app level (Tiwana, 2014, p. 166). In financial performance, one can think of the moment where the breakeven occurs.

4.3.3. Composability

Composability is the ease of which internal changes can be made in a subsystem without compromising the integration that the subsystem has with other subsystems. The measurement of this metric happens in terms of effort and person-hours that are needed after internal changes have been made so that the subsystems can be reintegrated in the ecosystem again. Composability is one of the important metrics for evolution because of three reasons. The first one is that the maintenance costs of software over its lifetime exceed the costs of the initial development costs with 700% (Tiwana, 2014, p. 168). The second reason is that with composability outside innovations are more absorbable. If your platform has high composability, it is easier to exploit technological changes that come from outside of the platform ecosystem. The last reason is that the different parts of a platform ecosystem do not evolve synchronically. All these reasons make composability a strategic metric of evolution.

4.4. Privacy

Smart cities are mainly meant to improve the life of its citizens, make better usage of energy and to speed up certain processes, all with the main goal to make Rotterdam a better place to live in. With the data that will be gathered via various ways, two important challenges arise: privacy and security. The concept of privacy is very important for cities, because if users deem a system as insecure for his/her privacy, the city will not be able to establish itself successfully (Bartoli et al., 2011).

According to Petronio (2012), privacy is defined by the feeling that someone has the right to own their privacy information. The Communication Privacy Management (CPM) theory shows us that people maintain and coordinate their own privacy boundaries. These are the limits of what they would like to share and what not. This means that individuals should make a balance between their competing needs for privacy and disclosure of information. People make choices about revealing or concealing information based on conditions they perceive as important. CPM states that although there may be a flow of private information from one to another, borders mark ownership lines so that the issues of control are clearly understood.

With all those connected devices and thereby the uprising of the Internet of Things, standards are evolving. Digital citizens are more instrumented with data that is available about their location, energy usage, and other activities. This makes it seem like privacy is disappearing. Privacy protecting systems are therefore needed to keep up with continuous technical changes and the gathering of more and more data. Their implementation will be essential to create a smart city in which the citizens of Rotterdam would like to live (Elmaghraby, 2014).

In such a smart city, there are several interconnecting systems that serve totally different purposes (like traffic control or energy management). These create a system of systems, which causes the exponentially growth of the complexity of such collaborating systems. As discussed before in 4.4, it would be a good idea to divide the platform into various pieces. That way, security systems can be easier implemented (Bartoli et al., 2011).

Another issue in the protection of the smart city is the organization of sensitive data. When personal data is gathered by types of ubiquitous sensors, smartphones, smart electricity meters, and smart vehicles, privacy will become more and more important. The challenge here is how to separate the data collected about a user, which is required when the city wants to provide high-quality personalized services, from the user's real identity. One consequence of that is that the usage of addressing identifiers must be avoided in future systems.

Protecting the privacy of the citizens will require the combination of legal and technical security measures (Elmaghraby, 2014). As important as it is to take the existing laws that serve as the most important guidelines for creating privacy-respecting smart cities, it is also important to keep in mind that the laws can only work together with the social and technological reality, not against them (Langheinrich, 2001). This works as well for the GDPR and businesses or governmental institutions.

4.4.1. Trade-off personalization and privacy

Privacy can be a major concern when smart cities want to make use of online personalization. Overall, customers are interested in personalized services and products, but are still concerned about how tech companies use their data. Even though the services that are provided can be valuable, a customer can still make the decision not to use them (Chellappa et al., 2005). This can happen due to the privacy concerns that arise from those services outweigh the benefits that come with it. The question that arises is: why would customers even make use of online personalization? There are multiple reasons for that choice. The perceived value could be higher than the importance of their privacy, they may be offered money so that privacy becomes less important, and lastly, customers can be unaware of the privacy risks of disclosing their information. A good example comes from people who agree on connecting Facebook to a certain game they play on their smartphone. This means that they willingly share their information from that app with Facebook (Li, 2012). This can be compared with citizens and the city.

The trade-off between the value of personalization and the concern for privacy is a subject with great importance within the privacy domain. Personalization is an important aspect for online vendors or platform ecosystems. Acquiring new customers can cost ten times more than retaining the current ones, so it is important for a platform to improve customer satisfaction and retention. Personalization is the key to this. In order to provide that personalized product or service, consumers need to provide information so that the vendor, in this case the urban data platform, can tailor his services exactly to the tastes of the consumer (Chellappa et al., 2005). This cannot be achieved without the consumer losing some privacy. The question is to what level the consumer would be willing to give away that privacy and for which reasons.

4.4.2. Concern for Information Privacy

Chellappa et al. (2005) argue that customers would be willing to share their preferences and personal information in exchange for apparent benefits like convenience. Online customers would share their preference information if the quantified value of the personalized services that they get out of it outweighs the quantified loss of information privacy. Individual consumers may not always be able to exercise their beliefs regarding privacy, therefore it has become natural that the safeguard of information privacy has fallen into the hands of governmental entities. This is where regulations such as the GDPR come from. Smith et al. (1996) developed an instrument that is called the Concern for Information Privacy (CFIP). This instrument provides guidelines how vendors should collect their information, how they should fix errors that are related to personal information, how they should inform their customers about the use of their information, and how they should prevent unauthorized access to information. A last guideline that can be added is one regarding enforcement. This requires that there should be an effective authority to enforce and impose sanctions for violations of the user information.

Trust is an important factor in the information privacy issue. There needs to be some basic form of trust so that consumers will conduct a certain commercial transaction. It could be argued that the greater the presence of trust factors, the greater the chance a consumer will make use of the products or services from the vendor. Trust also plays a big role in situations that involve sharing of information and thereby the concern for privacy. Two factors that can build trust are the consumer's familiarity with the vendor, and past experiences between the two of them.

In the end of their study, Chellappa et al. (2005) conclude that vendors can do little to influence the privacy concerns of consumers other than following the before mentioned guidelines. What they can do, is try to indirectly affect the privacy concerns of consumers by trust building.

4.4.3. Privacy Protection Tools

In order to build and maintain some long-term relationships, there needs to be a certain level of trust. Trust-creating actions can make customers/third parties make more frequently use of platforms and can lead to a higher acceptance of personalization. Therefore, four privacy protection tools have been developed by Li (2012). The first one is *anonymity*. This can be ensured through the use of pseudonyms (Ishitani et al., 2003). The 'Managing Anonymity while Sharing Knowledge to Servers' (MASKS) framework balances the privacy concerns of users with their desire for personalized services. Masks uses some kind of relevation scheme that places an anonymity barrier between private data and Web services, and controls the information that flows across that barrier towards the service. This will give a higher level of trust because if customers believe that they cannot be identified as a person, the likelihood of them sharing their personal data is higher (Li, 2012).

The second privacy protection tool consists of *privacy statements* and *privacy policies*. Privacy certifications can lead to trust from customers. However though, only a few people actually make the effort to read published privacy statements. The third tool is *security seal.* These seals assess the privacy standards of a company on accessible privacy statements. The last tool is related to *information transparency*. This measures the awareness from customers about how companies deal with the data they collect from those customers (Li, 2012).

Li et al. (2012) concluded from their studies that providing privacy signs will positively impact customers' likelihood of making use of personalization. These signs create trust for customers so that they are more willing to disclose personal data. Therefore, it will be important for Rotterdam as a smart city to combine security and privacy features in order to get the attention of citizens and establish a sense of trustworthiness. Trust will enable citizens to suspend their worries about privacy, so that they are willing to provide personal information to obtain personalized services. Furthermore, the impact of privacy concerns and the willingness of customers to provide information can be related to the reputation of a company. Rotterdam needs to make sure that citizens think of the city as a trustworthy city who will treat their personal data with respect.

Proposition 1: *The existence of privacy protection tools will lead to a lower amount of security issues, and hence positively influence the level of evolution of an urban data platform.*

4.5. GDPR

As discussed before, the General Data Protection Regulations are the new European privacy regulations. It has already been implemented in 1995, but some rigorous changes will be implemented in May 2018, which implies that companies and governments have to change their approach towards data privacy. A survey from Deloitte showed that 15% of all companies in the Netherlands thought that they would be compliant in May 2018 (Lowijs, 2018).

The GDPR will give individuals some more rights and strengths regarding their data privacy and will ask for more transparency and accessibility from companies. An important aspect in the new GDPR regarding the smart city project, are the stricter rules about giving consent. *"The conditions for consent have been strengthened, and companies will no longer be able to use illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it."* (GDPR, 2017). This means that the consent has to be variable and that individuals generally will have more rights when you rely on consent to process their data. In order to achieve that user consent, integration of security and privacy mechanisms must be a key concern in current studies (Bartoli et al., 2011). The six most important aspects of the GDPR are: The rights of individuals, right to be informed, the right to be forgotten, when needed, the instalment of a Data Protection Officer, obligations on data processors, and lastly Data Protection Impact Assessment and data breach response (Malyon, 2017).

Law and regulation, typically, are lagging some decades behind the technological development. The shift towards the Internet of Things complicates that even more. Think about traffic safety or healthcare. This is where the government needs to step in so that they can obtain mission-critical relationships with IoT device providers. Probably the most significant areas of concern are the ones about ownership, use, and security of data that is generated by IoT devices. For the civil society, the balance between their security and the facility that they get from data is a pressing question (Dowden, 2016). The challenges are enormous. It is for instance extremely difficult to foresee how some GDPR concepts like privacy by design can be accommodated in a smart city where huge amounts of data are being gathered and stored. Furthermore, there is the emergence of "decentralized" or "distributed autonomous organizations" which has already prompted debate among lawyers as it is often unclear who has been contracted or which company is in charge. This happens as well with platforms, the governance, which will be discussed in chapter 4.7 of a platform can be shared which makes it difficult to link the right owner to the right data.

4.5.1. Tech companies

Tech giants like Apple, Google, and Facebook are examples of platform ecosystems which intensively use public and personal data. Facebook for instance has connections with many other companies which makes it possible for them to personalize advertisements based on other websites that you have visited.

Since last year, national governments have started to chase those tech giants. Facebook for instance, has been dinged for privacy infractions due to their WhatsApp acquisition. This is related to the GDPR, as noncompliance with GDPR could incur penalties of up to 4% of a company's global revenues (Roberts, 2017). 52% of organisations believe that GDPR will result in fines for their business. 68% believes that it will dramatically increase the cost of doing business in Europe (Tankard, 2016). When the GDPR starts on the 25th of May, it will therefore be a significant advantage for those who prepared early. The GDPR will serve as a global standard for new innovations and consumer trust in technology. GDPR will bring more legal certainty and can serve as a starting point for international standards and will make the EU a trustworthy digital market (Albrecht, 2016). This does not only count for tech companies, but is also applicable for governmental institutions, cities, and countries. Just recently, Microsoft announced that they would extend the rights that are provided by Europe's GDPR to all their customers worldwide (Al-Heeti, 2018). They do this because they think that GDPR establishes important principles that are relevant globally so that they can gain trust from all their customers. *"Privacy is also the foundation for trust. We know that people will only use technology that they trust. Ultimately, trust is created when people are confident that their personal data is safe and they have a clear understanding of how and why it is used"* (Brill, 2018).

A good example that shows the importance of being prepared for the GDPR comes from the Dutch Tax Authorities. Due to a crisis in their ICT system, they could not collect taxes for a certain period. This cost them up to €450 million. They were supposed to start using their new ICT system from the start of 2017, while the old system would not work anymore after the 31st of December. It turned out that there was no back-up of the old system so that taxes had to be inserted manually which caused a big delay (Jonker, 2017). If you relate this to the GDPR readiness of a platform ecosystem it could lead to a delay in implementing certain aspects of the platform, which for instance could cause a loss of revenue for app developers. The question that arises here, is if the level of GDPR readiness will indeed positively influence the implementation and evolution of an urban data platform.

Proposition 2: *A high level of GDPR readiness positively influences the level of evolution of an urban data platform.*

4.6. Platform architecture

The platform architecture is the first gear in a platform's gear motor. The platform requires an architecture of participation to be able to grow its ecosystem (Baldwin et al., 2006). The app developers that participate in the platform must be able and motivated to innovate their apps around the platform. Platforms must manage the balance between coordination and autonomy. The primary focus of architecture is to have a framework that decomposes a complex ecosystem into relatively independent subsystems. One way to do that is to split the system up into smaller pieces. This means that you will get a collection of black boxes that talk to each other (Tiwana, 2014, p. 80). That is in theory where platform thinking stands for, which is the main difference with just one company that implements all these black boxes. In a platform ecosystem, there are many companies who can create those black boxes. These are the apps developed by independent entrepreneurs. In the end, ecosystem architecture should ideally partition the ecosystem in two subsystems: a reusable and stable platform and a set of complementary apps (Baldwin et al., 2009).

Even though the platform has an overarching architecture, the architecture from individual apps can vary from one app to another. It is therefore needed to have a microarchitecture for apps. This will define how the app communicates and interoperates with the platform. A common used technique here is the usage of an open API. There are four elements within microarchitecture: presentation logic, application logic, data access logic, and data storage (Tiwana, 2014, p. 86). The last two are the most important regarding GDPR compliancy. There need to be good rules and agreements between the app and platform owner to make sure that the data from the app is GDPR compliant.

What could serve as a good architecture model for the smart city Rotterdam in the Ruggedised project is the client-server architecture which can be seen in the figure below.

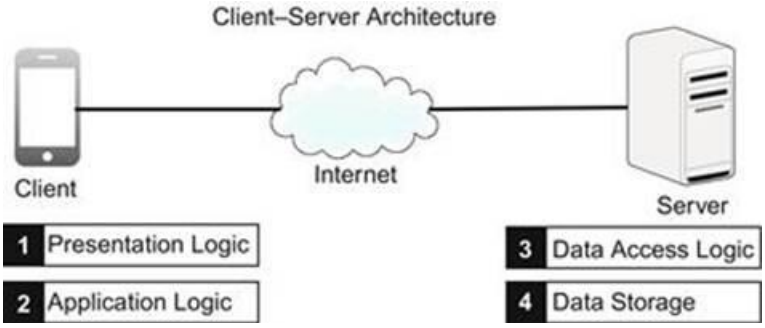


Figure 3: Client-Server Architecture (Source: Tiwana, 2014)

The reason for the fit with this model is that the platform owns the server and therefore holds control over the data storage and usage of it. This can be important with sensitive data and the compliancy within the GDPR.

There are some parallels between the architecture of cities and the architecture of platform ecosystems. In a city, the law enforcement happens by hand of the city. In a platform ecosystem, the interface standards are enforced by the platform owner. This is part of the governance aspect within a platform.

4.7. Platform Governance

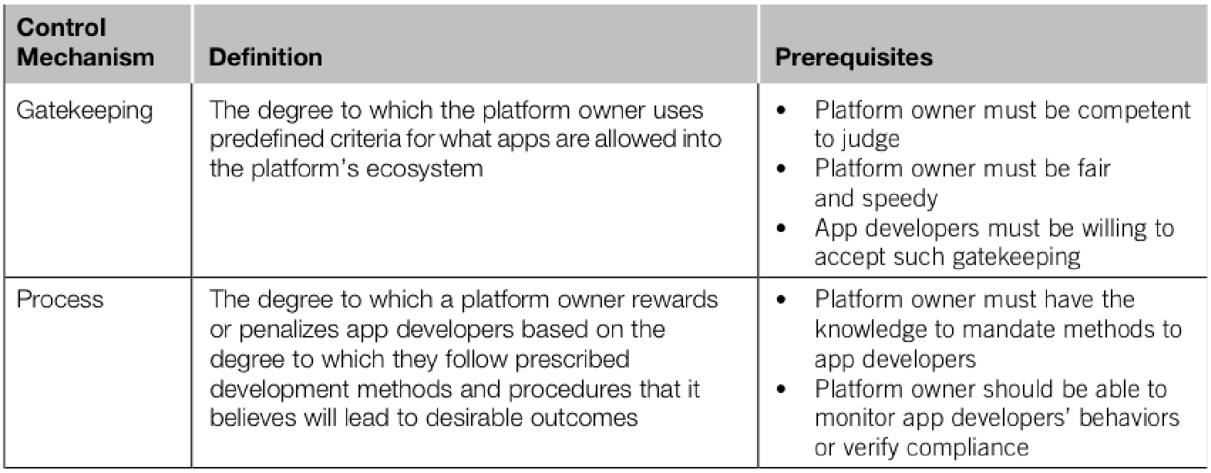
The second gear in the platform's gear motor is the governance. Together with the architecture, these two factors enable the evolution of the platform, which has been discussed in chapter 4.3. Platform ecosystems can be compared to symphonies. The platform owner acts as the conductor and the app developers are the musicians. The individual musicians choose to follow the lead of the conductor who does not have the depth of specialized musical talent and has limited direct authority. Orchestration rather than control should be the focus of governance in a platform. In the end, the goal of platform governance is to reduce behavioural complexity.

Platform governance has three dimensions: division of the authority and responsibilities between the platform owner and app developers, collection of mechanisms that give the platform owner control over app developers, and pricing policies (Tiwana, 2014, p. 118). Misalignment in any of those three dimensions can lead to the destruction of the ecosystem. The third dimension will not be discussed in this study, as it is not the focus in the research.

The first dimension, decision rights, states who can make certain decisions. They can be split up in strategic and implementation decisions. Strategic decisions are direction-setting and specification-oriented. If the strategic decisions of the platform would be centralized, it gives the platform the opportunity to lock out rival platforms and lock in app developers (Tiwana, 2014, p. 126). But app developers should have some sort of input in those strategic decisions, as they understand their own needs and they have a better understanding of the emerging needs of end-users.

The second dimension of governance is control. The control comes from the platform owner over app developers using various control mechanisms. The platform owner can make use of three formal mechanisms and one informal mechanism. These four mechanisms are: gatekeeping, process control, metrics, and relational control (Tiwana, 2014, p. 119). Bresnahan and Shane Greenstein (2014) did research on various software platforms and the usage of control mechanisms. They found out that Apple has a strict approval process for all apps. Thereby they want to guarantee a certain level of quality and safety to their end-users. Google's platform Android was being governed in a nonhierarchical way and did not have the control over the distribution of apps. *"The lack of control of information has led to some coordination failures and fragmentation, as different hardware vendors have created different, sometimes* *incompatible, devices"* (Bresnahan & Greenstein, 2014). This demonstrated the need to for platform owners to step up and intervene in some platform processes by using these control mechanisms.

The two that are the most important for the context of this study are gatekeeping and process control. The definition of those two can be found in the figure below.



Control Mechanism	Definition	Prerequisites
Gatekeeping	The degree to which the platform owner uses predefined criteria for what apps are allowed into the platform's ecosystem	• Platform owner must be competent to judge • Platform owner must be fair and speedy • App developers must be willing to accept such gatekeeping
Process	The degree to which a platform owner rewards or penalizes app developers based on the degree to which they follow prescribed development methods and procedures that it believes will lead to desirable outcomes	• Platform owner must have the knowledge to mandate methods to app developers • Platform owner should be able to monitor app developers' behaviors or verify compliance

Figure 4: Control Mechanisms. (Source: Tiwana, 2014, p. 119)

4.7.1. Gatekeeping

Gatekeeping can be an important control mechanism for the platform owners of the smart city, as this can ensure a certain quality of data and a certain level of compliancy. There needs to be some sort of boundary for certain sensitive subjects or applications that require too much data from the citizens of Rotterdam. This means that the platform owners will have "bouncer rights" to exclude outsiders from the platform (Boudreau, 2010). It is the prerogative of the platform to open or remove certain restrictions on usage, development, and commercialization of the platform. Otherwise, app developers have the choice to implement apps with every sort of content they would like, which could eventually lead to a bad reputation of the urban data platform. Furthermore, some app developers might nog secure their app as good as expected or require their customers to share certain personal data while not using it by the GDPR standards. These actions can be prevented by gatekeeping. It represents the degree to which a platform owner uses predefined objective acceptance criteria so that it can be judged what kind of apps and app developers are allowed into the platform. These criteria are not just there to show what is allowed into the ecosystem but also who is allowed into the ecosystem. Three important requirements must be met for control via gatekeeping in order to be viable (Tiwana, 2014, p.

123). First of all, the platform owner must be sufficiently competent enough to judge the submissions from app developers. Secondly, the platform must do this fairly and speedily. Thirdly, the app developers must be willing to subject themselves to gatekeeping. These are requirements the platform owners of the urban data platform of Rotterdam should consider when using gatekeeping.

4.5.2. Process Control

Process control is the degree to which the platform owner hands out rewards or penalizes app developers based on the degree to which the app developers follow the development methods, rules, and procedures. These rules and procedures should lead to desirable outcomes in terms of apps interoperating well with the platform owner (Tiwana, 2014, p. 124). Compliancy will be rewarded and noncompliance will be penalized. This will prevent the app developers from messing with the prescribed rules and thereby possibly harming end-users of a platform. Furthermore, this will prevent the platform from being penalized by the GDPR committee. If that would happen, they could get a fine or they might have to delete all the data that has been gathered.

Proposition 3a: *A high degree of control mechanisms implemented by platform owners will positively moderate the effect of the degree of GDPR readiness on the level of evolution of an urban data platform.*

Proposition 3b: *A high degree of control mechanisms implemented by platform owners will positively moderate the effect of privacy protection tools on the level of evolution of an urban data platform.*

4.8. Conceptual framework

In this section, the conceptual framework for GDPR readiness in smart cities will be presented. Based on the discussed literature, my personal opinion, and the steering from the municipality of Rotterdam, propositions are developed. The variables and the previously mentioned propositions can be found in the model below. All variables are related to the platform ecosystem.

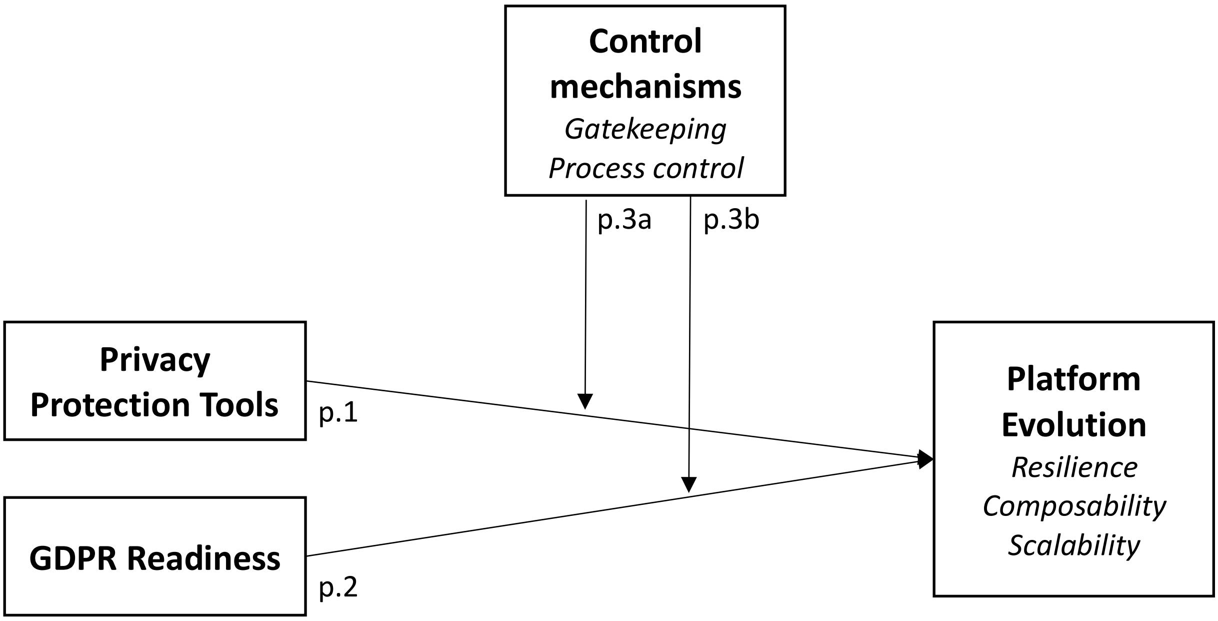


Figure 5: Conceptual model

5. Methodology

5.1. Research strategy

Smart cities are still quite a new subject in the academic world. Besides that, the new GDPR still has to be implemented while writing this study which makes it hard to find relevant literature about the combination of both. We can relate that to the importance of privacy of citizens within smart cities though. There are some real-life cases from cities or companies present in which privacy and the way people think about their privacy is a subject. This makes it a suitable study for an exploratory (multiple-) case study so that we can provide the city of Rotterdam with guidelines how to cope with the GDPR.

However though, before getting into a case study, two other methods will be used as preliminary research. First of all, there will be an expert validation with employees from KPN who have specific knowledge about GDPR. Furthermore, a questionnaire will be send out to the leads of other smart city initiatives in Europe. In this questionnaire, everyone within the main project can ask questions about their topics so that everyone is optimally prepared for their case studies.

In this study, the book of Yin (2013): Case Study Research: Design and Methods, will be used to get the most value out of this approach. Case studies are sometimes criticized because they can be subjective and they give too much attention for the researcher’s own interpretations (Flyvbjerg, 2006). Furthermore, case studies are often seen as less rigorous than quantitative methods. The case study however though, has its own rigor. The advantage of a case study is that it can “close in” on real-life situations.

The kind of cases that we want to investigate here, are other smart city projects so their GDPR readiness and platform evolution can be studied. To be able to get a clear picture and outcome, it would be wise to test four cases. The smart cities that would be interesting to study are Rotterdam, Utrecht, Eindhoven, and Den Haag. The proposed selection of cases would be an information-oriented selection. There we would choose the selection of maximum variation cases (Flyvbjerg, 2006). The goal here is to obtain information about the significance of various circumstances for the process and outcome of cases: four cases that are very different on one dimension.

The best method therefore would be a multiple-case study approach, which gives us one unit of analysis and the thorough research of four cases. Multiple-case studies may be preferred over single-case designs. Single-case studies are vulnerable because you put “all your eggs in one basket”. Moreover, there could be an analytic benefit from having two or more cases (Yin, 2013). This study will follow the case study protocol proposed by Yin, as this can help by preventing the case study becoming too subjective. The application of this case study protocol can be found in Appendix B.

5.1.1. Research Design

This section will elaborate on the research design of this study. As discussed before, this will consist of a questionnaire that will be send out by the research leader of the project. Every student within the Ruggedised project will get the chance to add questions about their topic so that they can use the outcomes of that questionnaire to prepare their case studies.
The questionnaire is structured in six parts that follow the platform life cycle:

1. IST: current situation of the Urban Data Platform in your city
2. ENVISION: Vision & Purpose, Scope and Use Cases
3. BUSINESS DESIGN: Platform Governance, Business Models and Financing
4. TECHNOLOGY DESIGN: Architecture, Data and Standards
5. DEVELOP: Accelerators and Barriers
6. SUCCESS FACTORS: what are the factors that drive business model success

(Source: *Questionnaire Urban Data Platforms*, 2018)

With the outcomes of this questionnaire, the propositions that have been designed can be validated. Furthermore, exploratory interviews will be held with employees from the municipality of Rotterdam and with employees from KPN. These people are specialists on the GDPR topic and they are informed about the research question and the conceptual model so that they can help with steering the study in the right direction. Lastly, in-depth interviews with several other smart city initiatives and stakeholders of those initiatives will be held. This will provide answers to the research question and the proposed hypotheses. In consultation with Jaap Dekker from the city of Rotterdam and the contact person of KPN, several cases have been selected and approached. A short introduction of the researcher and the topic have been provided so that the approached contacts are up-to-date on the topic. This introduction mail can be found in Appendix A. Due to the exploratory nature of this study, the interviews consist mostly of open questions to provide an environment that allows the interviewee to elaborate on certain subtopics.

5.1.2. Unit of Analysis

The unit of analysis defines what the "case" actually is (Yin, 2013, p. 29). As described in 3.1, this study will provide insights in the effect of the degree of GDPR readiness on the short-term evolution of an urban data platform, and in particular, the urban data platform of the smart city Rotterdam within the Ruggedised project.

5.1.3. Case Selection

The selected cases are chosen on the fact that they should provide insights and results so that the research question can be answered. Therefore, a case should be connected to a smart city project. This can either be a municipality who is implementing a smart city model and therefore has to deal with the GDPR, or a partner/consultant of the project who can give valuable insights about their analysis of the effect of GDPR readiness on an urban data platform. In order to generalize findings, the various cases should have various characters. This means that we are looking for extreme cases, ranging from cases that are already successful in implementing the new GDPR regulations to cases that are still at the beginning of their urban data platform and thereby the implementation of GDPR.

The cases have been selected by using the replication method. This is similar to the method that Hersen & Barlow follow for multiple experiments (1976). Starting with the uncovering of a significant finding within a single experiment, the research goal thereafter would be to replicate this finding while conducting more experiments. Some of the replications would then duplicate the exact conditions of the original experiment, and some of the replications would alter some conditions that seem irrelevant. Only those kinds of replications would make the original finding robust and worthy of further investigation (Yin, 2013, p. 47). Multiple-case studies have the same underlying logic. If all the cases turn out as is predicted in the propositions that have been drafted, they provide compelling support. If the cases are contradictory, the initial propositions should be revised and tested with another set of cases. An important aspect of the replication theory is the development of a theoretical framework. Case selection and the specification of measurements are other important steps in the design and data collection process. Both the individual and multiple-case results should be the focus in the conclusion. Furthermore, a cross-case analysis should be examined. This case study method can be found in the figure below:

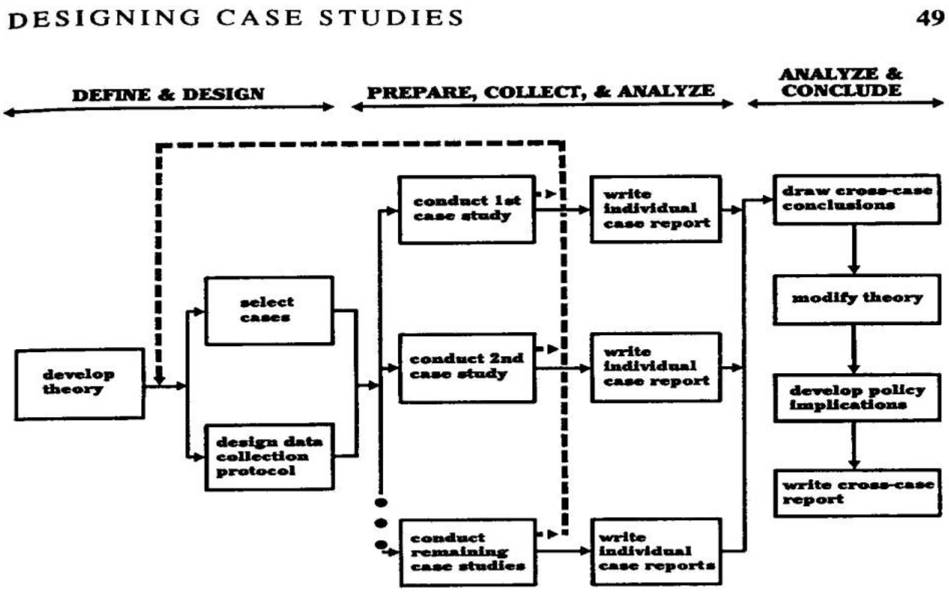

DESIGNING CASE STUDIES
49
DEFINE & DESIGN
PREPARE, COLLECT, & ANALYZE
ANALYZE & CONCLUDE
develop theory
select cases
design data collection protocol
conduct 1st case study
conduct 2nd case study
conduct remaining case studies
write individual case report
write individual case report
write individual case reports
draw cross-case conclusions
modify theory
develop policy implications
write cross-case report

Figure 2.5. Case Study Method
SOURCE: COSMOS Corporation.

Figure 6: Case Study Method Replication

Lastly, the cities and companies that have been selected, must be willing to cooperate and to share their insights. At least one interview per case is required, but it would be preferable to get several insights within one case. The analysis will be based on a combination of available documentation and insights from the interviews.

5.1.4. Selected Cases

An overview of the selected cases and the interviewees that belong to the various cases can be found in the tables below. Not everyone has the same job title, but everyone was able to provide eligible insights on either the GDPR readiness, the governance, and the evolution of an urban data platform.

Interviewee	Stakeholder	Function
Frank Vieveen	Gemeente Rotterdam	Programmamanager Smart City
Roland van Ravenstein	KPN	Business Developer
Marcel van Oosterhout	Erasmus Universiteit	Senior Projectmanager Technology Department
Rick Klooster	Future Insights	Founder & CCO
Roland van der Heijden	Gemeente Rotterdam	Productmanager Digitale Stad

Table 1: Interviewees Rotterdam

Interviewee	Stakeholder	Function
Thomas Kruse	Gemeente Utrecht	Strategisch adviseur bedrijfsvoering
Stefanie Kelterman	Gemeente Utrecht	Projectleider AVG
Arjen Hof	Civity	CEO
Hans van Impelen	Gemeente Utrecht	Functionaris Gegevensbescherming

Table 2: Interviewees Utrecht

Interviewee	Stakeholder	Function
Tim Vergeer	Gemeente Eindhoven	Business Consultant RD
Tine Gebuis	Gemeente Eindhoven	Functionaris Gegevensbescherming
Rick Schager	Gemeente Eindhoven	Smart ICT Architect

Table 3: Interviewees Eindhoven

Interviewee	Stakeholder	Function
Uwe Montag	City of München	IT Strategy Smarter Together

Table 4: Interviewee Munich

5.1.5. Additional Sources of Information

Besides the cases that have been chosen, there is a close collaboration with the city of Rotterdam and with KPN. Within the city of Rotterdam, my main contact who provides me with information is Jaap Dekker, and there are several other sources that provide applicable information on this subject. Regarding KPN, Roland van Ravenstein provides useful guidelines and information and connects me to certain people within KPN that are specialists in the GDPR domain. Several informal interviews with employees of the city of Rotterdam and KPN have been held to gain exploratory information.

5.2. Data Collection

5.2.1. Triangulation

One of the goals when doing research is to design a study that has internal and external validity, reliability, and procedures in place to decrease potential biases (Shih, 1998). Triangulation is a method to increase that validity and reliability. "*Triangulation is the combination of two or more data sources, investigators, methodologic approaches, theoretical perspectives, or analytical methods within the same study"* (Kimchi et al., 1991). The corroboration of multiple perspectives or sources can lead to an increased validity of a study (Yin, 2013). This thesis makes use of triangulation by using multiple sources of data. As said before, these various sources of data are the questionnaire, exploratory interviews, and in-depth interviews, which is complemented by desk research. Potential problems that can arise regarding construct validity can be addressed because these sources provide multiple measures of the same phenomenon (Yin, 2013, p. 99). An important aspect of triangulation however, is that the information from these various sources should be aimed at corroborating the same fact. If the data is really triangulated, this means that the facts that are stated in the conclusion of this study are supported by more than a single source of evidence (Sieber, 1973).

5.2.2. Interview Protocol

The interview protocol of this study is inspired by the protocol of Vermerris et al. (2014). When possible, the interview will be held face-to-face. For some projects this might not always be possible, due to limited time availability or geographical distance. First of all, the key elements of the interview are being explained to the interviewee. This includes for instance the scope and the duration of the interview. Then an introduction question will be asked regarding the current position of the interviewee in the company and some elaboration on his daily activities. After this introduction phase, questions regarding the specific variables will be asked. What should be kept in mind regarding those questions is that although there is an interview protocol and a certain line of inquiry needs to be followed, the stream of questions should be fluid rather than rigid (Rubin & Rubin, 1995). There is for instance room for some off-topic, but still somehow related answers. The interviewee will be asked if there is any additional documentation. A site report will be drafted and send to the interviewee so that he or she can check if the answers are correctly noted and transcribed. The complete interview protocol can be found in Appendix D.

5.3. Measurement of Variables

5.3.1. Platform Evolution

All short-term evolution metrics of a platform will be measured during the interviews with the stakeholders from the various cases. Several questions per metric have been designed in order to obtain results that can be used for the within- and cross-analysis.

5.3.2. GDPR Readiness

The GDPR readiness of a smart city and its urban data platform can be measured via the existence of certain aspects of the GDPR. The first step for organisations is to have a data register. For governmental institutions, the existence of a Data Protection Officer is a must, so this is certainly a checkpoint. Furthermore, privacy by design is an important factor. The execution of a privacy impact assessment for new processes/ideas is something that should be done as well and there should be a method of obtaining consent.

5.3.3. Platform Governance

As stated before in section 4.5, this study mainly focuses on two control mechanisms, which are gatekeeping and process control. The figure below shows the measurement levels from Tiwana (2014), which can be used to show which mechanisms, and to what extent, are being applied in a platform ecosystem. These measurements will be adapted to low, medium, high, so that the same measurements can be used for every variable.

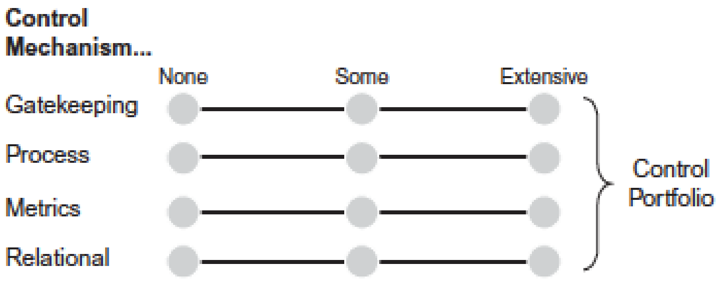


Figure 7: Measurement of control mechanisms

5.3.4. Privacy

Four privacy protection tools have been adopted from Li (2012). Via qualitative data from the interviews, the existence of those tools will be tested so that they can be scored as low, medium, or high. This means that with the existence of one tool the score is low, with the existence of two or three tools the score is medium and with the existence of four tools the score is high.

5.4. Data Analysis

As stated before, this study follows the case study protocol of Yin (2013). This protocol encompasses four sections. The first one consists of an overview of the case study project, including objectives and relevant literature. This has already been discussed in chapter 1-4. The second section covers the field procedures like the presentation of credentials and general sources of information. The third part consists of the case study questions, which are in this case the questions of the interview protocol. The last section is a guide for the case study report. Furthermore, this study uses four tests that have been widely used to ensure the quality of empirical social research (Rowley, 2002). These tests will be explained in Appendix C.

5.4.1. Within-case and Cross-case Analyses

In order to get a convenient conclusion out of the analysed data that is gathered from the selected cases, a within-case analysis and a cross-case analysis need to be performed. Generalization in a study cannot be developed without integrating a within-case analysis and a cross-case analysis (Ayres, 2003). The within-case analysis provides key elements of a case and consists of precise descriptions of each case. By doing this, the individual case can be understood in its own context. The idea is to become intimidate familiar with each case. This is central to the generation of insight, as it helps to cope with the enormous volume of data you get from these cases (Eisenhardt, 1989). This familiarity accelerates the cross-case analysis. In the cross-case analysis, the goal is to search for patterns across the various cases. The key to a good cross-case analysis is to look at the data in many divergent ways. The tactic is to select dimensions, which have been drafted in chapter four and chapter 5.3. This makes it possible to look for within-group similarities coupled with inter-group differences. The idea here is to go beyond initial impressions. By doing this, the accuracy and reliability of the study will be improved. Furthermore, cross-case analysis increases the probability of finding novelties in the data. The cross-case analysis will not only be executed on the four in-depth cases, but also on the cases from the questionnaire. In the end, those findings will be compared, to check whether the propositions hold for both studies.

5.4.2. Necessary Condition Analysis

The variables that have been chosen are all being assessed in a table with a low, medium or high score. This is done for the independent variables as well as the dependent variable. A proposition has a positive outcome if more than half of the cases are in the expected cells. This means for instance that when you have a proposition that states that a higher level of the independent variable X will lead to a higher level of the dependent variable Y, should have cells with the same expected value. When the outcome is medium, the variable will not be taken into account, as propositions are only tested on an unambiguous nature.

Besides the cross-case analysis, the Necessary Condition Analysis (NCA) will be used to determine the impact of a certain variable. This is done by assessing if the independent variables are really necessary to reach the desired outcome of the platform evolution. The necessary condition are the characteristics of an organization that are necessary but not sufficient on its own to reach the desired outcome. Dul states it as the following: *"A necessary determinant must be present for achieving an outcome, but its presence is not sufficient to obtain that outcome"* (Dul, 2016).

In this case, the Discrete Necessary Condition will be used, as both the dependent and independent variables can have a value of low, medium or high. This Discrete Necessary Condition is showcased in the figure below.

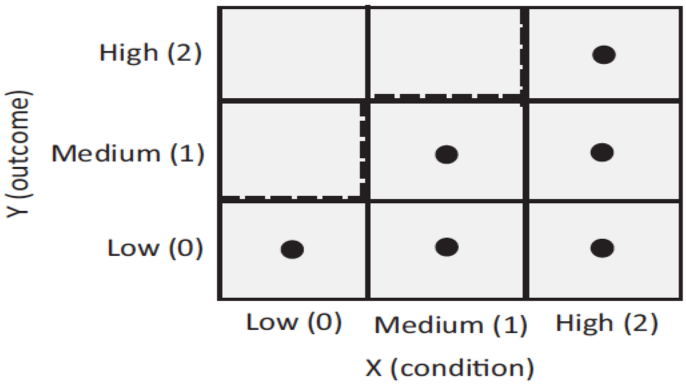


Figure 8: Contingency table of the discrete necessary condition

Dul (2016) argues that the empty corner in the upper left corner indicates that there is a necessary condition present. The question that arises here is if the necessary condition is large enough to be taken seriously? Therefore, there is a need to calculate the effect size. The effect size can be described as the *"quantitative reflection of the magnitude of some phenomenon that is used for the purpose of addressing a question of interest"* (Dul, 2016). In this case, it should represent how much of the value of necessary condition X constrains Y. It is the size of the constraint that the ceiling has on the outcome. The effect size will be stronger if the ceiling zone is larger. To calculate the effect size, the formula d = C/S will be used. D is the effect size, C is the size of the ceiling zone, and S is the scope. The scope consists of the potential area with observations.

The necessary condition analysis can also be examined in R, which offers a package that is called the NCA. This package does three main things: First of all, it makes NCA plots, these are scatter plots with the ceiling lines. Secondly, it calculates NCA parameters. Lastly, it calculates values of the variables that are in the bottleneck table, so that it can be determined which X is the bottleneck for a certain Y (Dul, 2016). This NCA package will be used to perform the NCA for the cross-case analysis.

6. Cross-case Questionnaire Analysis

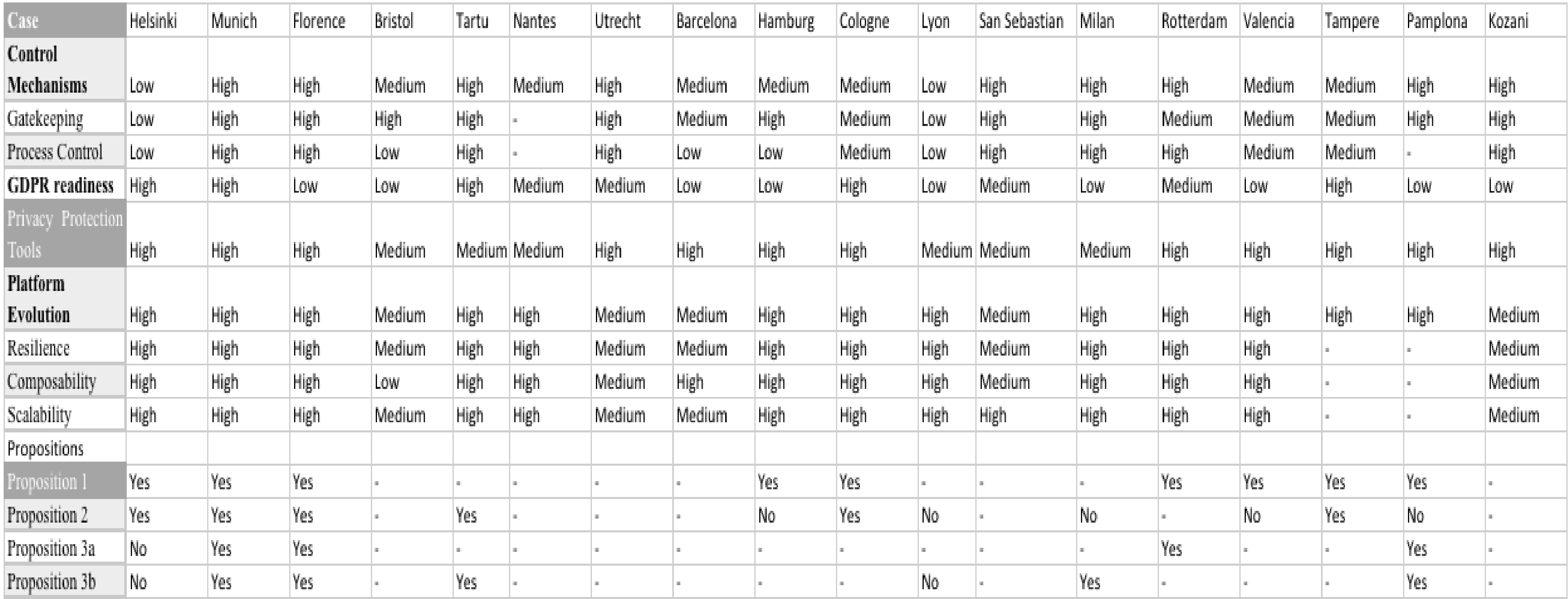
In this section, the several cases from the UDP Questionnaire will be examined via a cross-case analysis. As the results come from a questionnaire, they will not be discussed as thoroughly as the four cases where interviews have been conducted. As discussed before, medium scores will not be taken into consideration, as they do not correlate with a positive or negative effect.

These cases are all cities that participate in a European smart city initiative and therefore have to comply to the new GDPR regulations. This makes them valuable cases for this study. There are some interesting points to notice in the table on the next page.

Firstly, it can be noticed that all cases score either medium or high on privacy protection tools. What can be concluded from that is that every city sees the importance of the usage of some form of privacy protection tools. Furthermore, only 6 out of the 18 cases scored medium, which emphasizes the importance of these tools even more.

Secondly, what can be observed is that only 5 out of the 18 cases score high on GDPR readiness. This is a relatively low score if we compare it to the outcomes of the cross-case analysis that will be discussed in chapter 8. The reason for this could be the fact that not everyone understood the information that had to be check boxed. One example is the city of Munich, who had a different understanding of privacy by design and therefore did not check that box.

Lastly, an interesting point what can be observed is that 13 out of 18 score high on platform evolution. This indicates that most of the platforms are meant to grow and be able to react to malfunctions or changes within the ecosystem. What came forward from the in-depth cases is that most platforms are build and tested so that they can be replicated to other cities in order to make the implementation of smart cities all over Europe possible. Therefore, the evolution of those platforms is something of great importance.



Case	Helsinki	Munich	Florence	Bristol	Tartu	Nantes	Utrecht	Barcelona	Hamburg	Cologne	Lyon	San Sebastian	Milan	Rotterdam	Valencia	Tampere	Pamplona	Kozani
Control Mechanisms	Low	High	High	Medium	High	Medium	High	Medium	Medium	Medium	Low	High	High	High	Medium	Medium	High	High
Gatekeeping	Low	High	High	High	High	-	High	Medium	High	Medium	Low	High	High	Medium	Medium	Medium	High	High
Process Control	Low	High	High	Low	High	-	High	Low	Low	Medium	Low	High	High	High	Medium	Medium	-	High
GDPR readiness	High	High	Low	Low	High	Medium	Medium	Low	Low	High	Low	Medium	Low	Medium	Low	High	Low	Low
Privacy Protection Tools	High	High	High	Medium	Medium	Medium	High	High	High	High	Medium	Medium	Medium	High	High	High	High	High
Platform Evolution	High	High	High	Medium	High	High	Medium	Medium	High	High	High	Medium	High	High	High	High	High	Medium
Resilience	High	High	High	Medium	High	High	Medium	Medium	High	High	High	Medium	High	High	High	-	-	Medium
Composability	High	High	High	Low	High	High	Medium	High	High	High	High	Medium	High	High	High	-	-	Medium
Scalability	High	High	High	Medium	High	High	Medium	Medium	High	High	High	High	High	High	High	-	-	Medium
Propositions																		
Proposition 1	Yes	Yes	Yes	-	-	-	-	-	Yes	Yes	-	-	-	Yes	Yes	Yes	Yes	-
Proposition 2	Yes	Yes	Yes	-	Yes	-	-	-	No	Yes	No	-	No	-	No	Yes	No	-
Proposition 3a	No	Yes	Yes	-	-	-	-	-	-	-	-	-	-	Yes	-	-	Yes	-
Proposition 3b	No	Yes	Yes	-	Yes	-	-	-	-	-	No	-	Yes	-	-	-	Yes	-

Table 5: Cross-case questionnaire analysis

Proposition	Supporting cases	Rejecting cases	Accepted
1	9	0	Yes
2	5	6	No
3a	4	1	Yes
3b	5	2	Yes

Table 6: Accepted propositions Questionnaire

6.1. Reflection on propositions

6.1.1. Privacy Protection Tools

Proposition 1: *A high level of privacy protection tools positively influences the level of evolution of an urban data platform.*

	Privacy Protection Tools			
		Low	Medium	High
Platform Evolution	High		Tartu, Nantes, Lyon, Milan	Helsinki, Munich, Florence, Hamburg, Cologne, Rotterdam, Valencia, Tampere, Pamplona
	Medium		Bristol, San Sebastian	Utrecht, Barcelona, Kozani
	Low			

Table 7: Scatter plot on empirical findings proposition 1

Observation: Table 7 demonstrates a scatter plot of the various cases. As can be seen in the table, nine out of nine cases support this proposition, as the medium score would not be taken into consideration. As the upper left cell is empty, this reveals the presence of a necessary but not sufficient condition. Moreover, in the NCA Plot on the next page, it can be seen that there is a positive relation between the two variables. It can be concluded that proposition 1 is accepted. The further discussion and comparison to the in-depth cross-case analysis will be discussed in chapter 9.

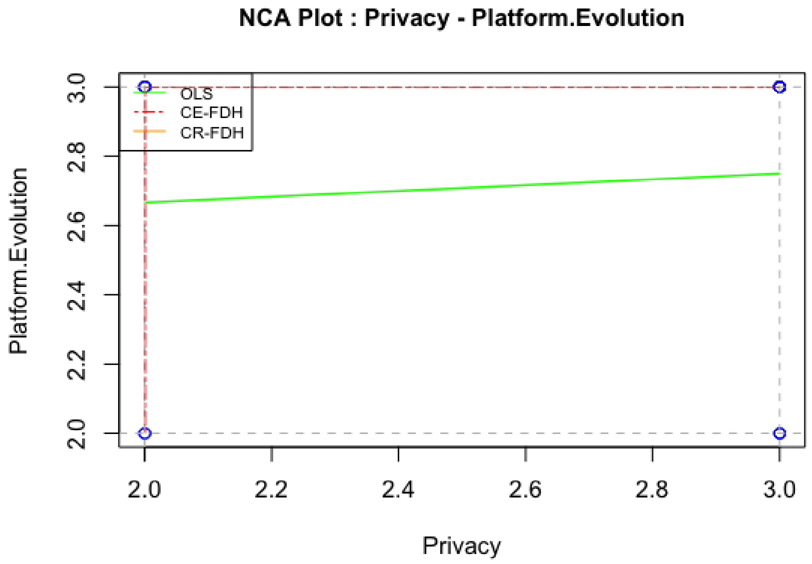


Figure 9: NCA Plot: Privacy – Platform.Evolution

6.1.2. GDPR Readiness

Proposition 2: *A high level of GDPR readiness positively influences the level of evolution of an urban data platform.*

		GDPR Readiness		
		Low	Medium	High
Platform Evolution	High	Florence, Hamburg, Lyon, Milan, Valencia, Pamplona	Nantes, Rotterdam	Helsinki, Munich, Tartu, Cologne, Tampere
	Medium	Bristol, Barcelona, Kozani	Utrecht, San Sebastian	
	Low			

Table 8: Scatter plot on empirical findings propositions 2

Observation

As can be observed from table 8, five out of 11 cases support the proposition, when again not taking variables with medium scores into account. In the NCA plot on the next page, however, a positive relation between GDPR Readiness and Platform Evolution is reflected. As the upper left cell in table 6 is not empty, the effect size here is 0. This would give evidence that proposition 2 is nor a necessary nor a sufficient condition, which means that the proposition is rejected. The further interpretation of this outcome will be discussed in chapter 9.

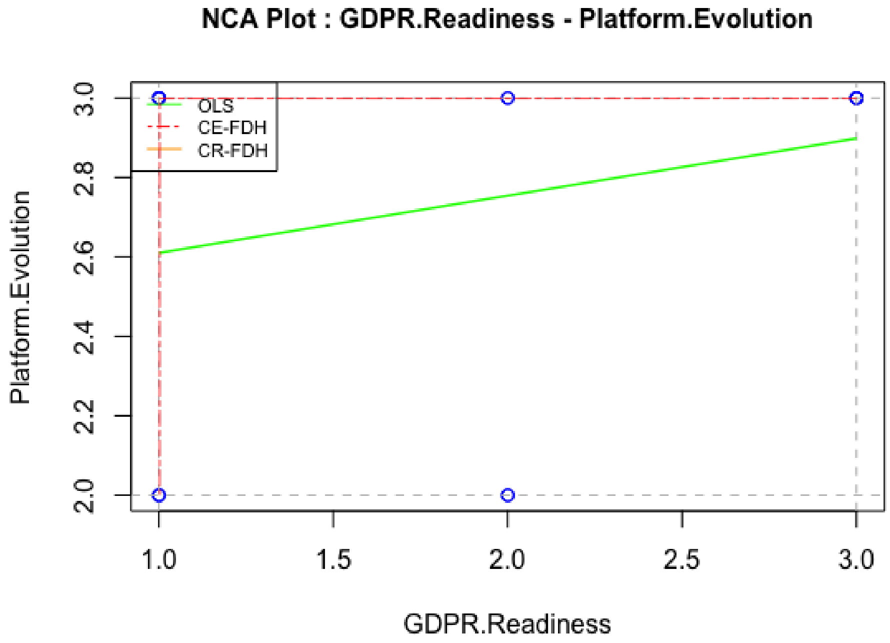


Figure 10: NCA Plot: GDPR.Readiness – Platform.Evolution

6.1.3. Control Mechanisms

As could be seen in table 6, proposition 3a as well as proposition 3b have been accepted by the empirical data that has been gathered from the data of the cases in the questionnaire. The comparison and further discussion of those propositions will be discussed in chapter 8 and 9.

7. Within-case Analysis

7.1. Case A: Rotterdam

Introduction

Rotterdam is the main case in this study, as this thesis is a collaboration with the municipality of Rotterdam and part of the Ruggedised project. As discussed before in chapter 2, Rotterdam is one of the lighthouse cities in the Ruggedised project, which means that Rotterdam will serve as an example. They want to introduce the Heart of South area, in which 13 smart solutions will be implemented (Ruggedised, 2018). This will be designed as an urban data platform that has an architecture with several layers, including data, intelligence, users, and applications. This basic design can be found in Appendix D.

Platform Governance: Gatekeeping

At this moment, it can be concluded that the gatekeeping variable for Rotterdam can be scored as high. KPN is the orchestrator who makes sure the platform works well and can check via tooling whether a third party meets the requirements (van Ravenstein, 2018). If KPN notices that a participant is not compliant, they will notify the city of Rotterdam. From that moment onwards, the city of Rotterdam is the one responsible to deal with this situation. There is no certain committee or protocol available. But although it will be an open data platform, not everyone can have access to all sorts of data. In the end, the GDPR will be the most important governance function.

Platform Governance: Process Control

The level of process control in Rotterdam is being scored as medium. Rewarding and penalizing participants of the platform happens in a natural way, but not by the platform owners. "*Take a look at Facebook, when it is discovered that you are not compliant, you will automatically be penalized*" (van Ravenstein, 2018).

Privacy

The results from the UDP questionnaire show that three out of four privacy protection tools are present on the UDP. The application of the last tool should be applied by the data providers and this is being checked by the platform owner. Therefore, it can be concluded that the privacy metric for the city of Rotterdam can be scored as high.

GDPR Readiness

Both KPN as well as the city of Rotterdam have their own Data Protection Officer and they are working on the data management of their data. As KPN is the orchestrator, they can install buttons that will signal them when someone on the platform does not meet the proposed requirements. They indicate this to the city of Rotterdam so that they can handle the situation. Furthermore, the municipality should have the data register ready at the 25th of May. Every new idea or process will require a privacy impact assessment. "*Concepts that do not directly relate to personal data are being chosen to see if the platform can handle it"* (van Ravenstein, 2018). It can be concluded that the GDPR readiness of the municipality of Rotterdam is high.

Platform Evolution: Resilience

There are various back-up systems that make sure that the platform keeps working. "*Let's say the whole platform would be down due to a failure, then it would be up and running again after one hour"* (van Ravenstein, 2018). Furthermore, the data providers and data customers are not present in the platform. Therefore, when an application has a failure, this has zero effect on the platform. Concluded from this, we can say that the resilience of the city of Rotterdam is high.

Platform Evolution: Scalability

One of the main topics of the Ruggedised project is scalability. *"This is one of the reasons KPN participates in the project"* (van Ravenstein, 2018). If you look at the project Talking Traffic, you can see that this is already possible. Millions of data streams are being used to give real-time information about the traffic in the Netherlands. The next step is the connection with the smartphones and navigation systems of drivers (Talking Traffic, 2018). This capacity for external software services regarding IoT devices comes from KPN and makes it possible to scale up. Therefore, it can be concluded that the scalability of the city of Rotterdam is high.

Platform Evolution: Composability

When a change is being made within the platform, it should not have an effect on the rest of the platform and the data providers and customers. However though, when KPN is working on the servers or functionalities, it could happen that the system collapses for a while. Therefore, the composability of the city of Rotterdam is medium.

Variable	Level	Indicator
Platform Governance		
Gatekeeping	High	Van Ravenstein: "*Although it will be an open data platform, not everyone can have access to all sorts of data*"
Process Control	Medium	Van Ravenstein: "*Take a look at Facebook, when it is discovered that you are not compliant, you will automatically be penalized*"
GDPR Readiness	High	Van Ravenstein: "*Concepts that do not directly relate to personal data are being chosen to see if the platform can handle it*" Klooster: "*So far, there is not a lot of personal data present in the digital city which makes it easier to adapt to GDPR*"
Privacy	High	UDP Questionnaire
Platform Evolution		
Resilience	High	Van Ravenstein: "*When an application has a failure, this has zero effect on the platform*"
Scalability	High	Van Ravenstein: "*One of the main topics of the Ruggedised Project is scalability*" Van der Heijden: "*In theory, it should be possible to work with millions of sensors and data sources*"
Composability	Medium	Klooster: *"When they work on the servers or functionalities, the whole network could collapse for a while"*.

Table 9: Case Overview Rotterdam

7.2. Case B: Utrecht

Introduction

The city of Utrecht is part of a Horizon 2020 EU funded project which has started last October and will last for 5 years. The name of this project is Iris. Utrecht, like Rotterdam in the Ruggedised project, is one of the lighthouse cities. This means that it will be a collaborator and test-bed for the following cities. The district that will be used as a demonstration is Kanaleneiland Zuid (Iris Smart Cities, 2018). As the project just started last October, it is still in the first phase and they have just started to develop the Urban Data Platform. Civity is an external company that is responsible for the construction and management of the platform. They have designed a City Innovation Platform that they implement in several cities throughout Europe (Civity, 2018).

Platform Governance: Gatekeeping

The platform owner of Utrecht will be a local business called Civity. They are specialized in smart cities and can provide a platform. At this moment, the municipality of Utrecht has not discussed who will be the responsible party to control third parties who want to access the platform. However, they have agreed upon the fact that those parties should be controlled on their quality, compliancy and other aspects. *"The UDP users have to comply to restrictions set by data providers and of course GDPR and other legislation"* (UDP Questionnaire, 2018). Furthermore, there are formal processes that a new participant has to go through when they want to join the platform. It can be concluded that the level of gatekeeping for Utrecht is high.

Platform Governance: Process Control

There is no direct process control at the platform of Utrecht, but after third parties have gone through the processes to get access to the platform, they could get paid for the provision of data which can be seen as a reward (UDP Questionnaire, 2018). No fines will be handed out for non-compliant behavior, but parties can be declined further access.

Privacy

Concluding from the UDP Questionnaire, it can be said that privacy can be scored as high.

GDPR Readiness

Utrecht has a new privacy policy since 2016 and since then the new GDPR has been kept in mind. This is a complex task as 90% of the cases consist of personal data. The instalment of a DPA has taken place and for every new idea a privacy impact assessment must be executed. As Utrecht is still at the beginning of their urban data platform, privacy by design can be executed for every new part of data processing. However though, they are not fully GDPR compliant at this moment (UDP Questionnaire, 2018). Some more information comes from The Guardian (2018). They found out that the city of Utrecht keeps track of young people that are hanging out in the streets, including their age group, whether they know each other etc. Therefore, one can conclude that the GDPR readiness of Utrecht is medium.

Platform Resilience

If there is a failure somewhere in the platform, there are multiple back-up hard drives that can substitute the hard drive that is going through the failure. Furthermore, most applications are connected to the platform via API's, which ensures that a malfunction in an application does not have an effect on the platform (Hof, 2018). Concluded can be that the resilience of the city of Utrecht is high.

Platform Scalability

Scalability is one of the starting points of the Iris project. They are working with open standards, work open by default and indicated that data storage and the processing of real-time data is not an obstruction anymore nowadays. The same counts for financial scalability, as the costs of the platform are high in the beginning, but when more applications and end-users will participate, those starting costs decrease with every new participant. Therefore, it can be concluded that the scalability of the city of Utrecht is high.

Platform Composability

Utrecht works with Fireware, which can be described as a big box of Lego with several building blocks. They try to do everything with small modules and components. The roadmap is designed to keep small modules so that the platform will be easy to change and adapt to the constantly changing digital environments (Hof, 2018). Concluded can be that the composability of the city of Utrecht is high.

Variable	Level	Indicator
Platform Governance		
Gatekeeping	High	Kruse: *“The UDP users have to comply to restrictions set by data providers and of course GDPR and other legislation”*
Process Control	Medium	Kruse: “*Data providers can get paid for sharing their data”*
GDPR Readiness	Medium	Kelterman: “*You are never ready*”. Van Impelen: “*The biggest threat are we as humans, mistakes can happen”*
Privacy	High	All privacy protection tools have been check boxed in the UDP Questionnaire.
Platform Evolution		
Resilience	High	Hof: “*When a hard drive malfunctions, replication from other hard drives will automatically start”.*
Scalability	High	Hof: *“Data storage and extra applications or end-users is not an obstruction anymore nowadays”.*
Composability	High	Hof: “*The roadmap is designed to keep small modules in order to make it easy to adapt/change”.*

Table 10: Case Overview Utrecht

7.3. Case C: Eindhoven

Introduction

The city of Eindhoven is participating in several smart city projects, including Triangulation and Synchronicity. The latter is the one that will be analyzed thoroughly in this case. The city council of Eindhoven has expressed the ambition that they want to develop into a city that takes advantage of the upcoming technologies like open data and design thinking, all for the benefit of its citizens. One of the main initiatives is the Smart Society Program (Synchronicity, 2018). Main priority here is to reduce CO2 emissions. This covers areas like energy, environment, planning, mobility and citizen engagement. The program is a collaboration between several cities in Europe and

Platform Governance: Gatekeeping

One can conclude that the level of gatekeeping from the Synchronicity project is medium. Everyone who wants to be part of the urban data platform can apply, after which a committee/jury decides if the third party can be part of the platform. However though, in the end, those third parties are responsible for the quality and compliancy of their data. It can happen that parties with low compliancy get access to the platform but if that gets noticed, those parties will be addressed. Furthermore, the data on the platform is freely available for everyone.

Platform Governance: Process Control

Overall, the level of process control in Eindhoven is medium. Compliancy is something that is expected from third parties. When bad behavior is being noticed, participating apps and app developers can be excluded from the platform. There are no real rewards, but when an application shows that they want to contribute to the platform for the sake of the citizens, the city of Eindhoven always wants to look at ways to help that application in becoming a partner.

Privacy

"*We need to go towards a situation where parties can get trademarks from companies like Deloitte and EY".* When introducing trademarks or something likewise, trust will be gained and that will make your platform succeed. From this information, it can be concluded that the city of Eindhoven does not have privacy protection tools yet. Therefore, the privacy metric will be scored as low.

GDPR Readiness

The city of Eindhoven has used the GDPR since its announcement as a starting point. They have appointed a Data Protection Officer, assessed a risk analysis and will execute a Privacy Impact Assessment for every new use case that arises. Furthermore, they operate mainly in public spaces to avoid that they have to handle personal data. The biggest risk for them, is that they could potentially follow people with their sensors. Before working with those sensors, they think about possible ways how it could harm people and work with privacy by design to prevent the platform from making mistakes (Gluhak, 2018). Therefore, it can be concluded that the GDPR readiness of the platform is high.

Platform Evolution: Resilience

The resilience of the platform from the city of Eindhoven is medium. There is always a fallback scenario, which is how the city of Eindhoven currently operates, which is independently of the platform. When the platform would have a failure, this could hurt applications in a way that they do not receive data for a while. However, the service of the city of Eindhoven should not suffer when that failure would take place. The platform could stop working, but because it mainly operates on the sensors in the public spaces, there would be no actual harm.

Platform Evolution: Scalability

The scalability of the Synchronicity project in Eindhoven is high. Athos is the party that delivers the software to build the platform. That software is made with the intention to make it easy to scale and to be able to process millions of streams of data from various apps. Additional or fewer end-users do not influence the technical performance of the platform (Tiwana, 2014, p. 166 ; Vergeer, 2018). On a financial level, there is no clear idea regarding the scalability.

Platform Evolution: Composability

The composability of the platform of the city of Eindhoven is high. The reason for that is that there are certain standards that have been set up by the platform and the participating apps have to comply to those standards. When the platform executes changes or upgrades, this should only take minimum effort from the applications to re-integrate with the platform (Vergeer, 2018).

Variable	Level	Indicator
Platform Governance		
Gatekeeping	Medium	Schager: *"In theory, it could happen that parties that are not compliant are present on the platform"*
Process Control	Medium	Vergeer: "*Compliancy is something that is expected from third parties"*
GDPR Readiness	High	Vergeer: *"The project operates mainly in public spaces to avoid the handling of personal data"* Gebuis: "*I should be informed about everything regarding personal data within the city of Eindhoven, but this does not happen yet*"
Privacy	Low	Vergeer: "*When introducing trademarks or something likewise, trust will be gained and that will make your platform succeed"*
Platform Evolution		
Resilience	Medium	Vergeer: *"There is always a fall-back scenario, which is how we are operating right now"*
Scalability	High	Schager: "*You should be able to connect everything. You make this possible with open standards and standard data models"*
Composability	High	*Vergeer: "When the platform executes changes or upgrades, this should only take minimum effort from the applications to re-integrate with the platform"*

Table 11: Case Overview Eindhoven

Additional notes

According to Tim Vergeer (2018), the new GDPR regulations can be seen as a chance, rather than a threat, in the development of smart cities. "*It could be a selling point to citizens"* (Vergeer, 2018). If citizens do not believe in the compliancy of your smart city platform, they could try to address that via the media or by approaching the government. This could potentially harm the project which is why Vergeer thinks that it is wise to keep the citizens involved and up-to-date on the compliancy of their platform. According to DPA Gebuis (2018), the execution of a smart city should be very transparent towards the citizens so that they are aware of what is happening at all times.

7.4. Case D: Munich

Introduction

Munich is part of the Smarter Together project. This is a project like the Iris or Ruggedised project, where there are three lighthouse cities and a couple of follower and observer cities. The lighthouse cities in this project are Munich, Lyon, and Vienna. The focus of the project is to find a right balance between ICT technology, institutional governance, and citizen engagement so that they can deliver smart solutions (Smarter Together, 2018). The cities that are part of the project will experiment with smart city components like co-creation and high-quality refurbishment measures to find new ways to add value in urban societies. The aim in Munich is to start an open, secure and city-wide smart urban data platform. That platform should act as a virtual data backbone to transform big data into smart data in order to improve urban planning and the quality of life in urban spaces (Smarter Together Munich, 2018). They already have an IOS app up and running that citizens can use.

Platform Governance: Gatekeeping

In the case of Munich, Siemens is the party who hosts and owns the platform. But that is still a trial project to see what works best. The city of Munich is collaborating with them to write a data gatekeeper which will decide who and what kind of data can access the platform. This data gatekeeper will make sure that the right parties and the right data flow into the platform (Montag, 2018). It can be concluded that the gatekeeping level of the city of Munich is high.

Platform Governance: Process Control

There will be rules regarding process control, but those rules have not been implemented yet. Normally they describe it in the use case. This is not being done automatically yet, but will be part of the platform. From this, it can be concluded that the level of process control of the city of Munich is high.

GDPR Readiness

One part of the data gatekeeper is to describe the rules and to tell the stakeholders what they are allowed to do and what they are not allowed to do. For Munich, the goal is to make everything as transparent as possible. They have developed a transparency dashboard that is part of the platform where they describe for each use case what they collect, how they collect it, and what they do with it. The idea of this comes from a co-creation workshop with the citizens (Montag, 2018). It can be concluded that the GDPR readiness of the city of Munich is high.

Privacy

All the privacy protection tools are part of the Urban Data Platform of Munich (Montag, 2018; UDP Questionnaire, 2018). Therefore, it can be concluded that the level of privacy is high in the city of Munich.

Platform Evolution: Resilience

There was no knowledge available about this metric yet. Therefore, this metric will be left out for this case.

Platform Evolution: Scalability

The platform of the city of Munich is a cloud-based platform. From a technical perspective, the scalability is there (Montag, 2018). For the users or programmers, they use API's so that should be easy to connect to the platform. The basic idea of the platform was that everyone in the city could access the platform. Furthermore, is the addition of data or the addition of applications feasible. It can be concluded that the scalability of the urban data platform from the city of Munich is high.

Platform Evolution: Composability

When a change or an upgrade happens within the platform, it should be easy for everyone else in the ecosystem to reintegrate with the platform. However, the city of Munich is not in that phase of the platform yet (Montag, 2018). Regarding the future, we can conclude that the composability of the city of Munich is going to be high.

Variable	Level	Indicator
Platform Governance		
Gatekeeping	High	Montag: "*In the data platform there is a data gatekeeper registry and this is the instance to influence the smart data platform"*
Process Control	High	Montag: "*One thing that we do not want to have on the platform, and will penalize, is privacy data"*
GDPR Readiness	High	Montag: *"Well I think it is ready, one part of the data gatekeeper is to describe the rules"*
Privacy	High	Montag: "*All the privacy protection tools are part of the UDP"*
Platform Evolution		
Resilience	-	-
Scalability	High	Montag: *"From a technical perspective, the scalability is there"*
Composability	High	Montag: "*The idea is that it should be very simple to reintegrate"*

Table 12: Case Overview München

Additional findings

The most important thing regarding the GDPR regulations according to Montag (2018), is that the people that are working with the platform are aware of these new regulations. The technical aspect should not be the hardest part. Most of the people that are working with the data and analyzing the data are not really aware of those new regulations. In his eyes, the GDPR regulations are absolutely positive for a smart city. "*It is the best thing that could happen" (*Montag, 2018).

8. Cross-case Analysis

In this chapter, the cross-case analysis will be discussed. As stated before, the previous chapter, which consists of the within-case analysis, accelerates the cross-case analysis. This analysis will compare the selected cases to search for patterns that arise throughout the various cases that have been analysed. This makes it possible to test the propositions that have been drafted in chapter 4. This will eventually lead to the rejection or acceptation of the propositions.

8.1. Findings

In table 13, the cross-case analysis can be observed. It states all the various aspects of the variables and the score that has been assessed throughout the interviews and supporting documentation. As discussed before, a proposition will be accepted when half of the cases or more than half of the cases score a high or low value (as the medium scores do not count) that is in line with the proposition.

Case	Rotterdam	Utrecht	Eindhoven	Munich
Control Mechanisms	**High**	**High**	**Medium**	**High**
Gatekeeping	High	High	Medium	High
Process Control	Medium	Medium	Medium	High
GDPR readiness	**High**	**Medium**	**High**	**High**
Privacy				
Privacy Protection Tools	**High**	**High**	**Low**	**High**
Platform Evolution	**High**	**High**	**High**	**High**
Resilience	High	High	Medium	-
Scalability	High	High	High	High
Composability	Medium	High	High	High
Propositions				
Proposition 1	Yes	Yes	No	Yes
Proposition 2	Yes	No	Yes	Yes
Proposition 3a	Yes	Yes	No	Yes
Proposition 3b	Yes	Yes	No	Yes

Table 13: Cross-case Analysis

8.2. Reflection on propositions

8.2.1. Privacy Protection Tools

Proposition 1: *A high level of privacy protection tools positively influences the level of evolution of an urban data platform.*

		Privacy Protection Tools		
Platform Evolution		Low	Medium	High
	High	Eindhoven		Rotterdam, Utrecht, Munich
	Medium			
	Low			

Table 14: Scatter Plot on Empirical Findings on Proposition 1

Observation

What can be observed in table 14 is that three out of four cases support proposition one. As discussed before in chapter 5.4.2. the NCA analysis will determine if a high level of a variable is a necessary condition or not. This would be the case if the upper left spot in the table would be empty. Regarding this proposition, this is not the case, as Eindhoven scored low on privacy protection tools. This means that the ceiling zone for this proposition is zero. What can be concluded is that privacy protection tools are not a necessary, and not a sufficient condition to have a high evolution of your platform.

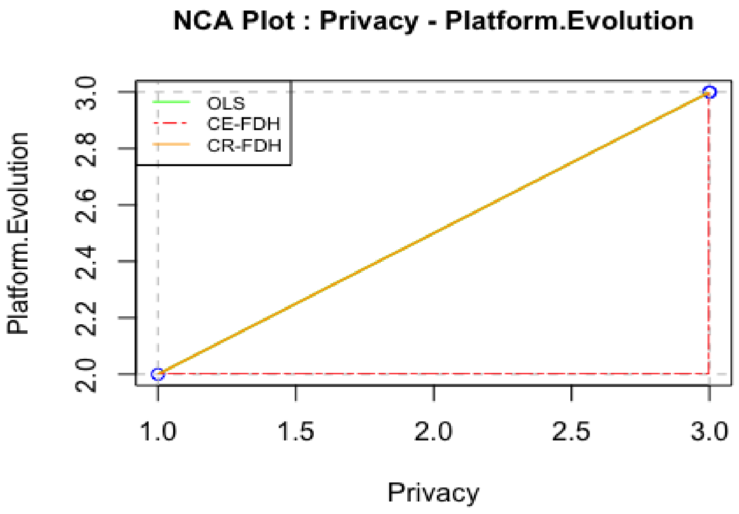


Figure 11: NCA Plot: Privacy – Platform.Evolution

Interpretation

Although the NCA analysis shows that privacy protection tools are not necessary to reach high evolution of your platform, the interviews indicated that a high level of privacy protection tools seems to generally increase the possibility of a high level of platform evolution. One of the important aspects of the privacy protection tools is the information transparency with your citizens. Stakeholders from all cases indicated that it is important to be transparent towards your citizens in order to gain their trust and eventually have a more successful platform. One example comes from Munich where Montag (2018) stated that they try to involve citizens at all times when building and implementing their platform. They make use of co-creation so that citizens know that their opinion is being valued. Furthermore, they have implemented a transparency dashboard where a description of how the data is collected and what they are going to do with the data is being given for each use case. This stimulates citizens to join the platform and help building it further.

Finding 1: *Information transparency is something that is valued by citizens and what can potentially lead to a higher success of the platform.*

Moreover, Eindhoven did not have the right privacy protection tools in place at the moment, but was definitely certain that it would stimulate the platform: "*When introducing trademarks or something likewise, trust will be gained and that will make your platform succeed"* (Vergeer, 2018). The answers from Utrecht and Rotterdam came out the UDP Questionnaire, so there is no elaborative evidence on the relationship between privacy protection tools and the evolution of a platform. However, some extra information has been gathered through some open questions at the end of the interviews. Mr. van Ravenstein from KPN (2018) indicated that the need for more data and information as well as the need for privacy are increasing. A platform that can answer both needs, will be a platform that can grow and evolve into a successful platform. Furthermore, stakeholders from the city of Utrecht indicated that gaining trust from your citizens by making sure that you can ensure a certain level of privacy, will stimulate them to join their platform.

Finding 2: *Privacy protection tools positively influence the level of evolution of an urban data platform.*

8.2.3. GDPR Readiness

Proposition 2: *A high level of GDPR readiness positively influences the level of evolution of an urban data platform.*

		GDPR Readiness		
Platform Evolution		Low	Medium	High
	High		Utrecht	Rotterdam, Eindhoven, Munich
	Medium			
	Low			

Table 15: Scatter Plot on Empirical Findings on Proposition 2

Observation

As can be observed in table 15, three out of four cases support the proposition, as cases with a medium outcome were not taken into account. The empty area in the upper left corner of table 12 implies that there is a necessary condition. This gives evidence that proposition 3 is a necessary but not sufficient condition, which means that a high level of GDPR readiness must be present in order to achieve a high level of platform evolution, but its presence is not sufficient to obtain a high level of platform evolution.

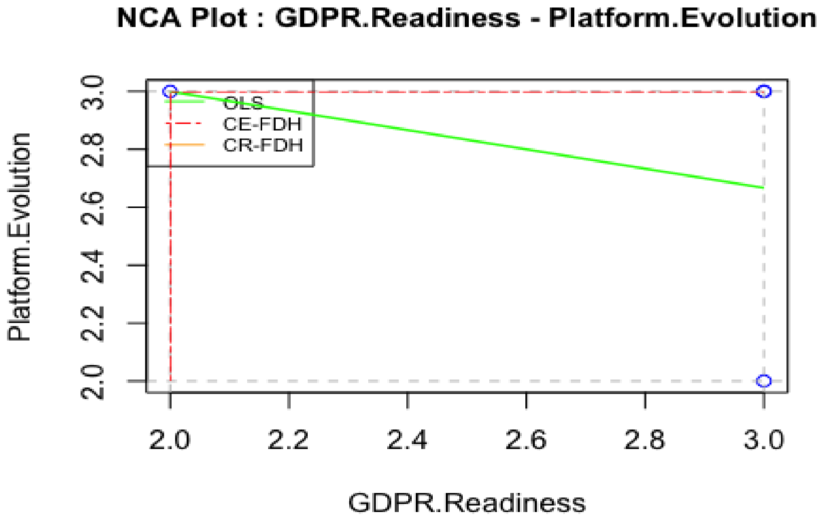


Figure 12: NCA Plot: GDPR.Readiness – Platform.Evolution

Interpretation

As discussed in the previous paragraph, it can be concluded that with a high level of GDPR readiness, it will be likely that the evolution of a platform will be scored high as well, and that it could be regarded as a necessary condition. There is no literature present on the direct relation between those two, there is however though literature present that depicts the GDPR as a positive change towards a trustworthy European Union (Albrecht, 2016). Although the results from the interviews do not show a direct relation between the two variables, some extra questions have been asked to gather thoughts about the perceived impact from the GDPR on the evolution on a platform. What was interesting here was the fact that there are two camps: one side thinks that it will impede the speed of innovation from a smart city, and the other side sees opportunities in the new regulations by gaining trust from citizens and getting everyone onboard with new smart city solutions. The first camp consists mainly of IT developers and the other camp consists mainly of business people. Both sides agreed that they need to speak more often with each other in order to keep up with the changing regulations and privacy issues. However though, the overall conclusion from both parties is that you need to make sure that you are compliant according to the GDPR regulations in order to keep your platform alive. Some stakeholders referred to the recent issues Facebook is facing regarding their compliancy and they all acknowledged the need for compliancy and trust.

Finding 3: *Communication between platform owners, business developers, and other stakeholders is necessary to make sure that GDPR is not an impediment but an accelerator.*

8.2.1. Control mechanisms

Proposition 3a: *A high degree of control mechanisms implemented by platform owners will positively moderate the effect of the degree of GDPR readiness on the level of evolution of an urban data platform.*

	Concept	Rotterdam	Utrecht	Eindhoven	Munich
Independent Variable	GDPR readiness	High	Medium	High	High
Moderator	Control mechanisms	High	High	Medium	High
Dependent Variable	Level of evolution	High	High	High	High
Evidence		Yes	Yes	No	Yes

Table 16: Evidence on moderating effect control mechanisms

Observation

It can be observed in table 16 that three out of four cases demonstrate evidence that control mechanisms positively moderate the effect the relationship between GDPR readiness and the level of evolution of an urban data platform. All three cases demonstrate the use of control mechanisms so that they can control the behaviour from participants of the urban data platform.

Interpretation

Control mechanisms are not only used to ensure certain quality levels within the platform ecosystems. All cases indicated that they use or will use some form of gatekeeping to ensure that participants of the ecosystem are GDPR compliant. The way of controlling is quite different though. In Rotterdam, Utrecht, and Munich certain tools within the platform need to make sure that a new participant provides data with the right quality and compliancy. For Eindhoven however, there is a certain committee that judges which parties gain access and which not. But this is a check to see if the third party can be of value for the platform and is not based on quality or compliancy. Process control was harder to touch upon for all cases, as they do not make use of rewards or penalties yet, but stated for instance that third parties with low compliancy would be pushed out of the ecosystem. Furthermore, rewarding did not seem to be something that would be used, solely in the form of payments for data.

Finding 4: *A high degree of control mechanisms implemented by platform owners positively moderates the effect of the degree of GDPR readiness on the level of evolution of an urban data platform.*

The striking point in the answers during the interviews was the fact that the division of governance was missing sometimes. With the tooling that is being used in Rotterdam, Utrecht, and Munich it can be seen which third parties do not comply with the requirements and compliancy of the urban data platform. However, after that step, it is not always clear who should be the party responsible to address the third party.

Finding 5: *The division of governance and ownership of data in an urban data platform is not always clear, which makes it hard to decide who needs to take responsibility*

Proposition 3b: *A high degree of control mechanisms implemented by platform owners will positively moderate the effect of privacy protection tools on the level of evolution of an urban data platform.*

	Concept	Rotterdam	Utrecht	Eindhoven	Munich
Independent Variable	Privacy Protection Tools	High	High	Low	High
Moderator	Control mechanisms	High	High	Medium	High
Dependent Variable	Level of evolution	High	High	High	High
Evidence		Yes	Yes	No	Yes

Table 17: Evidence on moderating effect control mechanisms

Observation

What can be observed from table 17 is that like with proposition 3a, three out of four cases demonstrate evidence that control mechanisms moderate the relation between privacy protection tools and the level of evolution. From the within-case analysis it became clear that every case makes use of some control mechanism to stimulate the desired behavior from participants in the platform ecosystem. However though, process control was scored medium three out of four times. This is due to the fact that most platforms are not completely up and running yet and they did not know for sure how they would implement process control in their platforms. For instance, the rewarding of good behavior had not been thought about yet.

Interpretation

Similar to proposition 1a, Rotterdam and Munich score high on every variable. Both cities have a good system for their control mechanisms which already makes sure that the privacy protection tools are present in the Urban Data Platform. All cities stated that they make use of gatekeeping to make sure that only third parties that prove to be a fit to the platform will be included. This is not only based on the right fit, but also on compliancy and quality (Montag, 2018). Third parties that can ensure quality, compliancy, and the right data for the urban data platform will attract more end-users. With the increase of end-users, more third parties will be attracted to build applications on the platform. This is an example of positive cross-side network effects (Tiwana, 2014) and will stimulate the evolution of the urban data platforms.

Finding 6: *A high degree of control mechanisms implemented by platform owners positively moderates the effect of privacy protection tools on the level of evolution of an urban data platform.*

Again, Eindhoven is the one that does not support the proposition. Although they make use of gatekeeping and process control in some form, no effect on the level of evolution could be noticed. This is for the reason that they do not make use of any privacy protection tools, which makes it hard for the control mechanisms to have a moderating effect.

8.3. Supporting propositions

Based on empirical evidence gained through the four cases that have been researched in this study, the developed propositions have been tested and evaluated with a cross-case analysis. Table 18 demonstrates which of these propositions have been accepted and which propositions have been rejected.

Proposition	Supporting cases	Rejecting cases	Accepted
1	3	1	Yes
2	3	1	Yes
3a	3	1	Yes
3b	3	1	Yes

Table 18: Accepted propositions

Proposition	Questionnaire	In-depth cases	Accepted
1	Yes	Yes	Yes
2	No	Yes	Yes
3a	Yes	Yes	Yes
3b	Yes	Yes	Yes

Table 19: Comparison findings questionnaire and in-depth cases

What can be concluded from table 19, is that all propositions have been accepted. The only proposition that has been rejected by one side, is the second proposition regarding the direct relation between GDPR and platform evolution. The explanation for this will be further scrutinized in the discussion.

9. Discussion

This chapter will discuss the findings from the cross-case analysis in order to find out if there is alignment between the existing literature that has been used in this thesis. If this is not the case, new literature will be assessed so that the empirical findings can be supported.

9.1. Privacy Protection Tools

From both the cross-case analysis from the questionnaire as well as the cross-case analysis from the interviews, a positive relation between privacy and platform evolution can be observed. The only difference between the two analyses is that for the cross-case analysis from the interviews, it was neither a necessary nor a sufficient condition while in the questionnaire it was a necessary, but not sufficient condition. This is due to the fact that Eindhoven did not make use of privacy protection tools. However though, they did see the importance of privacy protection tools while further developing their platforms (Vergeer, 2018). These findings are in line with previous findings on the effect of privacy on choices that consumers make. It corresponds with findings from Chellappa (2005), where they argue that the greater the presence of trust factors, the greater the chance a consumer will make use of the products or services from the vendor. Li et al. (2012) concluded from their studies that providing privacy signs will positively impact customers' likelihood of making use of personalization. These signs create trust for customers so that they are more willing to disclose personal data.

As said before by Lit et al. (2012), trust-creating actions can make customers/third parties make more frequently use of platforms and can lead to a higher acceptance of personalization. Therefore, four privacy protection tools have been developed by Li. Furthermore, from the within-case analyse came forward that privacy protection tools will positively influence the evolution of a platform:

"*When introducing trademarks or something likewise, trust will be gained and that will make your platform succeed*" (Vergeer, 2018)

There is a transparency dashboard with a description of each use case, how the data is collected, what we do with the data, so that citizens can see what we are doing with the data in the city and they have indicated that this stimulates them to use the platform". (Montag, 2018)

From the questionnaire it appeared that every case made use of privacy protection tools. This was either being done by the urban data platforms themselves or required from the data providers that are connected to the platform. Concluding from this information can be that privacy protection tools gain a certain level of trust from the citizens, which will stimulate them to join the platform. Eventually this will lead to a higher scalability and therefore has a positive effect on the short-term evolution of a platform.

9.2. GDPR Readiness

A higher level of GDPR readiness positively influences the short-term evolution of a platform, and in this case particularly an urban data platform. What turned out to be the case in the questionnaire, is that this proposition did not hold. Some cases indicated that they did not have installed a Data Protection Officer yet, or were not working by privacy by design. Unfortunately, no further information could be obtained from them due to time constraints. Therefore, it is hard to say to what extent some of the answers are to be trusted. This is one of the limitations that will be discussed in chapter 10.

However though, during the in-depth interviews with the other four cases, three out of four cases supported the proposition. During those interviews, it became clear that the general opinion was that GDPR compliancy will help a platform flourish. This is both for the reason that it prevents smart cities of getting fines from the AP, but it also makes sure that they obtain a certain level of trust from the citizens. People have the right to know what kind of effects certain data streams have on their privacy and would feel more connected to a city if there is a good understanding of what is happening within those platforms (Gebuis, 2018).

Furthermore, although there is not much literature to be found on GDPR, and especially not on the effect of GDPR on platforms, the existing literature complies with the findings from this study:

"*It is the best thing that could happen". (Montag, 2018)

"GDPR will bring more legal certainty and can serve as a starting point for international standards and will make the EU a trustworthy digital market" (Albrecht, 2016).

"Privacy is also the foundation for trust. We know that people will only use technology that they trust. Ultimately, trust is created when people are confident that their personal data is safe and they have a clear understanding of how and why it is used" (Brill, 2018).

What can be noticed from these findings, GDPR and privacy are closely related and comply each other. As there is not much existing literature on GDPR, this is something that could be studied more thoroughly. This will be touched upon in chapter 10 where the directions for future research will be discussed.

9.3. Control Mechanisms

As the role of platform owners is more like an orchestrator instead of a manager, it seems right to make use of governance mechanisms to be able to still have some sort of influence. Therefore, the use of control mechanisms as a moderating effect on the relationship between privacy and GDPR readiness, and short-term evolution has been researched.

First of all, the results show us that the use of control mechanisms positively moderate the level of GDPR readiness on the short-term evolution of a platform. As stated before, gatekeeping was the most important control mechanism, as many platforms did not know for sure how to make use of process control. This is due to the fact that they are not in right phase of their lifecycle yet.

The findings on control mechanisms contribute to the existing literature from Bresnahan and Shane Greenstein (2014). They did research on various software platforms, consisting of Apple and Google. Apple has a strict approval process for all apps. Thereby they want to guarantee a certain level of quality and safety to their end-users. Google's platform Android was being governed in a nonhierarchical way and did not have the control over the distribution of apps. *"The lack of control of information has led to some coordination failures and fragmentation, as different hardware vendors have created different, sometimes incompatible, devices"* (Bresnahan & Greenstein, 2014). This demonstrated the need to for platform owners to step up and intervene in some platform processes by using these control mechanisms.

Furthermore, like Tiwana (2014) discussed, a purpose of platform control is to facilitate coordination between the platform and the app developers that are connected to the platform. If apps can seamlessly interoperate and integrate with a platform, the level of composability will be high. Therefore, the usage of control mechanisms will be a positive moderator that will enable the short-term evolution of a platform.

10. Conclusion

The main goal of this thesis was to gather information on the effect of the new GDPR on the evolution or success of an urban data platform. With the research that has been done, guidance for urban data platform managers is provided in order to succeed in the management of their platform. The main case for which the research has been done is Rotterdam, a lighthouse city in the Ruggedised project. The overarching research question: *"What is the perceived impact of GDPR on the short-term evolution of an urban data platform?"* has been answered with: **a high level of GDPR readiness has a positive effect on the evolution of an urban data platform, by scrutinizing four cases via in-depth interviews and 18 cases via a questionnaire that has been send out to urban data platform managers throughout Europe**. The logic behind this positive effect complies with the logic that has been presented in the scarce literature that has been written on GDPR. During the interviews, it also became clear that the majority of the interviewees believe that a high level of GDPR readiness will have a positive effect on your urban data platform. Therefore, even though the questionnaire rejected the proposition, it can be concluded that there is a positive relation. Both methods have used a cross-case analysis to improve the accuracy and reliability of this study. Furthermore, cross-case analyses increase the probability of finding novelties in the data.

10.1. General Conclusion

The aim of this research was to study the perceived impact of the GDPR regulations on the evolution of a platform, and in particular an urban data platform. With the usage of a questionnaire and a multiple-case study these concepts have been scrutinized and several useful findings were the result of this analysis. Firstly, it has been observed that a high degree of GDPR readiness leads to a greater success of the evolution of a platform.

Furthermore, the use of privacy protection tools ensures a certain level of trust from citizens, which in the end leads to a positive effect on the evolution of a platform. When people feel that the city and its platform are to be trusted, they are more eager to join the platform and share their own data for instance. A good example how that trust can be obtained is the transparency dashboard of the city of Munich. Moreover, multiple interviewees stated that the creation of trust from citizens will positively influence the success of a platform. If you find the right balance between providing as much data as possible and protecting the privacy of your citizens, the urban data platform will flourish.

Thirdly, the use of control mechanisms has proven to create a higher degree of privacy and GDPR readiness and therefore, they positively moderate the effect between one of those and the short-term evolution of a platform. What came out of the interviews, was the fact that they often used gatekeeping to ensure a certain level of GDPR compliancy and privacy. Process control is not being used that often, as has been discussed in chapter 9.3. The use of those control mechanisms align the governance and architecture of a platform which allows a platform to have a high level of composability. Therefore, it can be concluded that they have a positive effect on the short-term evolution of a platform.

A summary of the general findings can be find below:

Finding 1: *Information transparency is something that is valued by citizens and that can potentially lead to a higher success of the platform.*

Finding 2: *Privacy protection tools positively influence the level of evolution of an urban data platform.*

Finding 3: *Communication between platform owners, business developers, and other stakeholders is necessary to make sure that GDPR is not an impediment but an accelerator.*

Finding 4: *A high degree of control mechanisms implemented by platform owners positively moderates the effect of the degree of GDPR readiness on the level of evolution of an urban data platform.*

Finding 5: *The division of governance and ownership of data in an urban data platform is not always clear, which makes it hard to decide who needs to take responsibility*

Finding 6: *A high degree of control mechanisms implemented by platform owners positively moderates the effect of privacy protection tools on the level of evolution of an urban data platform.*

10.2. Theoretical Contributions

This study contributes to existing theories in various ways. As stated before, platform ecosystems and smart cities are relatively new concepts and there is a need for better understanding on how they work. Smart cities or urban data platforms are being developed in every part of the world and the management and governance of those platforms are topics that have not completely been understood yet.

Firstly, this study has various contributions to existing literature on topics like GDPR, privacy, and platforms ecosystems. With Tiwana (2014) as a guidance, it has tested and validated his existing theories on platform ecosystems. As platform ecosystems and smart cities are relatively young subjects, there is no excessive literature to be found on those topics, which makes this study a good addition to the existing literature. The privacy protection tools from Li et al. (2012) that have been used to test a certain level of privacy, have been connected to the evolution of a platform and has proven to have a positive effect. It was known that privacy protection tools created trust among customers, but the relation between privacy and the evolution of a platform ecosystem had not been tested yet.

Secondly, two of the control mechanisms that have been designed by Tiwana (2014) have been used to test if there is a moderating effect on the relations between privacy and evolution, and GDPR readiness and evolution. Gatekeeping is not always the right mechanism, as it will allow less third parties and could scare potential other third parties. However though, this study provides evidence that the usage of control mechanisms will have a positively moderating effect on proposition 1 and proposition 2. It will make sure that the level of GDPR readiness and privacy stays high, so that a positive effect on the evolution of an urban data platform can be realized.

Lastly, not only existing concepts have been tested and validated. New concepts like GDPR have been discussed so that a relation between GDPR and the evolution of a platform could be tested. As the GDPR has just been implemented since the 25th of May, this is a very young subject that has not been studied a lot. There was no existing literature on the relation between GDPR and the evolution of a platform, so these novel findings could be a direction for future research on platform ecosystems.

10.3. Practical Implications

Regarding managerial recommendations, this research can serve as a guidance for managers so that they can realize a high evolution for their platform. The focus on the new GDPR regulations, the importance of privacy and its privacy protection tools, and the short-term evolution of a platform ecosystem, might help platform owners to develop their platform.

The findings from this study are related to concepts from academic literature with the addition of several case studies and therefore it could be of value when bridging the gap between academic literature and practice. Platform owners, and in particular the platform owners of the urban data platform of Rotterdam, can test their own practices against the other cases in this study so that differences or similarities can be discovered. This could help them with reflecting on their current operations, GDPR readiness, the usage of control mechanisms and how this all relates with each other.

An important recommendation that came forward during the interviews, is to make sure that there is information transparency towards citizens and that there are trust-creating tools present. This has also been discussed in 9.1.

Furthermore, what can be seen in the newspapers these days, is that companies who do not treat the privacy of their customers rightfully, will be penalized for their actions. This can happen in the form of fines, but also by damaging of their reputation. A recent example of this is Facebook. Therefore, it is of great importance that platforms make sure that they are GDPR compliant. What came forward during the interviews is that platforms who can meet the need for more real-time info and data, combined with the need for privacy, will be the platforms that are going to flourish.

10.3.1. Managerial Recommendations Ruggedised

As this study is a collaboration with the city of Rotterdam, which is part of the Ruggedised project as a lighthouse city, there are some special recommendations for them. Even though Umea and Glasgow have not filled in the questionnaire, they are Lighthouse cities of Ruggedised and the data that has been gathered from Rotterdam can be used to give recommendations to all three of them.

First of all, what came forward from the interviews with stakeholders from the smart city project in Rotterdam is that there need to be good agreements on who the platform owner(s) will be in order to prevent miscommunication and bad governance. It seemed like the ownership of the platform, and therefore the governance of the urban data platform, was not completely clear. Even though gatekeeping is being used via tools in the platform KPN has developed, it was not clear who should be the one to tell a third party to adjust their compliancy or who should remove a third party when that is necessary.

Secondly, during an interview with Klooster (2018) from Future Insights, it became clear that the various stakeholders did not completely understand each other. There is no common language between IT developers and business people and therefore they tend to talk in ways that the other party does not understand. This can cause the implementation of the wrong tools or functionalities which will eventually steer the platform in the wrong direction.

Lastly, the need for privacy and the creation of trust is a topic that came forward throughout most of the interviews. Therefore, it would be good for Rotterdam to follow the steps from the urban data platform in Munich. With the usage of co-creation workshops and information sessions about the implementation of the urban data platform, you involve citizens in the process which will create a certain level of trust. This will make it easier to convince them to join the platform and share parts of their personal data. In the end, this will lead to the positive evolution of the platform.

10.4. Limitations

This study holds several limitations regarding the scope of the research, the methods that have been used and the cases that have been scrutinized.

Firstly, as this study conducted a multiple-case study with solely four cases and 18 other cases from a questionnaire, this could lead to limitations for generalizability and could be seen as subjective and a lower level of representativeness. With interviews, the author always has relatively high influence on the research. Working with a larger sample could improve the generalizability and validity of this study.

Secondly, even though several interviews have been conducted per case for triangulation purposes, many of the findings depend on the point of view from the interviewee and the score the author gives the several metrics. For two out of four cases, only people from the municipality were able to participate in an interview which could lead to biased outcomes. Furthermore, the cases have been picked by the author himself, which could enable a potential bias and subjectivity from the author.

Thirdly, the measurement constructs that have been developed to score dependent variables, were all treated equally. The variables that have been studied throughout this study have been classified as low, medium, or high, where the usage of multiple levels could have been better. Moreover, this can generate extreme scores which could harm the richness of insights that have been gathered. This could for instance overestimate the impact of a certain variable.

Fourthly, the findings from the cross-case analysis about the questionnaire are not from the same level as the findings from the in-depth interviews of the other four cases. People might have filled out the survey without complete knowledge of the meaning of each question and did not have the opportunity to clarify themselves like the people during the interviews.

Fifthly, due to time constraints and the scope of this thesis, not all concepts that influence platform evolution have been studied. There are certainly more concepts that influence the evolution of a platform, which could be included in future research. One of those concepts is for instance the architecture of a platform. Due to the scope of this study, these elements could not be incorporated in the research design.

Lastly, as GDPR is quite a new concept. Not much literature has been written about GDPR, and certainly not about the influence of GDPR on a platform ecosystem or urban data platform. This made it hard to touch upon certain relations between variables. Furthermore, most cities are at the forefront of their urban data platform and could not answer every question with certainty as some things were just not running yet.

10.5. Directions for Future Research

As platform ecosystems, urban data platforms, and GDPR are quite new concepts in the academic world, this study offers multiple opportunities for future research.

Firstly, a replication of this study could be done within a different context. As this study has been written in collaboration with the city of Rotterdam, the scope of this research was a smart city, and in particular an urban data platform. Therefore, the multiple-case study has been conducted among other smart city initiatives. It could be interesting to replicate this study in other cities around the world or other industries, as companies also deal with the new GDPR. This could contribute to the generalizability of this study.

Secondly, as this thesis relies mainly on the writings of Tiwana (2014) but only scrutinizes two control mechanisms and the short-term evolution metrics, future research could examine the other control mechanisms in relation to other evolution metrics. The relation between GDPR and mid-term metrics could for instance be tested, as GDPR would already be implemented for a while and smart cities would be in a different phase as well.

Concluding could be that overall, platform ecosystems, smart cities, and GDPR are concepts that are quite unexplored so far. This gives possibilities for future research. The new GDPR regulations will significantly change the way we work around privacy and that gives lots of interesting research. Furthermore, smart cities are being implemented in more and more countries, and it would be interesting to observe the various phases that they will go through.

Bibliography

Albrecht, J. P. (2016). *How the GDPR Will Change the World*. Eur. Data Prot. L. Rev., 2, 287.

Al-Heeti, A (2018) *Microsoft says it's extending GDPR rights to consumers worldwide,* Accessed: 25-05-2018, URL: https://www.cnet.com/news/microsoft-says-its-extending-gdpr-rights-to-consumers-worldwide/

Allwinkle, S., & Cruickshank, P. (2011). *Creating smart-er cities: An overview*. Journal of urban technology, 1*8*(2), 1-16.

Ayres, L., Kavanaugh, K., & Knafl, K. A. (2003). *Within-case and across-case approaches to qualitative data analysis*. Qualitative health research, *13*(6), 871-883.

Baldwin, C. Y., & Clark, K. B. (2006). *The architecture of participation: Does code architecture mitigate free riding in the open source development model?*. Management Science, 52(7), 1116-1127.

Baldwin, C. Y., & Woodard, C. J. (2008). *The architecture of platforms: A unified view*

Bartoli, A., Hernández-Serrano, J., Soriano, M., Dohler, M., Kountouris, A., & Barthel, D. (2011, December). *Security and privacy in your smart city*. In Proceedings of the Barcelona smart cities congress (pp. 1-6).

Berrone, P., Ricart, J.E., Carrasco, C. (2016). *The Open Kimono: Toward A General Framework for Open Data Initiatives in Cities,* California Management Review 2016, Vol. 59 (1) 39-70.

Boudreau, K. (2010). *Open platform strategies and innovation: Granting access vs. devolving control.* Management Science, 56(10), 1849-1872.

Bresnahan, T., & Greenstein, S. (2014). *Mobile computing: The next platform rivalry*. American Economic Review, *104*(5), 475-80.

Brill, J. (2018) *Microsoft's commitment to GDPR, privacy and putting customers in control of their own data*, Accessed: 25-05-2018, URL: https://bit.ly/2IE3ffy

Chellappa, R. K., & Sin, R. G. (2005). *Personalization versus privacy: An empirical examination of the online consumer's dilemma*. Information technology and management, 6(2-3), 181-202.

Dowden, M., Jones, G. (2016) *Smart cities need smart laws*, Womble Bond Dickinson LLP, Accessed at: 24-01-2018. URL: https://www.lexology.com/library/detail.aspx?g=6f80ba1b-76d4-4ee1-b8b8-1714f07216e4

Dul, J. (2016). *Necessary condition analysis (NCA) logic and methodology of "necessary but not sufficient" causality.* Organizational Research Methods, 19(1), 10-52.

Eisenhardt, K. M. (1989). *Building theories from case study research.* Academy of management review, 14(4), 532-550.

Elmaghraby, A. S., & Losavio, M. M. (2014). *Cyber security challenges in Smart Cities: Safety, security and privacy.* Journal of advanced research, *5*(4), 491-497.

Evans, D. S., & Schmalensee, R. (2007). *Catalyst code: the strategies behind the world's most dynamic companies*. Harvard Business School Press.

Fildes, N. (2017) *Meet the "connected cow",* Financial Times.

Flyvbjerg, B. (2006). *Five misunderstandings about case-study research.* Qualitative inquiry, 12(2), 219-245.

Gluhak, A. (2018) *SynchroniCity: Delivering an IoT enabled Digital Single Market for Europe and Beyond,* Accessed: 01-05-2018. URL: https://bit.ly/2rheAXK

Griffinger, R., Fertner, C., Kamar, H., Kalasek, R., Pichler-Milanovic, P., Meijers, E. (2007) *Smart cities – Ranking of European medium-sized cities,* Vienna University of Technology

Green Digital Chapter (2017) *What can cities do to protect privacy?* Accessed 04-01-2018 URL: http://www.greendigitalcharter.eu/tag/gdpr

GDPR (2017) *GDPR Key Changes*, Accessed: 05-01-18,
URL: https://www.eugdpr.org/key-changes.html

Hersen, M., & Barlow, D. H. (1976). *Single case experiment designs*.

Hollands, R. G. (2008). *Will the real smart city please stand up? Intelligent, progressive or entrepreneurial?*. City, 12(3), 303-320.

Ishitani, L., Almeida, V., & Meira Jr, W. (2003). *Masks: Bringing anonymity and personalization together.* IEEE Security and Privacy, *1*(3), 18-23.

Jadoul, M. (2017) *Why smart cities should adopt an open ecosystem on a horizontal platform*, Open Ecosystem Network, accessed: 18-01-18, URL: https://open-ecosystem.org/articles/why-smart-cities-should-adopt-open-ecosystem-horizontal-platform

Jonker, U. (2017) *Belastingdienst hield ICT-systeemcrisis onder de pet*, accessed: 20-02-18, URL: https://fd.nl/economie-politiek/1232267/belastingdienst-hield-ict-systeemcrisis-onder-de-pet

de Joode, A. (2011) *Effective corporate security and cybercrime*, Network Security Volume 2011, Issue 9, September 2011, p. 16-18.

Kimchi, J., Polivka, B., & Stevenson, J. S. (1991). *Triangulation: operational definitions.* Nursing research, 40(6), 364-366.

Langheinrich, M. (2001). *Privacy by design—principles of privacy-aware ubiquitous systems.* In Ubicomp 2001: Ubiquitous Computing (pp. 273-291). Springer Berlin/Heidelberg.

Letaifa, S.M. (2015) *How to strategize smart cities: Revealing the SMART model*, Journal of Business Research 68, p. 1414-1419

Li, T., & Unger, T. (2012). *Willing to pay for quality personalization? Trade-off between quality and privacy*. European Journal of Information Systems, 21(6), 621-642.

Lowijs, J. (2018) *Master thesis interview Deloitte.*

Malyon, P. (2017) *What are the most important elements of the GDPR,* Accessed: 25-05-2018, URL: https://www.edq.com/uk/blog/what-are-the-most-important-elements-of-the-gdpr/

Mulligan, C.E.A. (2013) *Architectural Implications of Smart City Business Models: An Evolutionary Perspective,* IEEE Communications Magazine

Petronio, S. (2012). *Boundaries of privacy: Dialectics of disclosure*. Suny Press.

Roberts, J.J. (2017) *Why Google, Facebook, and Amazon should worry about Europe,* Accessed: 04-02-2018, URL: http://fortune.com/2017/07/20/google-facebook-apple-europe-regulations/

Rowley, J. (2002). *Using case studies in research*. Management research news, 25(1), 16-27.

Rubin, H. J. (85). Y Rubin, IS (1995) *Qualitative interviewing. The art of hearing data.*

Ruggedised (2017) *About Ruggedised,* Accessed: 03-01-2018
URL: *http://www.ruggedised.eu/project/about/*

Ruggedised (2017) *Rotterdam*, Accessed: 08-04-2018
URL: http://www.ruggedised.eu/cities/rotterdam/

Shih, F. J. (1998). *Triangulation in nursing research: issues of conceptual clarity and purpose*. Journal of advanced nursing, 28(3), 631-641.

Sieber, S. D. (1973). *The integration of fieldwork and survey methods.* American journal of sociology, 78(6), 1335-1359.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). *Information privacy: measuring individuals' concerns about organizational practices.* MIS quarterly, 167-196.

Talking Traffic (2018) *Clusters and expertise,* Accessed on: 26-04-2018
URL: https://www.partnershiptalkingtraffic.com/

Tankard, C. (2016). *What the GDPR means for businesses*. Network Security, *2016*(6), 5-8.

Tiwana, A. (2014). *Platform ecosystems: aligning architecture, governance, and strategy*. Newnes.

United Nations (2017) *World population to hit 9.8 billion by 2050, despite nearly universal lower fertility rates – UN,* Accessed on: 04-01-2018,
URL: http://www.un.org/apps/news/story.asp?NewsID=57028#.WlH10ZPygWp

Vermerris, A., Mocker, M., & Van Heck, E. (2014). *No time to waste: the role of timing and complementarity of alignment practices in creating business value in IT projects*. European Journal of Information Systems, 23(6), 629-654.

Yin, R. K. (2013). *Case study research: Design and methods*. Sage publications.

De Weck, O. L., Roos, D., & Magee, C. L. (2011). *Engineering systems: Meeting human needs in a complex technological world*. MIT Press.

van Zoonen, L. (2016). *Privacy concerns in smart cities*. Government Information Quarterly, 33(3), 472-480.

Case Study Sources

Civity (2018) *City Innovation Platform*, Accessed: 25-04-2018
URL: https://www.civity.nl/city-innovation-platform

Van der Heijden, R. (2018) *Master thesis interview.*

Hof, A. (2018) *Master thesis interview.*

Van Impelen, H. (2018) *Master thesis interview.*

Iris Smart Cities (2018) *Utrecht, The Netherlands*, Accessed on: 12-04-18
URL: http://irissmartcities.eu/content/utrecht-netherlands

Gebuis, T. (2018) *Master thesis interview.*

Kelterman, S. (2018) *Master thesis interview.*

Klooster, R. (2018) *Master thesis interview.*

Kruse, T. (2018) *Master thesis interview.*

Kruse, T. (2018) *Questionnaire Urban Data Platforms*, Accessed on: 01-05-2018

Montag, U. (2018) *Master thesis interview.*

Van Oosterhout, M. (2018) *Master thesis interview.*

Van Ravenstein, R. (2018) *Master thesis interview.*

Schager, R. (2018) *Master thesis interview.*

Smarter Together (2018) *We are smarter together*, Accessed on: 23-05-18

URL: https://www.smarter-together.eu/

Smarter Together (2018) *Munich,* Accessed on: 23-05-2018
URL: https://www.smarter-together.eu/cities/munich#/

Synchronicity (2018) *Eindhoven,* Accessed on: 12-04-18,
URL: https://synchronicity-iot.eu/cities/eindhoven/

Vergeer, T. (2018) *Master thesis interview.*

Vieveen, F. (2018) *Master thesis interview.*

11. Appendices

11.1. Appendix A: Introduction e-mail

Beste ..,

Mijn naam is Daniel Bos, ik ben een Master student Informatiemanagement aan de RSM, Erasmus Universiteit. Sinds januari heb ik het genoegen om een afstudeeronderzoek binnen het Ruggedised project te mogen doen (zie link naar project onderaan mail). Mijn onderzoek is toegespitst op de verwachte impact van de invoering van de nieuwe GDPR op een urban data platform. De GDPR zal vanaf 25 mei worden ingevoerd en dit heeft grote gevolgen voor het verzamelen en analyseren van data binnen een smart city. In mijn onderzoek stel ik de vraag of de GDPR gereedheid van een smart city invloed heeft op de evolutie/het succes van een smart city. In samenspraak met mijn coaches is besloten om verschillende case-studies uit te voeren bij stakeholders van het Ruggedised project of andere smart city initiatieven, waarna ik door Jaap Dekker ; strategisch i-adviseur, gemeente Rotterdam (010-2671704) op uw expertise gewezen ben.

Bent u bereid om mij middels een persoonlijk gesprek kennis bij te brengen over uw verwachtingen rondom de impact van de GDPR? De personen/functies die voor mij interessant zijn, zijn de volgende: Functionaris Gegevensbescherming, CISO en / of CIO, GDPR/AVG specialist, Business Developer.
De ervaring leert dat een dergelijk gesprek ongeveer één uur in beslag neemt. Ik ben vrij flexibel in mijn beschikbaarheid en ik kan me voorstellen dat u een volle agenda heeft, dus wellicht kunt u kijken of het ergens in de week van 26 maart of in de week van 2 april lukt. Ik hoor graag over uw beschikbaarheid in deze periode.

Met vriendelijke groet,

Daniel Bos

http://www.ruggedised.eu/cities/rotterdam/

11.2. Appendix B: Case Study Protocol

Case Study Protocol Elements	Applicability to this study
An overview of the case study project	Overview of the case study project is covered in chapter 1 till 5.
Field procedures	- Access has been gained to the key organizations and interviewees - Sufficient resources in the field were present - Clear schedule of data collection activities has been made - Provision for unanticipated events
Case study questions	The interview protocol has been used while conducting the interviews (Appendix D).
A guide for the case study report	There is a clear table of contents available that serves as a guide through the several cases.

Table 20: Case Study Protocol (Source: Yin, 2013)

11.3. Appendix C: Validity & Reliability

Tests	Case study tactic	Phase of research in which tactic occurs
Construct validity	Use multiple sources of evidence	Interviews have been conducted, a survey has been sent out, exploratory interviews and public available information are used.
	Establish chain of evidence	Every case has been researched thoroughly and described in detail.
	Have key informants review draft case study report	Interviewees have the chance to comment on the interview transcript, but not on the actual report.
Internal validity	Do pattern matching	Propositions based on the literature have been tested via a cross-case analysis.
	Do explanation building	Has not been applied to this study.
	Do time series analysis	Has not been applied to this study.
External validity	Use replication logic in multiple case studies	Propositions could be validated by making use of comparable cases.
	Use case study protocol	Case study protocol has been developed and is being used for the interviews.
Reliability	Develop case study database	The interviews have been recorded and transcribed, and additional information has been collected.

Table 21: Validity & Reliability

11.4. Appendix D: Interview Protocol

Interview Protocol

1. **Introduction** In the beginning of the interview, the following aspects of the interviews were discussed:

- Aim and scope of the interview
- Conditions regarding confidentiality
- Format of the interview
- Duration

2. **General Question** Thereafter, the current position of the employee was asked.

3. **Platform Governance**: Thereafter, questions were asked about variables of interest regarding the governance of the platform, namely gatekeeping and relational control.

a. **Governance Gatekeeping (Rustenburg, 2016)**

- Is there an (extensive) process/protocol which determines which parties gain access and which parties do not?
- Is there a committee/individual/organ in the organization that actively judges which parties gain access and which do not?
- Is the process regarding the acceptance of- and contribution to the platform clearly documented and available to the developers?
- Is the data freely available to similar stakeholders at the same time?
- Is the roadmap of the platform available to all developers?

b. **Process Control**

- To what extent does the platform reward or penalize specific behaviour?
- Are there any rules, methods or procedures participants have to follow?
- Is compliancy being rewarded and to what extent?

4. **How would you, in general, describe the degree of GDPR readiness in your organization?**
   - **a.** Our Urban Data Platform is not GDPR compliant
   - **b.** We have done a risk analysis
   - **c.** We have done a risk analysis, and we have installed a Data Protection Officer
   - **d.** We have done a risk analysis, we have installed a Data Protection Officer, and we have done a Privacy Impact Assessment
   - **e.** We have done a risk analysis, we have installed a Data Protection Officer, we have done a Privacy Impact Assessment, and we make use of Privacy by Design – we are fully GDPR compliant

- What are your measures regarding Privacy by design?
- How do you make sure you can still find all the data that is being saved to be able to handle requests regarding the ‘Right to be forgotten’?

5. Privacy Protection Tools have been developed to get customers/citizens to trust companies. The platform owner can check if these protection tools are in place when parties want to access the urban data platform. *Check the applicable box for each protection tool that is being checked when a new party wants access.*

Protection Tool	Check box
Anonymity of data (pseudonyms)	
Presence of a privacy statement	
Presence of a security seals	
Information transparency with citizens	

6. Platform Evolution

Scalability

To measure platform evolution in terms of scalability, the interviewee is asked to describe the latency, the responsiveness of the platform, an estimate of error rates for each additional or fewer end-user or app at the platform level. The same estimate will be asked for financial scalability: where does the break-even occur?

- To what extent is the platform scalable?
- What is the capacity of a subsystem to support a larger/smaller number of end-users/apps/external software services?

Composability

- When a change is being made within an app, how much effort does it take to reintegrate with the platform or with the other apps?
- When a change is being made within the platform, how much effort does it take to reintegrate with the other apps within the ecosystem?

- **Resiliency**
  - How does the platform perform when there is a failure somewhere in or outside of the platform?
  - How is the bounce back when an app on the platform malfunctions?

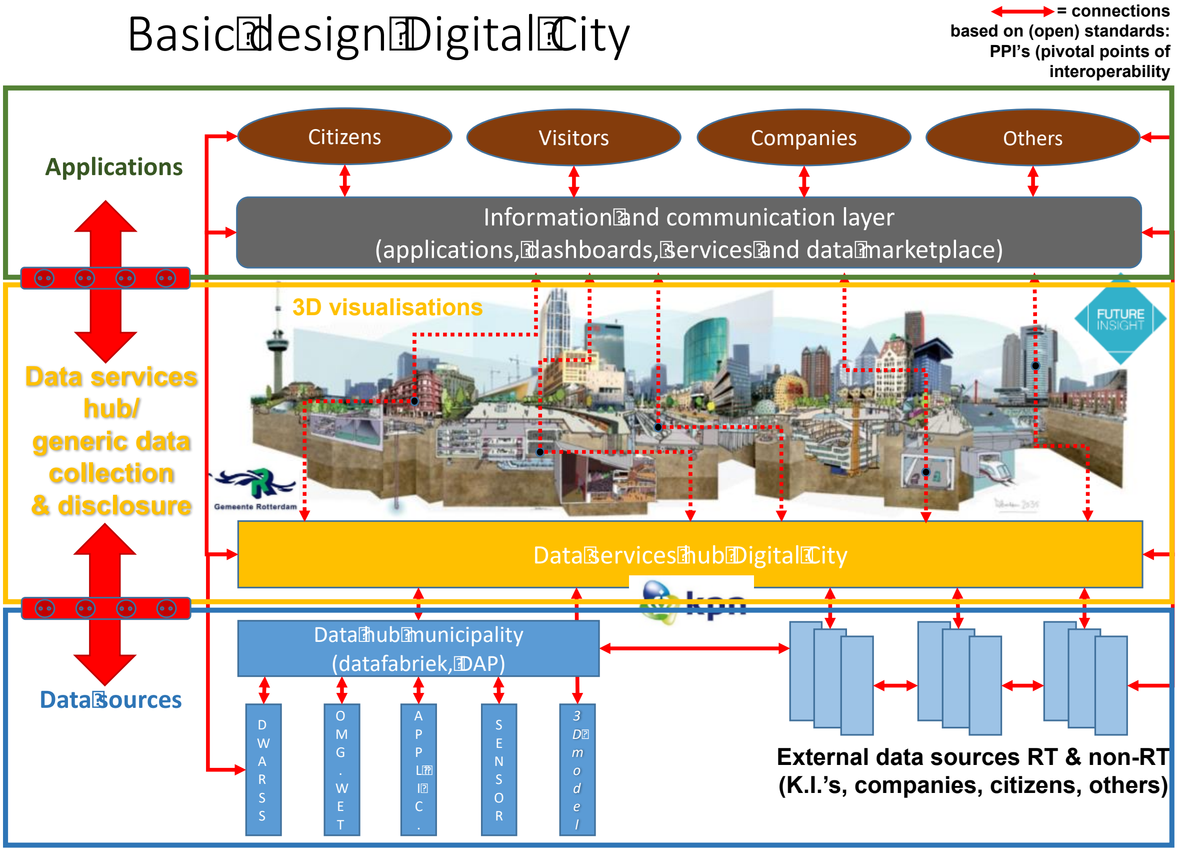
General performance

- Which factors influence performance?
- *(Could GDPR be a cause of lower/higher performance?)*

7. Supporting documentation

- Do you possess any useful documentation that I might use to find out more about your platform?
- Do you have any other useful insights on the GDPR regulations regarding your urban data platform?
- Could you think of other people that could give valuable insights regarding this topic?

11.5. Appendix E: Basic Design Digital City



Basic design Digital City

= connections based on (open) standards: PPI's (pivotal points of interoperability

Applications

Citizens

Visitors

Companies

Others

Information and communication layer (applications, dashboards, services and data marketplace)

3D visualisations

FUTURE INSIGHT

Data services hub/ generic data collection & disclosure

Gemeente Rotterdam

Data services hub Digital City

kpn

Data hub municipality (datafabriek, DAP)

DWARSS

OMG.WET

APPL I C.

SENSOR

3D model

External data sources RT & non-RT (K.I.'s, companies, citizens, others)

Data sources

Source: Van der Heijden, R. (2018)

11.6. Appendix F: R script NCA Analysis

Case	Control Mechanisms	GDPR Readiness	Privacy	Platform Evolution
Helsinki	1	3	3	3
Munich	3	3	3	3
Florence	3	1	3	3
Bristol	2	1	2	2
Tartu	3	3	2	3
Nantes	2	2	2	3
Utrecht	3	2	3	2
Barcelona	2	1	3	2
Hamburg	2	1	3	3
Cologne	2	3	3	3
Lyon	1	1	2	3
San Sebastian	3	2	2	2
Milan	3	1	2	3
Rotterdam	3	2	3	3
Valencia	2	1	3	3
Tampere	2	3	3	3
Pamplona	3	1	3	3
Kozani	3	1	3	2

Table 22: NCA Analysis input Questionnaire

Case	Control Mechanisms	GDPR Readiness	Privacy	Platform Evolution
Rotterdam	3	3	3	3
Utrecht	3	2	3	3
Eindhoven	2	3	1	2
Munich	3	3	3	3

Table 23: NCA Analysis input multiple-case analysis

```
#install.packages("data.table")
library(data.table)
library(NCA)
setwd("~/Documents/BIM/Thesis Data Security")
data <- fread("NCA2.csv")
str(data)
nca(data, c("Control.Mechanisms","GDPR.Readiness","Privacy"),"Platform.Evolution")
```