Aalto University
School of Business

Utilizing open data in a cross-border smart city

Overview of data subject's rights and attitudes under GDPR

Master's Thesis

Jesse Leino
Aalto University School of Business
Information and Service Management

Spring 2021

Aalto University
School of Business

Aalto University, P.O. BOX 11000, 00076 AALTO
www.aalto.fi

Abstract of master's thesis

Author	Jesse Leino
Title of thesis	UTILIZING OPEN DATA IN A CROSS-BORDER SMART CITY
Degree	Master of Science in Economics and Business Administration
Degree programme	Information and Service Management
Thesis advisor(s)	Hadi Ghanbari & Matti Rossi
Year of approval	2021
Number of pages	107
Language	English

Abstract

Smart city has been an emerging trend as late as from the 90's and many modern cities aspire to be smart. For a smart city to be efficient, it needs to gather data about its residents, thus it is paramount that the city administration that aspires to implement smart city services to acknowledge citizens' preferences and privacy concerns regarding that data collection. Smart city applications will have to work under regulation but also need to seem safe and appealing for citizens. Smart city initiatives often utilize open data generated from different applications and services in the city, and this thesis reviews promising smart city applications powered by open data. I am basing my research on earlier literature about smart cities and provide definitions for smart cities and open data as well as discuss open data enabled services and the enabling technologies of these services. The main contributors for emergence of smart city services are enabling technologies and the services can be divided into subgroups of services, smart people, smart living, smart environment, smart governance, smart economy and smart mobility. The regulatory body referred to in this thesis is the European Data Protection Regulation (GDPR) as the cities used in my thesis, Helsinki and Tallinn are both in the EU. I review the regulatory requirements set by the GDPR for digital smart city applications utilizing open data gathered from citizens. The main areas of GDPR regarding smart city data collection are the principles relating into processing of personal data and the rights of the data subject. I also survey citizens attitudes and preferences regarding data collection for smart city purposes. The findings of the survey suggest that citizens hold more value to their privacy and security than user experience when addressing digital smart city services. The thesis aims to support digital implementation of FinEst-Twins – a smart city initiative between Helsinki and Tallinn. FinEst-Twins is the first global cross-border smart city Center of Excellence and it focuses on mobility, energy, built environment, governance, and urban analytics & data.

Keywords smart city, open data, digital services, privacy, information security

Contents

List of Tables

List of Figures

1 Introduction

1.1 Research motivation

As the urbanization of the world is at hand, it is crucial that cities and other communities answer the needs of the growing population. It has been estimated that almost three quarters of the world´s population will live in urban areas by 2050 (UN 2011). This creates an incentive for cities to operate at the best possible level and requires them to adopt new technologies to enable basic services. Smart cities are now answering this need of new, interactive and technology oriented urban living space.

Smart City has been a trendy term since the 90s, and it is very appealing for many cities to label themselves as smart cities. Everyone wants to be smart. The definition of smart city is not universal however, and some researchers have criticized this trend of labelling every city with even minor ICT applications "smart" (Hollands, 2008), and therefore in this thesis the term 'smart city' is thoroughly defined before the actual literature review.

For a smart city to be efficient, it needs to gather data about its residents. For example, to conduct an optimal public transportation network, the developers of that network should have strong understanding of where and when citizens travel daily, meaning that they need location data from citizens.

Open data provides many opportunities for digital innovations and developing novel digital solutions in smart cities. However, these services must comply with different regulations and at the same time they must be appealing to citizens and consider their preferences. Smart city initiatives often utilize open data generated from different applications and services in the city. Like in the previous public transportation example, data is generated through citizen's personal public transportation tickets when they tag them to a reader in the public transportation vehicles. The public transportation network developers can view this data and adjust the network by adding buses or trams to high traffic areas and timings. Open data raises many questions related to privacy and the consent of the data subject. ''Connected devices have generated new types of data, and new types of privacy concerns. As more products are equipped with sensors that track location, usage, condition, and other information, marketers can offer new products and features that seem to deliver higher quality (Hoffman & Novak, 2018; Porter & Heppelmann, 2014). However, such products and features also allow consumer information to be used in new contexts,

potentially threatening entrenched norms and generating privacy concerns. Personal health or fitness trackers, for instance, feed consumer data directly into the cloud to facilitate consumer activity dashboards and comparisons with peers. If this data gets used for a purpose other than fitness tracking, such as for insurance or credit scoring, the new context for the data would likely raise privacy concerns.'' (Bleier, et al., 2020)

I have studied the relation between open data and smart city initiatives by reviewing relevant literature and observing FinEst Twins (http://www.finesttwins.eu/) – a smart city initiative between Helsinki and Tallinn. Finest-Twins is the first global cross-border smart city Center of Excellence (CoE) and it focuses on solving urban challenges related to mobility, energy, built environment, governance, and urban analytics & data. I find it important to research the effects of open data related to this smart city initiative, as it is the first cross-border smart city CoE. As an entity in the EU, FinEst Twins CoE must comply with the GDPR, but since it extends between two EU states, cross-border users may have different preferences due to the diverse cultural background of the citizens. Therefore, I aim at understanding how these concerns should be combined while developing cross-border smart city services.

As the regulatory environment regarding consumer data protection tends to be homogenous across the European Union due to the European Data Protection Regulation (GDPR), I'm using it as a general framework when discussing data subject´s rights. I think it is important to research and recognize the opportunities and risks related to a cross-border smart city and its open data backed-up services.

1.2 Research problem and theoretical framework

The goal of my thesis is to look into promising smart city applications powered by open data. I also aim to look for the pain points of the applications regarding data management and to be more precise, consumer data protection. This thesis is divided to one major research question and two minor questions as follows:

- How open data could be used for developing digital services in cross-border smart cities?
    - What are the regulatory requirements set by the GDPR of using cross-border open data for developing digital services?
    - What are the attitudes and privacy concerns of citizens regarding data processing in smart city context?

The articles regarding these subjects are numerous and new digital services enabled by open data emerge continuously providing a fruitful field for research. As these services often collect data from citizens, I found it rather strange that data privacy regarding these applications is rarely mentioned. As the research regarding these applications rarely discuss privacy and the rights of the data subjects, this thesis aims to fill the research gap in consumer data protection and the problem of data usage related to the consent of the data subject. GDPR is my main tool for studying rights of the data subjects and I survey citizens from Helsinki and Tallinn to acquire a holistic view of the citizen´s perspectives and attitudes regarding the data collection and processing for smart city services. I am basing my research on earlier literature about smart cities. I provide definitions for smart cities and open data and discuss open data enabled services and the enabling technologies of these services I am also going to study in my literature review how the consent of the data subject is considered in smart city applications.

In this thesis I'm using GDPR as one of the main tools to conduct my research. GDPR is the most influential regulation in the European region and in cross-border smart city setup it is highly relevant regarding digital services that are powered by open data. The principles of GDPR are lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality as well as accountability (GDPR, art. 5). These principles form an essential part in my survey, as the respondents are asked to rank these principles to screen their attitudes towards different aspects of data protection. I

have assembled the principles of GDPR in the table below with deeper explanations of their meaning.

Table 1. Principles of GDPR

	Personal data shall be:
Lawfulness, fairness and transparency	processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not to be incompatible with the initial purposes
Data minimization	adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
Storage limitation	kept in form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject
Integrity and confidentiality	processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with these principles

(GDPR, art. 5, 2018)

Technology Acceptance Model (TAM) is an information systems theory that aims to explain how users come to accept and use technology. TAM is another theoretical tool for my research, paired with the GDPR. There are various implications of TAM, but in this thesis, I am using five distinctive elements that have been recognized in TAM models in earlier literature. The TAM elements to be compared are 'perceived ease of use' (Venkatesh & Davis, 2000), 'perceived usefulness' (Venkatesh & Davis, 2000), 'self-efficacy' (Karimi & Niknami, 2011), 'cost reduction' (Roca et al., 2006) and 'time saving' (Roca et al., 2006). I adopted TAM to my thesis as it offers suitable elements to compare with the GDPR principles. In the survey, the respondents will have to compare and rank the GDPR principles and TAM elements with each other, leading to a holistic view of how these attributes are perceived by the public.

The third theoretical tool in my thesis is the theory of basic human values by Schwartz (2012). This theory is a well-known set of basic human values that form a widely accepted values structure from social sciences. I am using this theory to gain a more humane meaning for the GDPR principles as the legal definitions of the principles are somewhat stiff. According to Schwartz (2012) human values can be divided to basic values that include all the core values recognized in cultures around the world. The values are self-direction, stimulation, hedonism, achievement, power, face, security, tradition, conformity, humility, benevolence, and universalism. These values are explained in more detail in the table below.

Table 2. Schwartz's human values

Human values	**Definitions**
Self-direction - thought	Freedom to cultivate ones own ideas and abilities
Self-direction - action	Freedom to determine ones own actions
Stimulation	Excitement, novelty, and change
Hedonism	Pleasure and sensuous gratification
Achievement	Success according to social standards
Power-dominance	Power through exercising control over people
Power-resources	Power through control over resources
Face	Maintaining ones public image and avoiding humiliation
Security - personal	Safety in ones immediate environment
Security - societal	Safety and stability in the wider society
Tradition	Maintaining and preserving cultural, family or religious traditions
Conformity - rules	Compliance with rules, laws, and formal obligations
Conformity - interpersonal	Avoidance of upsetting or harming other people
Humility	Recognizing one's insignificance in the larger scheme of things
Benevolence - caring	Devotion to the welfare of in-group members
Benevolence - dependability	Being reliable and trustworthy member of the in-group
Universalism - nature	Preservation of the natural environment
Universalism - concern	Commitment to equality, justice and protection for all people
Universalism - tolerance	Acceptance and understanding of those who are different from oneself

(Perera et. al. 2019

Perera et. al. (2019) have mapped the values with the principles of GDPR by recognizing links between a certain principle and basic human values. In their research the links are either explicit or implicit. For instance, if we examine the GDPR principle of '*accuracy*' which grants the data subject the right to have inaccurate data rectified or erased without delay, has an *explicit* link with '*power – resources'* human value, which is defined as power through control over resources (Perera et. al. 2019). Thus, the data subject has power over their personal data under the accuracy principle.

Furthermore, if inaccurate personal data were to be stored of an individual, it could in certain circumstances affect the public image of that individual. This implies that the '*accuracy*' principle has also an *implicit* link with the '*face*' human value of Schwartz's theory – maintaining one's public image and avoiding humiliation (Perera et. al. 2019). In the following figure I have assembled the mappings of the GDPR principles and Schwartz's human values by Perera et. al. (2019) with their implicit and explicit links. Note that all the principles are directly linked to *privacy* and *self-direction – action*, these links are not shown for the sake of clarity.

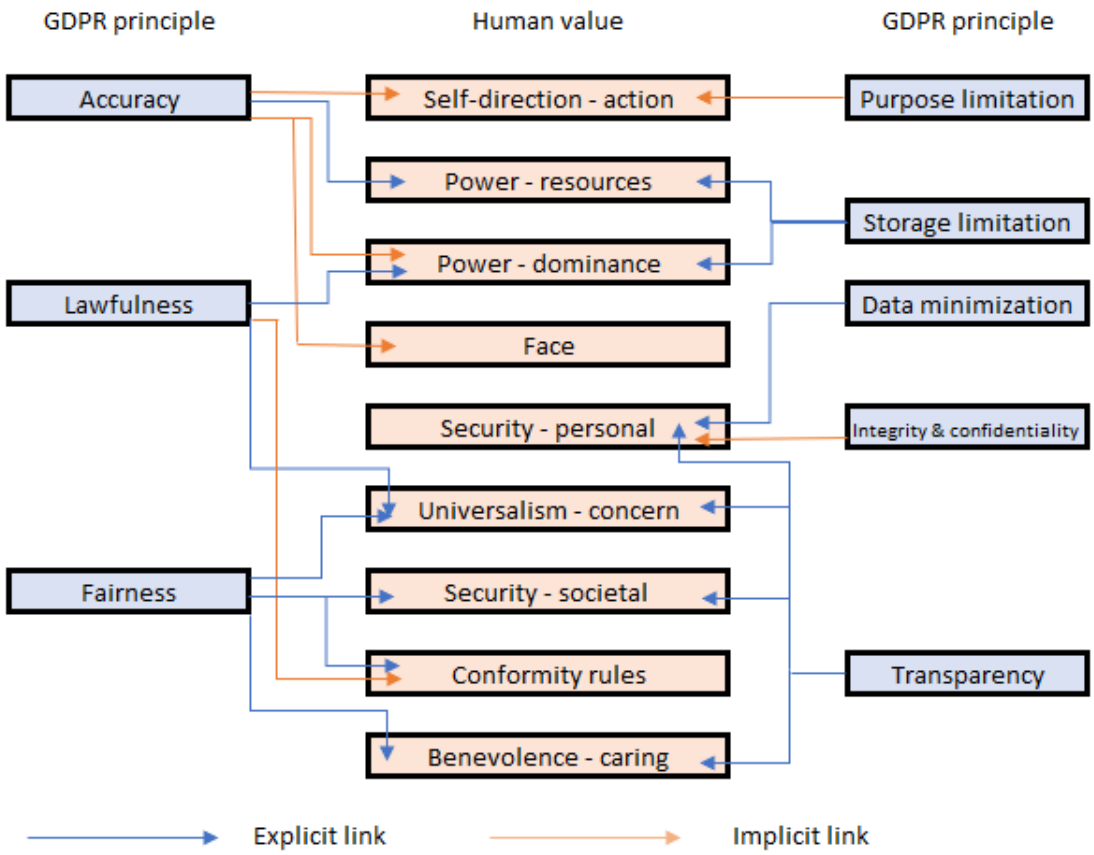


Figure 1. GDPR principles mapped with human values
(Perera, et al. 2019)

As seen in the figure, all of the GDPR principles can be linked to Schwartz's human values either explicitly or implicitly and most of the principles even have several links to human values. I find this combination of regulatory principles and humane aspect not only fascinating but also relevant to the FinEst Twins project. Smart city applications will have to work under regulation but also need to seem safe and appealing for citizens. In this thesis, I am setting the following preliminary hypothesis: *the GDPR principles that have stronger links to human values are seen as more important by the citizens than those with weaker links.*

Thus, should the hypothesis be correct, FinEst Twins should look at the important principles more closely and figure out which principles affect a certain service and how to highlight to the consumers that the principle is being considered in a service or application. Thus, I am identifying which GDPR principles and TAM elements are seen as the most appealing from the citizens perspective. I am comparing the perception of the respondents of the TAM elements and GDPR principles. My goal is to compare which attributes are viewed as the most important by the citizens comparing security and privacy characteristics of a service through GDPR with its benefits set by TAM. I will also try to capture the preferences of specific demographic groups (e.g. nationality, age, education). This enables me to provide theoretical and practical implications on the influence of users' preferences and concerns in the development of digital services in cross-border smart city context.

1.3 Structure of the thesis

The thesis consists of seven chapters. First being the introduction, second being the methodology and third being the literature review about smart cities and their digital applications. After the literature review, I introduce the regulatory requirements set by the GDPR in chapter four. Fifth chapter consists of my survey of citizen's attitudes towards data processing and finally conclusions are presented in chapter six. The references and appendixes will be after the conclusions. The first meta part is naturally the table of contents, and the lists of tables and figures in which the reader can navigate straight to the section the find interest in. After the table I have listed the relevant tables and figures in the thesis.

In the second chapter I will introduce the thesis subject and explain why I find it important to research this subject and provide a theoretical framework regarding the subject. In the methodology section I will explain how I conducted my research, introducing the tools

and websites I used to look for relevant literature, and go in detail how I conducted the empirical part of my thesis.

The fifth chapter consists of the literature review in which I will discuss the relevant earlier literature considering my subject. The chapter consists of several subchapters varying from digital services to data privacy and regulatory challenges regarding open data applications. After the literature review, I have conducted my empirical research and discuss the results of the research. The empirical research is conducted by a survey of citizens in Helsinki and Tallinn as well as discussing European Data Protection Regulation.

Finally, the last chapter consists of findings from my empirical research and the conclusions that I have drawn regarding the earlier literature and the empirical results. After conclusions you will find the list of references and appendixes.

2 Methodology

2.1 Research methodology

In this thesis I have conducted a literature review to identify relevant research on the topic and an online survey to collect empirical data as well as an overview of the GDPR principles to follow when processing citizen's data. First, I am going to briefly introduce my literature review process and then the process of collecting my secondary data source GDPR, and finally the research process of the survey part of the thesis.

Webster and Watson (2002) state that the major contributors to offer knowledge about a certain topic under investigation is likely to be the leading journals. Thus, the major references for my literature review were conducted from scientific journals regarding ICT and smart cities. As my subject is closely related to the newest ICT applications and digital services, the publications that I have included in my literature review should not be outdated. For example, articles regarding digital services from the 90's will probably not be relevant in today's smart city environment. Furthermore, I used a process suggested by Webster and Watson (2002) of using keyword searches in Google Scholar, ProQuest and ScienceDirect among others to search keywords such as 'smart city', 'open data', 'smart city services' and 'open data enabled digital services' to name a few. Should I find an article that was cited by many other authors or be otherwise special in its relevance to my topic, I would follow the forward as well as backward citations of that article.

As for my secondary data source GDPR, I naturally searched through the regulation to find relevant parts regarding my thesis. I used the official website of GDPR (www.gdpr-info.eu) to review the articles and recitals that I needed. I mainly used chapters 2 and 3 which cover the principles of the regulation as well as the rights of the data subject as those are the main subjects that I am discussing in this thesis under the regulatory framework. These chapters cover articles 5 – 23 and recitals 39-73. I did review the articles from the official regulation and assembled them as tables to the thesis. As some articles use cross referencing with other articles, I did write those parts by hand rather than use cross referencing myself for the sake of clarity and readability. After every table that introduces a certain article, I added a short text to further explain the contents of the table. These are mainly referencing from the recitals that support the article in question.

For the empirical part I assembled a questionnaire which surveys citizens digital orientation, their use of digital services and their attitudes towards data processing in the

light of GDPR principles. I conducted the survey using Discover, which is a streamlined, web-based survey platform for choice analytics by Sawtooth Software. The survey consisted of four questions related to demographic background, a single question about digital orientation, two questions about their concerns towards data processing of service providers and a question about their familiarity with the GDPR. Finally, the respondents were asked to rate the attributes of GDPR and TAM through best-worst-scaling in twelve different scenarios. The best-worst scaling is a method of data collection in which the respondents provide top and bottom ranked items from a list. The method is used to obtain more choice data from individuals and to understand choice processes (Louviere et. al., 2015). I will present the survey later in chapter 7.

2.2 FinEst Twins

FinEst Twins is a cross-border smart city initiative between Helsinki and Tallinn. The agents of this initiative are Tallinn University of Technology, Forum Virium Helsinki, Aalto University and the Ministry of Economic Affairs and Communications of Estonia. I will use FinEst Twins as the case example in my thesis for the cross-border smart city concept, and therefore find it important to explain the initiative (Soe, 2017).

The vision of the FinEst Twins project is to build an ICT-driven Smart City Centre of Excellence (CoE) based in Estonia, and it aims to mobilize all leading actors and stakeholders in Estonia. Furthermore, the project seeks to establish a long-term partnership with their Helsinki region counterparts, capitalizing on the macro region´s scientific knowledge, innovativeness and entrepreneurship, and act as a reference and hub for cross-border scientific and innovation cooperation projects and ventures (Soe, 2017).

"The main focus areas are Mobility, Built Environment and Energy. Supportive layers are Data Architecture and Smart City governance (see figure 2). In other words, the Finest Twins will pilot new mobility solutions such as Mobility as a Service, mobile positioning data, twin ports, intelligent street crossings, automatic vehicles etc. (some pilots in the preparatory phase), new built environment solutions (zero-energy houses, new generation heating solutions, planning of large-scale real estate projects) and new energy solutions (smart grids, optimization of energy demand to avoid peaks, connected meters and sensors)" (Soe, 2017). The following figure visualizes the focus areas:

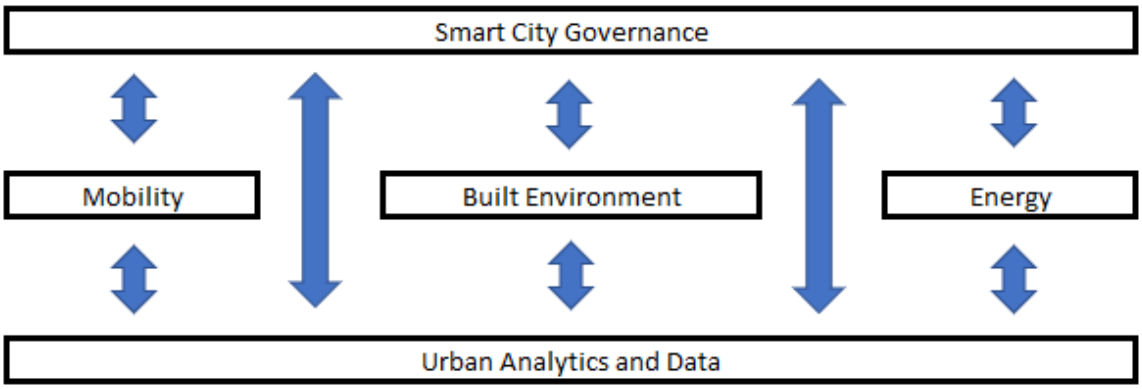


Figure 2. FINEST Twins focus areas
(Soe 2017)

The key objectives of the project are:
1. "Scientific, innovation and business-related co-operation between Helsinki and Estonia in the Smart City fields of living, mobility and environment. Promoting efficient exchange of knowledge, building a joint research portfolio, supporting faster cross-border take-up of Smart City innovations.
2. Joint-production of cross-border services in order for both regions to benefit (economies of scale, better added value services, et al.). The CoE will bring together all main public and private actors, facilitating communication, networking and the building of long-term cooperation and true partnerships in macro-region.
3. Developing FinEst Twins cities (macro-region) as one integrated Smart City open "living laboratory" acting as a test bed for new innovations, and focusing on close-to-market innovations, city-driven innovations and open engagement of local innovator ecosystems." (Soe, 2017)

3 Literature Review

In this section I am first defining the key concepts of the thesis such as smart city and open data. After defining concepts, I will discuss smart city application that have already been implemented in smart cities around the world and their enabling technologies. Finally, I am going to discuss the problem of consent of the data subjects and the regulatory requirements regarding the collection of personal data from citizens.

3.1 Definition of concepts

In this section I am going to define the key terminology. As the definition of smart city seems to be somewhat vague, my aim in this section is to define it properly utilizing earlier literature on the topic. I am also going to define other relevant concepts regarding the thesis.

3.1.1 Smart city

Smart city as a concept sounds like a clear concept by intuition, a city with smart infrastructure. However, a consensus of the definition of smart city has not been achieved in the academia. Hollands strongly criticizes the lack of definition of smart cities: ‘’Debates about the future of urban development in many Western countries have been increasingly influenced by discussions of smart cities. Yet despite numerous examples of this ‘urban labelling’ phenomenon, we know surprisingly little about so-called smart cities, particularly in terms of what the label ideologically reveals as well as hides’’ (Hollands 2008). Similar critique has been presented by many other researchers. Therefore, my first aim in this research is to coherently define the term ‘smart city’.

Forrester, an American market research company defines smart cities as cities that use smart computing technologies to make critical infrastructure components and services of a city more interconnected, intelligent and efficient (Washburn et. al. 2009). Angelidou (2014) defines smart city as “urban settlements that make a conscious effort to capitalize on the new Information and Communication Technology (ICT) landscape in a strategic way, seeking to achieve prosperity, effectiveness and competitiveness on multiple socio-economic levels.” Anthopoulos (2015) defines smart city as an urban space with innovative features. As opposed to earlier definitions, he argues that not all the innovative features are necessarily

related to ICT and further states that the features of a smart city can be divided into six dimensions:

- *Smart people,* meaning not only the level of education and qualification but also the quality of social interactions regarding integration and public life
- *Smart living,* enhancing quality of life and social coherency, as well as efficiency regarding energy, food, water, housing, culture, health, safety, tourism, etc.
- *Smart environment,* is described by appealing natural conditions, green spaces and low pollution levels as well as waste and emissions control and resilience against climate change
- *Smart governance,* in terms of ensuring urban utility and service availability and aspects of political participation and functioning of the administration
- *Smart economy,* in terms of sustainable growth and city competitiveness such as innovation, entrepreneurship, trademarks, productivity and flexibility of the labor market as well as the integration of in the national and international markets
- *Smart mobility,* addressing transportation and traffic management issues as well as the accessibility of information and communication technologies (Anthopoulos 2015; Balakrishna 2012.)

These dimensions are the basis of the so called "smart city architecture" which is further formed by three basic building blocks: 1) large-scale instrumentation pervasive sensors, 2) ubiquitous high-speed network infrastructure and 3) data management, ambient intelligence and autonomous decision. Figure 3 visualizes the building blocks of smart city architecture:

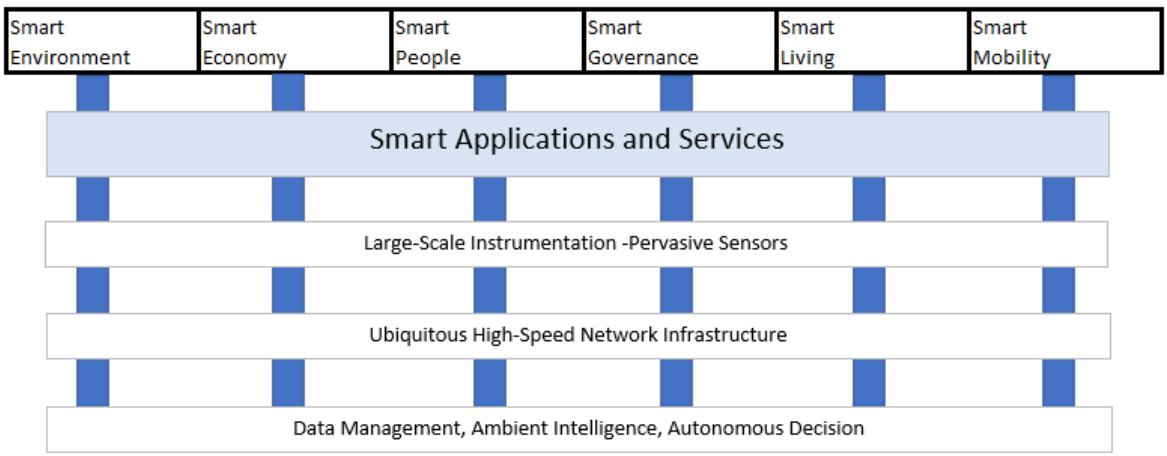


Figure 3. Building blocks of smart city architecture
(Balakrishna 2012)

So even though the definitions are similar, they seem to have slight variation between researchers and professionals. One of the major dissent seems to be the inclusion of ICT technologies, as some researches argue that smart cities are defined by their utilization of ICT technologies, and as stated above, some researchers argue that smart city features are not necessarily all related to ICT.

Even though not all features of a smart city would not be supported by ICT, the relevant literature indicates that all smart cities utilize ICT in some ways. Giffinger (2007) raises the citizen centric perspective of smart cities by stating that smart cities are built on the smart combination of endowments and activities of citizens. Caragliu et al. (2009) complements the citizen centric approach by highlighting the investments in in human capital, but also to transport and modern ICT infrastructure. The goal is to achieve higher quality of life and sustainable economic growth. Also, Setis-EU (2012) highlights the technological viewpoint and states that smart cities combine diverse technologies to improve lives of citizens.

Hall (2000) discusses the interconnectivity of critical infrastructures to optimize resources and to increase security and service provision. Su (2011) in turn states that smart city is a digital city powered by Internet of Things (IoT). Finally, Dameri (2013) states that smart city is a geographical area in which technologies such as ICT, logistic and energy production are cooperating in order to benefit citizens in the area. Moreover, the area is governed by well-defined pool of subjects that state the rules and policy for the area.

The technologies and services adopted by a smart city aim to increase the well-being of citizens, and the overall functionality and efficiency of the city´s features. In addition to ICT applications, smart cities adopt sustainable technologies, that aim to reduce pollution and energy consumption. Moreover, also ICT can be used to build strategies supporting sustainable urban environment (Dameri & Cocchia 2013).

To conclude this chapter of defining a smart city, I have a table of most used and cited definitions of a smart city assembled by Dameri & Cocchia (2013).

Table 3. Smart city definitions

Smart City Definitions	
"A Smart City is a well performing city built on the 'smart' combination of endowments and activities of self-decisive and independent and aware citizens".	Giffinger 2007
"A city to be smart when investments in human and social capital and traditional (transport) and modern (ICT) communication infrastructure fuel sustainable economic growth and a high quality of life, with a wise management of natural resources, through participatory governance".	Caragliu et al. 2009
"Smart City is the product of Digital City combined with the Internet of Things".	Su 2011
"A city that monitors and integrates conditions of all of its critical infrastructures, including roads, bridges, tunnels, rails, subways, airports, seaports, communications, water, power, even major buildings, can better optimize its resources, plan its preventive maintenance activities, and monitor security aspects while maximizing services to its citizens".	Hall 2000
"Smart City is a city in which it can combine technologies as diverse as water recycling, advanced energy grids and mobile communications in order to reduce environmental impact and to offer its citizens better lives".	Setis-EU 2012
"A smart city is a well-defined geographical area, in which high technologies such as ICT, logistic, energy production, and so on, cooperate to create benefits for citizens in terms of well-being, inclusion and participation, environmental quality, intelligent development; it is governed by a well-defined pool of subjects, able to state the rules and policy for the city government and development".	Dameri 2013

3.1.2 Open data

The second term that I am going to define is open data. The definition of open data is not as scattered and debatable as that of smart city, as the concept of open data is clearer and more structured. Bonina (2013) defines open data as follows: “a piece of content or data is open if anyone is free to use, reuse, and distribute it – subject only, at most to the requirement to attribute and/or share-alike.” Open definition website (2020) define that data is open if anyone is free to access, use, modify, and share it by anyone for any purpose (www.opendefinition.org, 2020).

Bonina (2013) further complements the definition by stating that in order to be “open data” data must be accessible, assessable, intelligible and useable. These concepts are explained in detail in the following table:

Table 4. Open data definitions

Open data features	Definition
Accessible	Data must be located in such manner that it can readily be found and in a form that can be used.
Assessable	In a state in which judgements can be made as to the data or information´s reliability. Data must provide and account that is intelligible to those wishing to understand or scrutinise them.
Intelligible	Comprehensive for those who wish to scrutinise something. Audiences need to be able to make some judgement or assessment of what is communicated.
Useable	In a format where others can use the data or information. Data should be able to be reused, often for different purposes, and therefore will require proper background information and metadata. The usability of data will also depend on those who wish to use them.

(Bonina 2013)

3.2 Smart cities in the service economy

In this section I am going to review the earlier literature about digital services that are enabled by smart city ecosystems. As I mentioned earlier, most of the world's population will live in cities in the future, creating challenges for city governments regarding social, human, and environmental issues, including how people consume services, live and travel in cities. This obliges (smart) city governments to adapt to the situation by utilizing new technologies.

3.2.1 Rise of the service economy

The importance of the service sector has been rising considerably since the 1950s. The share of service in value added was 60 percent in 1950 and has since grown to 80% in 2000 (Buera & Kaboski 2012) and the trend does not seem to wind down. Another notable issue is the change of the nature of services. Nowadays services are unbundled from the production processes and many companies have adopted this ideology of selling services rather than products. Also, the ever-increasing amount of information in economy and society, and the digital development affect city governments. The city governments are responsible for providing numerous services, infrastructure and basic welfare for their citizens and these contextual changes demand them to adapt rapidly. This creates an incentive for the smart cities to observe the service economy and to create an atmosphere where service driven

enterprises can thrive. Smart cities also enable services themselves and I find it important to review the nature of the service economy before discussing particular services enabled by smart cities.

Buera & Kaboski (2012) argue that the 20 per cent rise of the service sector from 1950 to 2000 is mainly driven by the growth of the skill-intensive services. Furthermore, they state that the share of low-skill industries declines. They stress that the increasing skill requirement and specialization play a major role in the strengthening service intensive economy.

Wölfl (2005) refers to the demand side of the market – stating that factors like high income elasticity of demand for certain services, demographic changes, ageing of the population in particular, the provision of certain services as public goods, and the growing role of services as providers of intermediate inputs. However, she also points out that employment and productivity growth in services are in many instances held back, for example the regulatory environment in the market can slow down the growth of the service sector.

Newer trend of the service sector is the emergence of the self-service economy. Self-service is a natural continuum for the service economy, as automation takes more important role in the modern society. Self-services such as ATMs and flight check-ins are present in our everyday lives and many companies find self-service appealing as to reduce labor costs and to improve customer´s user experience. Castro, et. al. (2010) state that self-service business models are one of the most important factors in increasing efficiency in modern organizations. To visualize the benefits of self-service, I added a figure of average bank transactions costs by technology:

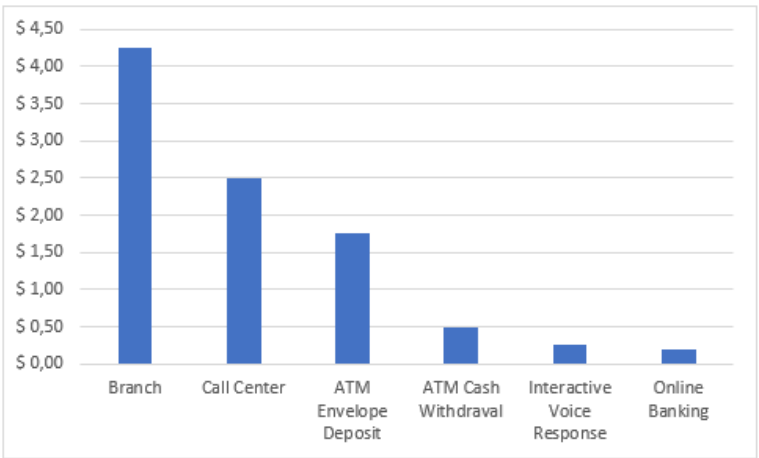


Figure 4. Estimated average back transaction costs by technology
(Castro et. al. 2010)

As the figure shows, the utilization of self-service can dramatically lower the costs of an organization. The costs saved depend greatly on the level of automation the organization is able to achieve.

Another emerging attribute of services is the ease of trade through ICTs as the global communication and delivery costs decrease due to the Internet and ubiquitous connectivity. Many local services have grown to global scale, and manual services can be digitized and automated (Kushida & Zysman 2009; Jorgenson & Wessner 2007; Rutherford 2002; Zysman 2004). Development of the "network economy" affects the nature of services regarding how they are produced, delivered and consumed. Service providers can also work together through electronic networks to share knowledge as well as risks and extend and reformulate value chains (de Man 2004; Bessant & Tidd 2007; Furubotn & Richter 2005).

To conclude, the service economy has risen through the increase of skill-intensive labor and the economic environment on the demand side. The trend on the service economy seems to be the ever-increasing utilization of self-service platforms and the internet has decreased the global communication and delivery costs of services. Electronic networks also create platforms for service providers to cooperate.

3.2.2 Smart public services

"Smart public services focus on conceptual systemization of the key dimensions of smart cities and their service functions and on building a conceptual model for smart service platforms. The discussion around smart public services is relevant to all aspects of local governments, including service provision, democratic processes, city planning and development policy" (Anttiroiko, et. al. 2014). A smart (public) service is a two-dimensional concept that connects behavioral and systemic approaches that reflect service consumption from the individual service consumers point of view as well as service provisioner´s organizational interaction (Anttiroiko et. al. 2014). The following matrix visualizes the relation of information, interaction and transaction services:

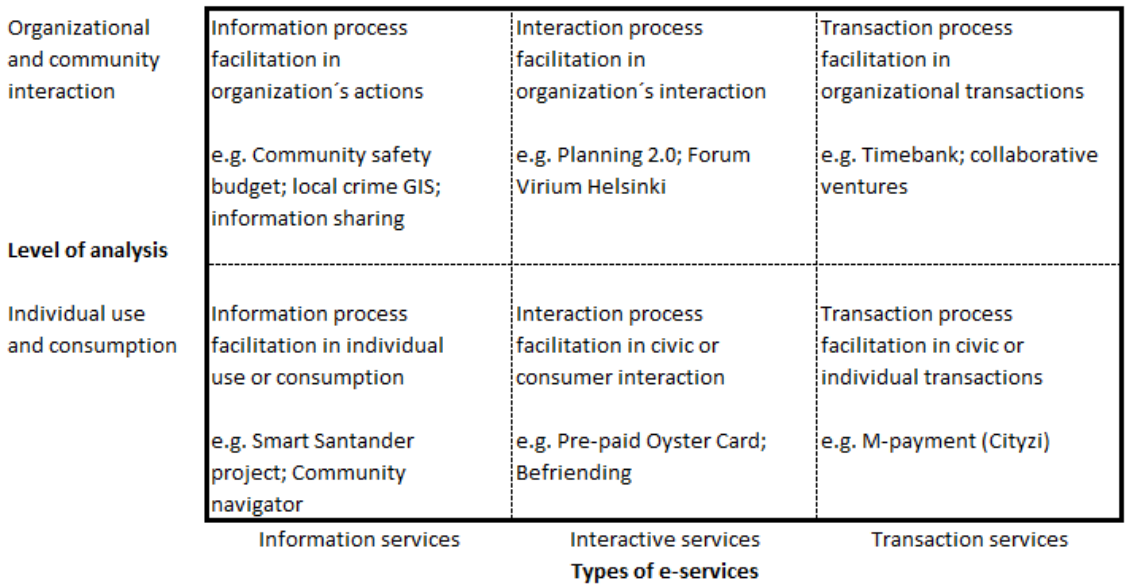


Figure 5. Individual and organizational dimensions of smart services
(Anttiroiko et. al. 2014)

The matrix explains how ICTs can be utilized to achieve smartness in urban communities using social and human systems and processes. "The fundamental idea behind this scheme is that smart information and smart communication systems are needed to build smart creative social systems, which again are conductive to sustainable urban life. When applied to services, it builds a logical connection between service informatics and intelligent and sustainable service systems" (Anttiroiko et. al. 2014). Meaning that the sole implementation of countless ICT systems is not enough to build a sustainable smart city with high quality of life – the implementation as well as the platform (the city in this case) in which the systems are implemented need to be taken into account in the process. The city government needs to facilitate a fluent atmosphere for the smart public services before implementing and investing in ICT innovations.

To implement successful services, the city government needs to also know their community. Anttiroiko et. al. (2014) even suggest that the citizens should be actively included in the developing process of the smart services, and that to some degree should be even given autonomy in developing urban infrastructure and running the services. This methodology to solve urban problems with pooled resources from the community itself could promote community well-being while saving resources from the city government to be allocated elsewhere.

The point of giving up control to the community is rooted in the idea of transferring the assets of the city to the voluntary stakeholder, so they can manage the assets to generate income to create sustainable small-scale community infrastructure and services more appropriate to the needs of the community. These services could include for example health, police and community safety budgets (Anttiroiko et. al. 2014).

3.2.3 The role of smart cities in the service economy

The radical economic shift from industrial to service driven economy sets challenges for urban governments such as integrating physical products and devices with services and dematerializing manual and siloed service packages into digitized and integrated service systems. The increasing skill requirement for service workers demands the city to also train it´s citizens for the more demanding service jobs. Also, the value creation process has changed from provider centric to more user centric approach – meaning that the customers have their own role in the value creation process. Third parties such as intermediaries and other stakeholders are a part of the service system, creating new perspective for the division of labor and patterns of interaction between private and public sectors. (Paton & McLaughlin 2008; Vargo et. al. 2008; Tien 2007; Gallaher et. al. 2006). All these changes have happened in a relatively short time frame – meaning that the city governments need to act swiftly and maintain an agile atmosphere constantly.

Anttiroiko et al. (2014) argue that the process of urban economic growth involves endogenous and creative-destructive economic and social evolution processes via organizational innovation. They further argue that increased flexibility of both service production and consumption are prerequisites for improving productivity in urban services. “This is a vital framing element in the efforts to build smart services that have multifunctional and synergistic natures as a one of the most important set of activities that is supposed to increase our well-being at individual and collective levels” (Anttiroiko et. al. 2014).

As stated earlier, smart cities utilize ICTs to increase their efficiency and to improve their processes and quality of life. Technological innovations are the essence of a smart city. However, social and ecological dimensions need to be considered as they are essential attributes regarding the quality of life in any city. Although the utilization of ICTs is seen as the defining feature of a smart city, Carillo (2006) argues that the concept also includes

policy and governance dimensions required for organizational innovation and investments in human capital.

To build a better urban society, the skills of the citizens need to be upgraded too. ICTs can only do so much if the people are not on board with the technological development. Often even the city government and its stakeholders are not familiar with the new ICTs or lack the skills to utilize them, creating a situation where the city councilors find it hard to choose which ICTs to even implement. Anttiroiko et al. (2014) suggest that smart city policy should be constructed in a way that recognizes the uncertainty which springs from the diversity of different socio-economic and demographic backgrounds.

The ultimate goal of a smart city is not that clear. Better community informatics, better quality of urban life and environmental efficiency are all great attributes, and luckily do not exclude each other. City governments should however note that these attributes should not be taken for granted, and the exclusivity of these attributes often depends on the implementation. Short term quality of life changes could be disadvantageous for the environment in the long run, for example incurring substantial debt to improve the quality of life in the short term in the expense of bankruptcy in the future. The following figure visualizes the degrees of smartness in the smart city concept through communication, functionality, quality of life and sustainability.

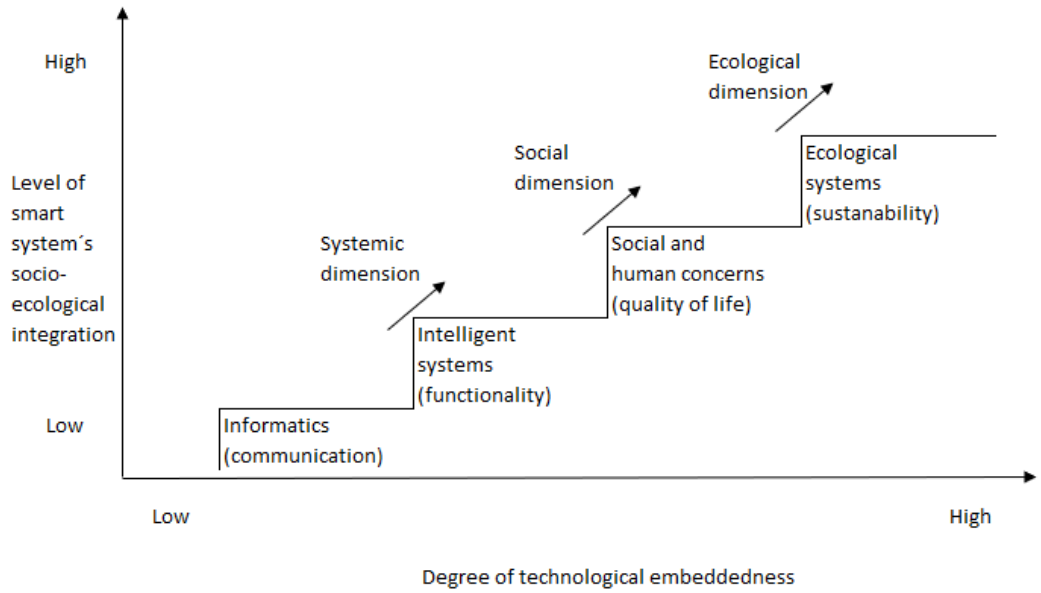


Figure 6. Degrees of smartness in the smart city concept
(Anttiroiko et. al 2014)

Smart city concept is strongly linked to wide use of ICTs in the urban context. However, if the city government focuses too narrowly on ICT implementation, on the expense of other features of the city by minimizing all other investments and ideas, the end result may not be a smooth ICT backed-up city, but a complex organization of ICTs that do not operate efficiently. "City governments have to become learning organizations before they can formulate and implement smart city policies to create smart consumption of their services so as to increase the outcome effectiveness of their policies and services" (Anttiroiko 2014). Eriksson-Zetterquist et. al. (2011) state that it is possible to create learning organizations to adjust stakeholder behavior regarding the smart city based on new knowledge and insights (Eriksson-Zetterquist et. al. 2011; Garvin 1993).

To conclude, cities cannot be considered smart just because they have managed to adopt some ICT systems. A functioning smart city surely does utilize ICT to develop networks of information between stakeholders and city government to improve services, but the technological platforms need to be embedded with the social platforms to achieve desired outcomes as a smart city. The city should be governed on a non-hierarchical basis with multiple stakeholders in order to promote collective interests. This so called "connected governance" allows the public agencies to share and integrate information using common standards (Anttiroiko 2012; Dais et. al. 2008).

3.3 Smart city services enabled by open data

In this chapter I am going to discuss digital services that are enabled by open data in a smart city environment. All of the examples used here utilize open data in some forms and the source of the data can be obtained through sensors, citizens and smart devices within the city. Smart city environment enables countless possibilities for new and innovative digital services. The list of possible services is endless, varying from smart traffic sensors that inform the drivers through open data about possible less crowded routes to smart waste disposal that signals the waste management whenever to transport the waste from a common residential trash cans to recycling centers and real time updates for public transportation vehicles – the list goes on. The innovations can also be focused on social aspects. For example, the covid-19 pandemic has emerged the importance befriending networks that offer supportive, reliable relationships through volunteer befrienders to people who would otherwise be socially isolated (https://www.befriending.co.uk/ 2020)

As seen above, the digital services enabled by smart city environment are various, and the technologies they utilize (although all of them ICTs) are not the same. Some use personal data collected from citizens smart devices, and some use public data collected by sensors in the city, some applications do not even utilize data but are rather social networks for the citizens such as Befriending projects as my focus in this thesis in open data enabled applications, I will cover them in closer detail. In the next subchapters I am first going to discuss the enabling technologies for the smart city applications, and then I am reviewing implemented and possible smart city services by the features introduced in the first chapter; smart people, smart living, smart environment, smart governance, smart economy and smart mobility.

3.3.1 Enabling technologies for smart city services

In this chapter I am discussing enabling technologies for smart city services. The smart city concept is impossible if the digital infrastructure of the city does not extensively support innovative digital services. Eckoff & Wagner (2017) have listed nine different enabling technologies in their research that are necessary for a smoothly operating smart city. These technologies are illustrated in figure 6. Eckoff & Wagner also recognized nine different smart city features different from the six features introduced above. However, in this thesis I am going to discuss the smart city features as six dimensional as it has clearer consensus in the science community (Giffinger et al. 2007; Balakrishna 2012; Anthopoulos 2015).

As seen in the below figure, Eckoff & Wagner (2017) state that there are nine different technologies enabling the smart city environment. The nine technologies are ubiquitous connectivity, smart cards, open data, sensor networks, wearable devices, Internet of Things, autonomous systems, intelligent vehicles and cloud computing. “These technologies in turn were made possible by other technological progress. To name a few, embedded systems have significantly expedited pervasive and ubiquitous computing. Smaller and faster microprocessors allow complex tasks to be computed by portable devices or even home appliances. Energy-efficient computing as well as long-lasting batteries extend the lifetime of mobile devices and exterior sensors. Lastly, radio technology such as passive RFID tags and microstrip antennas have made it possible to equip even the smallest items with communication capabilities, making them a potential part of the interconnected smart city” (Eckoff & Wagner 2017).

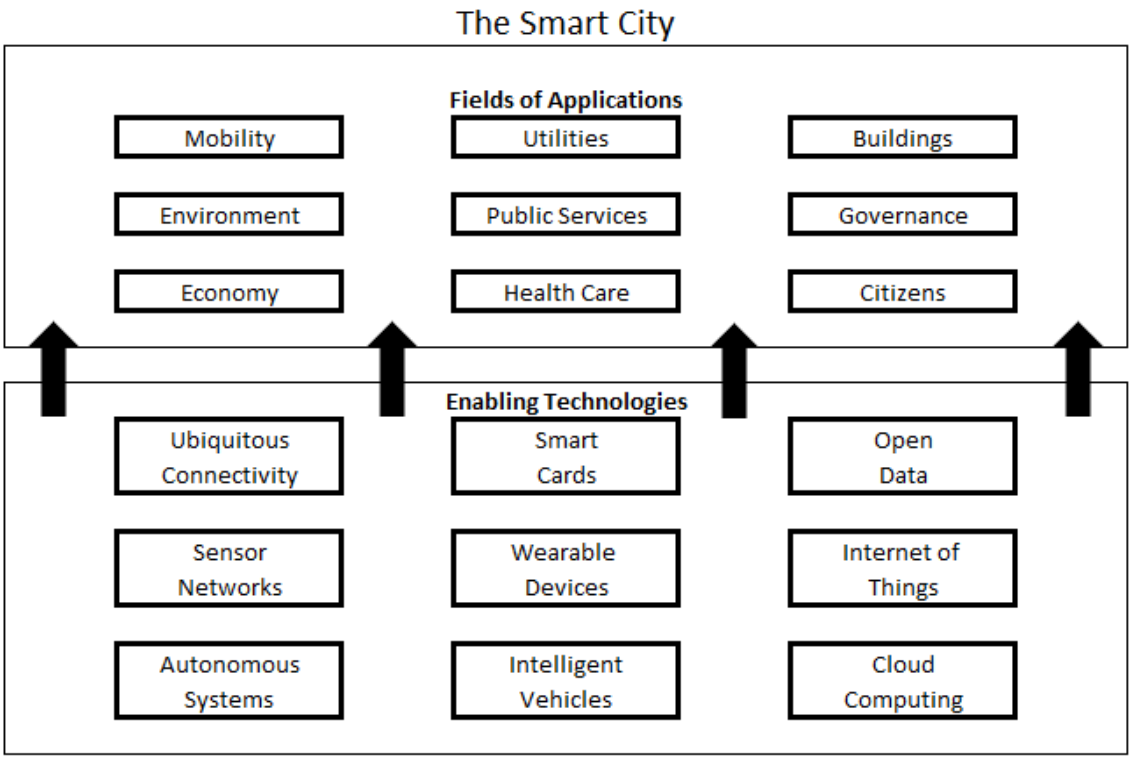


Figure 7. Smart city applications and enabling technologies
(Eckoff & Wagner 2017)

Most smart city applications and services combine these enabling technologies. For example, ubiquitous connectivity and sensor networks can form a map for air pollution monitoring. *Ubiquitous connectivity* is one of the key elements in any smart city. It allows efficient Machine-to-Machine (M2M) and Machine-to-User (M2U) communication and most homes in urban areas are equipped with broadband Internet connection. Ubiquitous connectivity also enables smooth flow of open data and allows it to be utilized in various applications as the data is available everywhere in the city. In Finland the cellular Internets are also mostly with unlimited data packages so most of the citizens are connected everywhere, even without their landlines or public WiFis.

Another everyday technology are *smart cards*. They are capable of transmitting authentication data, function as cashless payment methods and can even hold identification information such as driver´s licence or travel documents (Phan & Mohammed 2003). During the recent years these smart cards have become contactless and can be read from a short distance. Many of the smart cards hold all the necessary data, allowing offline usage.

Open data – meaning data that is publicly available for third parties allows many smart city applications to emerge. Open data also increases government transparency as well

as service development by third parties that can access the city data. All of the other enabling technologies listed in this chapter also either provide or utilize open data regarding the smart city environment.

Sensor networks form the basis for many smart city applications. The sensors can monitor for example pollution, noise levels, temperature, humidity and other environmental attributes. They are constantly collecting data from their surroundings providing information to back up decisions and actions and are often used when developing smart mobility and smart environments. Sensor networks can also cover citizen´s personal smart devices such as smartphones (Cilliers & Flowerday 2014).

Wearable devices such as smart watches provide information provide personal data of the wearer such as blood pressure, heart rate or even brain activity (Martin et al. 2000). Combined with ubiquitous connectivity, these devices can provide valuable information to enable for example smart healthcare and allows citizens to monitor their body to improve personal healthiness.

Internet of Things (IoT) is "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" (Rose et al. 2015). Meaning that common objects are equipped with communication technologies such as smart air conditioning and other smart meters (Rial & Danzeis 2011; Jo et al. 2013). IoT is often used in smart living related applications. IoT connected device provide open data about physical devices that can be further used to improve the functionality of smart city applications and services.

Autonomous systems, for example autonomous vehicles will drastically form the future of our cities. An anticipated change through autonomous vehicles is the shift from ownership of a vehicle to shared autonomous vehicles (Fagnant & Kockelman 2014). Public autonomous systems can also be implemented by the city officials in the form of delivery systems or street cleaning.

Intelligent vehicles are strongly linked to autonomous vehicles as they are vehicles equipped with sensors that recognize details and patterns from their environment. "They can exchange information in an ad-hoc fashion, inform infrastructure nodes such as traffic lights and dynamic traffic signs, or access centralized services like traffic information or emergency services using cellular technology" (Eckoff & Wagner 2017). Intelligent vehicles are also largely powered by data generated from their environment.

Finally, cloud computing refers to the outsourcing of computational tasks to third parties. These third parties can provide hardware, operating systems or software applications as a service (Takabi et al. 2010). Due to the high scalability of cloud-based services, they are often used by smart cities to power web services to ensure their availability during high traffic seasons (Eckoff & Wagner 2017).

3.3.2 Smart people

Smart people – or smart citizenship aims to develop smart communities that enable life-long learning programs and smart education and focus on employability. Digital inclusion is a major key for smart citizenship, and for instance subsidized broadband internet in lower income areas would be a great way to improve digital inclusion (Edwards 2016; Woods et al. 2016; Eckoff & Wagner 2017). A good example of social inclusion through smart citizenship or "smart people" is the Befriending project in the United Kingdom. Befriending UK operates in the United Kingdom and it offers befriending projects which organize effective support for children and young people, families, people with mental health problems, people with learning disabilities and older people among many others. The service offers supportive and reliable relationships to citizens that would otherwise be socially isolated (https://www.befriending.co.uk/ 2020).

To achieve proper digital inclusion and life-long learning programs, smart cities need to adopt citizen centric development methods. One way of implementing citizen centric development is the introduction of citizen centric open data applications. An example of these applications would be the concept of Living Labs. The concept of Living Lab has been emerging since the mid-1990s and it is seen as a valuable tool for researchers, social innovators and companies. In Europe, several Living Labs are used for cooperation between citizens and public and private actors to create services (Schaffers et al. 2007; Almirall & Wareham 2008; Katzy & Klein 2008). Livings Labs focus on User-Driven Innovation (UDI) that functions as the basis for co-creation and knowledge. They often utilize open data to test and develop new products and services regarding eHealth, energy saving, citizen participation in government, manufacturing among others (Hielkama & Hongisto 2012). Living Labs focus on bringing together different stakeholders in the field to share their knowledge and expertise to develop new services and products. Many companies such as Nokia or Philips use Living Labs for ideation and product development through the user-driven environment (Hielkama & Hongisto).

The role of open data in the Living Lab environment is crucial. Hielkama & Hongisto (2012) provide an example of open data innovation in Living Labs through open competition. The first data set made public by Helsinki city officials was the data about public transportation. Forum Virium, a Living Lab operating in Helsinki established in 2005, held an open data competition in which public agents could use the data of public transportation and in addition they were provided an Application Programing Interface (API) to take part in a competition for the best application utilizing the data. This inspired individual programmers as well as SMEs to create their own applications and more than 50 applications were submitted for the competition.

Another similar open data powered competition by Forum Virium is the Apps4Finland, which makes local government data available regarding environmental data, spatial information, statistics about health and welfare as well as population surveys and traffic and location services (Hielkama & Hongisto 2012). “The Apps4Finland competition has four categories of eligible entries, applications, visualization series, ideas, and data. The applications category is for working applications, which will be freely available during the competition and for 2 months after closing. The visualization series is for innovative ways to visualize data from one or more of the public services. The ideas category is for concepts and unrealized applications, while the data category is for opening more data to the public, as well as for innovative ways in cleaning or converting the data. Over 140 submissions were done in the various categories and prizes were given to the winners” (Hielkama & Hongisto 2012).

3.3.3 Smart living

As mentioned before, smart living aims to increase the quality of life and social coherency, as well as efficiency regarding energy, food, water, housing, culture, health, safety and tourism. In this subchapter I am going to review some smart city services related to smart living such as energy management and smart tourism and review the role of open data in these services.

Many smart city services are IoT based. Internet of Things provides intelligent Machine-to-Machine and Machine-to-User communication and provides a solid base for smart city services (Balakrishna 2012). An innovative IoT-based smart city application that I am going to discuss here is the smart heat energy management application. The Brunswick Centre and Ampthill estate in London utilizes an IoT-based energy platform that allows

smart heat energy management addressing retail domain in a specific area. An application called Energyhive exploits sources, sinks and mediation of sensors and processors of IoT data. The properties in Brunswick Centre are equipped with Wi-Fi routers and heat meters connected to it. The properties also have a tablet displaying relevant data such as real-time energy consumption. The application is used by retailers, residents and visitors in the area. Energyhive also includes energy production and demand, shopper dynamics and environmental and energy data from retail and restaurants (www.energyhive.com, 2020). The real-time reporting of electricity usage allows the reduction of overall demand increasing sustainability in the area. The smart meters will automatically reduce energy usage by real time screening of weather, outside temperature and lighting. The technology also detects anomalous events such as rapid rise in the inside temperature, implicating a fire for example (Kyriazis et al. 2013). In the long run, the accumulating (open) data will allow the energy companies to monitor the energy demand more efficiently, enabling them to offer cheaper deals for electricity for the end-users during off peak times.

IoT could also improve medical care regarding smart medical treatment. IoT can help hospitals to implement smart medical care with smart patient records combined with drug information and personal as well as management information. Intelligent inventory management regarding medical equipment and materials would also be easier with smart inventory monitoring enabled by IoT technology (Xue 2010).

Smart tourism is defined by ICT adoption in tourism in many forms. It covers central reservation systems such as *Airbnb* and other booking sites for tourism related activities as well as social media in forms of blogs and other posts about tourism destinations. A smart tourism destination is defined by Lopez de Avila (2015) as "an innovative tourist destination, built on an infrastructure of state-of-the-art technology guaranteeing the sustainable development of tourist areas, accessible to everyone, which facilitates the visitor's interaction with and integration into his or her surroundings, increases the quality of the experience at the destination, and improves residents' quality of life." The key feature is the ICT integrated to the destination´s infrastructure. For instance, in Barcelona the city provides IoT backed up bicycles that show one´s location on map via a smart phone app. Tourists can use these bicycles to navigate the city ecologically and safely while the city government can obtain data about tourist movement (https://ajuntament.barcelona.cat/digital/ca; Gretzel et al. 2015). Should the data about tourist movement be open, it would allow tourists and other citizens to plan their activities such that they would avoid the most crowded places at the time, evening out the traffic among the popular tourist attractions.

3.3.4 Smart environment

Smart environment is aims to improve sustainability, quality of life, as well as public safety in the city. Smart environment covers sensors that track for instance air pollution or noise within the city, enabling the citizen to access this data via pollution maps from their personal smart devices. This allows citizens to avoid unhealthy or even dangerous areas within the city if these data are open and available for the citizens (Carlsen 2014; Burange & Misalkar 2015). The smart sensors can also be used for seismic readings to detect earthquakes proactively and to preserve historical buildings (Baldini et al. 2013; Burange & Misalkar 2015). The sensors can be used for other kinds of natural disasters also such as forest fires, floods, tsunamis and tornadoes. The early warning and proactive actions can save lives and reduce property damage in the case of a natural disaster. Also, smart waste collection and emission control are part of the smart environment feature.

Zanella et al. (2014) discuss noise monitoring as a potential smart city application. Noise can be seen as "acoustic pollution" as high decibel levels are harmful for humans, even more so when being affected to it continuously. In that sense, noise monitoring IoT devices can be implemented in for example city centers to monitor the noise levels. Such service could also increase safety in a city by recognizing social disturbance from the noise. If the algorithm would for example recognize the noise of a glass shattering and aggressive yelling as potential threat to public security, it could instantly alarm security and police forces in the area. This would increase greatly the safety of city night life and increase the confidence of business owners in the area. Noise monitoring would also allow law enforcement to allocate their resources more efficiently by monitoring the noise levels around different districts of the city. Citizens on the other hand could also monitor the high noise levels implicating high number of people in the area and plan their evening to go to a less crowded district. The controversy in this application rises from individual's privacy issues, as installing microphones throughout the city could be seen as a serious privacy violation. (Zanella et al. 2014)

Smart city sensors could also be utilized in preserving historical structures. As proper maintenance of historical buildings requires constant monitoring which is rather expensive as the buildings tend to be very large or partly inaccessible, smart city sensors could provide data about the building´s condition. Sensors could track humidity, temperature and pollution as well as calculate seismic readings of earths vibration which slowly damages the buildings. These data would allow the city government to react proactively and maintain these

historical buildings more easily and precisely. This would also decrease the cost of evaluating the level of maintenance needed. These sensors could also be used on residential infrastructure, but for the more fragile historical buildings the benefits would be more considerable as their maintenance tends to be expensive and tedious (Lynch & Kenneth 2006; Zanella et. al. 2014). If these sensors would be implemented into residential and public buildings, similar measurements could be made. In the case of residential and public buildings however, the data could be used to improve citizens comfort in the building through automation. For example the sensors in an office building could signal the air conditioning of a hot and humid day and then adjust the ventilation accordingly and thus increasing productivity of the office workers while also reducing the costs of heating or cooling through proactive measures. (Kastner et al. 2005; Zanella et al. 2014)

A well-known IoT application that is already used in many cities including Helsinki is the smart waste management. Waste management can ruin a city´s aesthetics if not handled properly. Overflowing garbage bins and litter make any city feel uncomfortable. Moreover, poorly operating waste management can be a threat for the environment and could for example poison the waters around the city. The implementation of an IoT application to waste management could lead to significant financial and ecological advantages. The waste containers could be equipped with sensors that track the load and send the data of these containers to the waste collector. The waste collector could the optimize their route throughout the city when emptying the containers and thus improve the efficiency of recycling. (Nuortio et al. 2006; Zanella et al. 2014)

3.3.5 Smart governance

Smart governance covers digital citizen services such as interaction with government services online, for example when applying for student aid, looking for social housing or applying for a university. Smart governance also enables citizen participation in the city´s events and even city planning. For example, MyHelsinki had a crowdsourcing competition online where citizens could make their own suggestions for how to use 4,4 million euros in Helsinki infrastructure. The competition proposals varied from football fields to new park areas, and the citizens of Helsinki could vote for their favorite proposal or make their own. MyHelsinki still has the possibility for citizens to submit events or places on the web-page, thus increasing citizen influence in Helsinki (https://www.myhelsinki.fi/en 2020). Smart governance also aims to increase efficiency and transparency regarding city governance and

to reduce bureaucracy through cross referencing enabled by open data (Belanche-Gracia et al. 2015). Helbig et al. (2009) further argue that governments may often be disconnected with citizen´s true needs and questions and that the governments often lack a clear picture what the service users actually want. Open data could be used as a bridge between government and citizens and it is helping public organizations to act as more open system that interacts with its environment (Janssen et al. 2012). The open data government platforms can help governments to learn from other organizations and agencies in delivering better services by increasing government responsiveness regarding issues raised by citizens (Irani et al. 2007; Agrawal et al. 2014).

Pereira et al. (2017) complement the statement that governments can use open data initiatives to promote disclosure of data and improve their interaction with city´s stakeholders. Through open data initiatives, the city government can obtain a clear picture of what the stakeholders want from an e-government service, allowing the officials to compare and integrate the perspectives of all stakeholders. Through the increased information about government processes the citizens can communicate their opinions more easily, thus increasing the inclusion of citizens in the governance process. This leads to better city governance by increasing transparency, accountability and participation (Gonzales-Zapata & Heeks 2015).

Another possibility enabled by open data is strong data driven decision making by the city government. Data can be used to observe certain dynamics within a city, thus allowing efficient planning of public transport for instance. A city could also use these data for example emergency mapping, by quickly knowing how many hospitals, schools or residential buildings are in the area of emergency (such as terrorist attack or natural disaster) (Pereira et al. 2017).

3.3.6 Smart economy

Smart economy aims for sustainable economic growth and city competitiveness. These can be achieved for example through public-private partnerships and new business models such as recommender services (Carlsen 2014; Elmaghraby & Losavio 2014). The cities can also offer collaborative spaces and entrepreneur networks and provide office spaces for small companies and start-ups to encourage entrepreneurship (Belance-Gracia et al. 2015). Smart economy also refers to the implementation of innovation to increase productivity and reduce costs. Smart economy covers deep cooperation between enterprises, research institutions and

the citizens in order to achieve innovative economic solutions (Bakici et al. 2013; Anttiroiko 2014). The Living Labs introduced earlier could also be included in the smart economy section.

The existing literature covering concrete smart economy open data applications and services seems to be rather scarce. The Living Labs and other innovation centres that utilize open data are an indirect contribution to the smart economy through open data, yet I could not find other concrete examples of open data applications contributing to smart economy. However, as smart economy covers the overall improvement in economic attributes such as increased innovation and cost efficiency, one could argue that all applications under the other features of smart cities contribute also to smart economy. Bruneckiene and Sinkiene (2014) have examined the common characteristics of smart economy which I have assembled in the table below:

Table 5. Characteristics of smart economy

Innovation and knowledge economy	Implementation of innovation, increasing productivity and reducing costs, in all sectors of the economy
Learning economy	The learning is the most important process in all spheres of economy
Digital economy	Widespread employment of information and telecommunication technologies in the economy
Competitive economy	The ability to compete globally and be open. Employing knowledge and innovation, a competetive battle is going on, based on higher profits, productivity, quality, resources cost efficiency and cost and waste reduction.
Green economy	Implementation of the sustainable development principles, focus on creating a free of pollution "clean" economy and the efficient consumption of energy. resources.
Network economy	Development of the competencies networking between universities, business and government.
Socially responsible economy	Enterprises and organizations are characterized by economic, ethical, legal and philantrophic responsibility.

(Bruneckiene & Sinkiene 2014)

3.3.7 Smart mobility

Smart mobility is designed to optimize traffic fluxes and quality of local public transport services (Benevolo, 2016). Madrid, the capital city of Spain has implemented smart mobility by installing smart traffic sensor backed-up by IoT technology. In Madrid there operates 213 bus lines with a fleet of 2076 vehicles (EMT Madrid 2020). Given such a tremendous number of vehicles, the city government has pursued both optimal driving conditions and minimizing air pollution. The vehicles are equipped with GPS sensors that track their

location and speed. Madrid has also deployed sensors on the streets to track traffic lights, air pollution and traffic congestion. The city has also included its citizens to complement the public sensors by giving them the possibility to provide additional information with their mobile devices such as filming road conditions or potential accidents. (Kyriazis, et. al. 2013)

The information generated by the sensors and the citizens allow the buses to drive more ecologically, predict driving conditions such as weather, traffic jams and road accidents. The eco-driving application for example informs the driver about traffic congestion ahead, signaling that increasing speed would be redundant because the traffic is stagnant further down the road. Thus, the driver would remain driving at slower speed and using less gas than he would without the information. In addition, IoT technologies can provide information from the experiences of others. For example, in bus traffic devices can track the actions of other vehicles such as braking or speed and inform other buses of bad driving conditions in certain areas. This allows other drivers to adapt in real time and optimize their cruising (Kyriazis et. al. 2013). The opening of these data about bus location would allow citizens to check their bus lines in real time, to see if the bus is late or early when they arrive to the bus stop.

Similar service is already implemented in Helsinki. The data of the public transportation network has been made public by the city officials and is available to developers. These data include timetables, public transportation lines and stops, and even disruptions and planned changes are available in real time are available online. The vehicles operating in the systems are equipped with GPS sensors that track their location (Hielkama & Hongisto 2012). An example of open data backed-up application is the Sporat.fi service that utilizes the data provided by GPS sensor on the tram network. The trams in Helsinki are equipped with GPS sensors and anyone can access the data about their movement through a website www.sporat.fi (2020).

Open data enables various smart city services through sensors, citizens and smart devices within the city. The main contributor for emergence of these services are the enabling technologies such as ubiquitous connectivity and IoT to name a few. The smart city services can be further divided to subgroups of services, smart people, smart living, smart environment, smart governance, smart economy and smart mobility.

3.4 Consent of the data subject

As all the applications mentioned in the previous chapter utilize data from citizens it is crucial that the service provider complies with data protection regulations. In this chapter I am going to discuss privacy in a smart city as well as consent of the data subject. I am going to provide a framework of different possible data breaches and introduce the European Data Protection Regulation (GDPR). However, in this chapter I will not go deep into details of GDPR, instead I focus on different possible data breaches which I have assembled in table 3. I will also provide examples of some of them. The deeper discussion around regulation and GDPR will be in chapter 6.

3.4.1 Privacy in a smart city

Privacy is considered as a basic human right at least in democratic states. Elwood (2011) defines privacy as a concern regarding acceptable practices with regards to accessing and disclosing personal and sensitive information about a person. Moreover, the sensitive information includes multiple domains such as identity privacy, bodily privacy, territorial privacy, locational and movement privacy, communications privacy and transactions privacy. These forms of privacy can be breached in various different ways in a smart city environment. In table 3. unacceptable practices regarding privacy are shown. Each of these practices cause different kind of harm (Solove, 2006).

Table 6. A taxonomy of privacy breaches and harms.

Domain	Privacy breach	Description
Information collection	Surveillance	Watching, listening to, or recording of an individual´s activities
	Interrogation	Various forms of questioning or probing for information
Information processing	Aggregation	Combination of various pieces of data about a person
	Identification	Linking information to particular individuals
	Insecurity	Carelessness in protecting stored information from leaks and improper access
	Secondary use	Use of information collected for one purpose for a different purpose without the data subject´s consent
	Exclusion	Failure to allow data subject to know about the data that others have about her and participate in its handling and use, including being barred from being able to access and correct errors in that data
Information dissemination	Breach of confidentiality	Breaking a promise to keep a person´s information confidential
	Disclosure	revelation of information about a person that impacts the way others judge her character
	Exposure	Revealing another´s nudity, grief, or bodily functions
	Increased accessibility	Amplifying the accessibility of information
	Blackmail	Threat to disclose personal information
	Appropriation	The use of the data subject´s identity to serve the aims and interests of another
	Distortion	Dissemination of false or misleading information about individuals
Invasion	Intrusion	Invasive acts that disturb one´s tranquility or solitude
	Decisional interference	Incursion into the data subject´s decisions regarding her private affairs

(Solove, 2006)

The emerging smart city phenomena raises various privacy issues regarding citizen´s personal data. Smart cities collect and store personal data through sensors, location devices, security cameras, among others. As an information and networking entity, smart city should be able to protect citizen´s data from unauthorized access, disclosure, disruption, modification, inspection and annihilation (Zhang et al. 2017). A unique challenge regarding smart cities is the processing of these data into manipulating people´s lives and environments (Zhang et al. 2017). Let us think the noise monitoring applications for instance. Noise monitoring could greatly increase city´s safety in certain areas by recognizing hazardous and alarming noises, but also what if the noise monitoring system also records private conversations? What if it recognizes individual´s voices and the system owner could eavesdrop on citizens and abuse that information to their benefit?

As this thesis is mainly focused on consent of the data subject rather than the overall data protection of individual´s data, I will not go into further detail about smart city data protection. Instead, I am reviewing literature regarding consent of data subjects in general,

and my aim is to connect these findings into smart city environment. Yeh (2017) states that in his study surveying Taiwanese cities reveal that "citizens are willing to accept and use ICT-based smart city services if the services are designed with innovative concepts that secure their privacy and offer a high quality of services".

Bleier et al. (2020) further state that personal data collected from individuals could lead to information misusage, potentially threatening entrenched norms and generating privacy concerns. They raise an issue regarding personal health or fitness tracking applications in the sense that if an application collects health data from its users and feed it directly into the cloud. This data is used to create leaderboards and comparisons with peers, for recreational use, but if this data gets used to other purposes than fitness tracking, such as insurance scoring, the new context of this recreational data would likely raise privacy concerns (Bleier et al., 2020). In this example of secondary use, the data subject might consent to their data being processed by the fitness and health tracking applications, but probably would not allow these data to be handed over to insurance scoring as it might result to a less desirable insurance policy for them. In the next chapter I am going to discuss the issue of consent in data collection regarding digital services.

3.4.2 Consent of the data subject

According to GDPR, personal data is any information relating to an identified natural person – the data subject. Also available (open) personal data is protected, as the information is not required to be in a structured data base to be protectable, meaning that information contained in free text in electronic documents may qualify as personal data. (Kelli et al. 2019)

As individuals use and interact with different smart city applications and services, data is generated about them continuously. As these services are so attached to our everyday lives, it would be incomprehensible for individuals to track which data of them is being collected and processed. Also, as many services force individuals to give up their data to use those services, it would also be very onerous for them to weigh up the costs and benefits of agreeing to terms and conditions in the moment of deploying the application. So, the individuals might agree to terms and conditions even though they have no idea where their data is being used or stored, not to even speak of the holistic effects of their data being merged with other datasets (Solove, 2013). "Even if someone wanted to proactively manage their data privacy across all these systems and apps, they would be faced with long, complex legal documents that in practice are non-negotiable—one either consents or is denied the

service" (Solove, 2013; European Data Protection Supervisor, 2014). This means that consent is often forced from individuals without them fully realizing the extent or consequences of their actions (Rubinstein, 2013).

Some applications lack the overall consent, as terms and conditions are either unimplemented or so difficult to reach that it is practically impossible. Zang et al. (2015) state that between a quarter and a third of all smartphone apps lack a privacy policy and do not seek consent. The letter of consent often includes secondary data usage such as data mining, analysis and repurposing which may lead to a situation where the data subject might accidentally give up their data to entities that they would not want to if they understood the depth of the agreement. The terms and conditions might also include rights to change terms of the agreement without notice, reducing the service providers accountability of proper data management (Kelli et al. 2019).

In many smart city applications, the data subjects have little to no possibilities to seek consent, as well as no choice of being surveilled. The sensors monitoring noise levels, electronic bus tickets, as well as surveillance cameras are rather difficult if not impossible to avoid. The only way to opt out from such surveillance is not to use public services and spaces. A person is forced to reveal themselves if using public services or even when just going outside. Citizens are also often unaware of these systems monitoring them, reducing the possibility of consent even more, not to even mention the full length of their data flow across the holistic data streams and systems (Crump & Harwood, 2014; European Data Protection Supervisor, 2014; Data Protection Working Party, 2014).

The consent of the data subject seems to be an awkward problem for smart cities. As their goal is to increase the quality of life and inclusion, it is necessary for them to collect data from their citizens to some degree. Similarly, they should ensure secure collection and handling of this data. Moreover, if these applications and services would continuously ask for user consent, many of the service users would probably consider the service as clunky, whereas smooth service provision would require ignorance over data subject´s consent. And as said, in many applications such as surveillance cameras and other passive monitoring devices, the consent is not even possible to give. It almost seems like the trade-off from smooth user experience in services is the loss of privacy and disclosing of personal data. Thus, smart city initiatives need to balance themselves between user experience and data privacy and security segments and finding that balance is one of the main goals of this thesis. In Europe, GDPR provides a framework for the processing of personal data. In the next segment I am introducing GDPR and the requirements it sets for using personal data.

4 Regulatory requirements set by the GDPR

In this chapter I have collected the main articles and recitals of the GDPR which affect the use of open data for developing smart city services. The GDPR sets the regulatory framework of data processing in the EU region, and it also reaches to states outside of EU as in order to move data outside of EU the country has to have adequate level of protection similar to the GDPR (GDPR art. 45, 2018). Failure of complying with the standards and principles set by the GDPR will lead to heavy fines up to 10M€ or in the case of undertaking up to 2% of the total annual turnover of the preceding financial year, whichever is higher (GDPR art. 83, 2018). Thus, the organizations in the EU region have a strong incentive to comply with the regulation. In this chapter I will first introduce the principles of GDPR regarding processing of personal data and lawfulness of processing. In the second subchapter I will introduce the conditions of consent of the data subject and in the third subchapter I will discuss the rights of the data subject.

4.1 Principles relating to processing of personal data

Article 5 of the GDPR discusses the principles relating to processing of personal data. The article introduces seven principles of GDPR regarding processing of personal data which I have assembled in the following table:

Table 7. Principles of data processing in the GDPR

	Personal data shall be:
Lawfulness, fairness and transparency	processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not to be incompatible with the initial purposes
Data minimization	adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
Storage limitation	kept in form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject
Integrity and confidentiality	processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with these principles

(GDPR art. 5, 2018)

Recital 39 of the GDPR complements these principles by stating that processing of data should also be transparent to natural persons that they are being subject to data collection and usage. The extent of the data usage should also be transparent. Transparency here means that the data is easily accessible and in such a format that is easy to understand. The identity of the data controller as well as the purpose of the processing should also be informed to the data subjects. Data controller in this case being the city administration or other service provider. Thus, the providers of smart city services should consider extreme transparency when processing personal data of citizens in the region. The data cannot be collected beforehand and make up the purposes later as the data subjects have a right to know explicitly to what purposes the data is being collected and these purposes need to be determined at the time of the collection of the data (GDPR recital 39, 2018). The data have to be adequate, relevant and limited for the purposes for which they are processed (GDPR

recital 39, 2018). This means that data collected for smart city application X could not be used freely for application Y if the usage is not determined in the data collection phase.

The time period that the data is stored should also be minimized and the data should be used only if the purpose of processing could not be achieved by other means (GDPR recital 39, 2018). This means that some applications could be denied from using personal data if there is a reasonable way to enable that smart city service without using personal data. Also, the service provider is obliged to set time limits for how long the data is being stored before erasure or for a periodic review (GDPR recital 39, 2018). "Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted" (GDPR recital 39, 2018). This could be achieved through consistent data management and giving citizens access to correct their data in the database.

4.2 Lawfulness of processing

In this chapter I will discuss the lawfulness of data processing under GDPR using mainly article 6 of the GDPR as well as its recital 40. Recital 40 of the GDPR states that "in order for the processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation (GDPR) or in other Union or Member State law as referred to in this Regulation" (GDPR recital 40, 2018). The article 6 of the GDPR sets a clear framework for lawfulness of processing in which certain conditions must hold. I have assembled these conditions to the following table:

Table 8. Lawfulness of processing

Processing shall be lawful only if and to the extent that at least on of the following applies:

1.	the data subject has given consent to the processing of his or her personal data for one or more specific purposes
2.	processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
3.	processing is necessary for compliance with a legal obligation to which the controller is subject
4.	processing is necessary in order to protect the vital interests of the data subject or of another natural person
5.	processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
6.	processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

(GDPR art. 6, 2021)

As in tasks 3. and 5. legal obligations or official authorities are mentioned, the legal basis for these processes shall be laid down either by Union law or Member State law. Also, the sixth task does not apply to processing carried out by public authorities. The purpose of processing shall also be determined by the Union law or Member State law to which the controller is subject (GDPR art. 6, 2018).

If the data is not processed for other than the initial purpose which had been given a consent by the data subject or constituted by regional or local authorities, the controller shall ascertain whether the another purpose is compatible with the purpose for which the personal data are initially collected (GDPR art. 6, 2018). The use of already collected data for other purposes may seem tempting for the providers of digital services in a smart city environment. However, the data collector is responsible to take into account the following characteristics regarding the data. The attributes have been assembled from article 6 of the GDPR:

Table 9. Data processing for purposes other than initially collected

1.	Any link between the purposes for which the personal data have been collected and the purposes of the intended further processing
2.	The context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller
3.	The nature of the personal data, in particular whether special categories of personal data are processed, or whether personal data related to criminal convictions and offences are processed
4.	The possible consequences of the intended further processing for data subjects
5.	The existence of appropriate safeguards, which may include encryption or pseudonymisation

(GDPR art. 6, 2018)

4.3 Conditions for consent

Recital 32 of the GDPR discusses the conditions for consent in data processing. According to the regulation, "consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including electrical means, or an oral statement" (GDPR, Recital 32, 2018).

Consent is given by electronic means for instance when ticking a box when entering a website or when choosing privacy settings for an application or other information society service. Consent can be given when there exists a statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data (GDPR, Recital 32, 2018). However, if for example entering a website, the boxes regarding data processing are pre-ticked, consent can not be indicated. The natural person has to tick the boxes manually for the conditions for consent to hold. As well as pre-ticked boxes, inactivity or silence do not grant consent for data processing (GDPR, Recital 32, 2018).

Consent should also cover all activities and purposes to which the data is used. If the processing has multiple purposes, consent should be given for all of them. Finally, "if the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it

is provided" (GDPR, Recital 32, 2018). Article 7 of the GDPR lists the conditions for consent according to the GDPR and I have listed them in the following table:

Table 10. Conditions for consent

1.	Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2.	If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3.	The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4.	When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

(GDPR art. 7, 2018)

Smart city application owners and service providers should ensure that processing of personal data complies with these norms. The data controller should be able to demonstrate that they have the data subject's consent and should form their letters of consent in such manner that they are easily accessible and understandable to ensure that the data subject is aware of the extent of the consent. The conditions introduced in an application's letter of consent should also be fair and the data subject should at least be aware of the identity of the data processor as well as for which purposes the personal data are being used. The data subject should also be able to refuse and withdraw consent without detriment (GDPR, Recital 42, 2018).

The GDPR offers slightly different conditions for child's consent in relation to information society services. According to article 8. of the GDPR, a lawful consent for data processing can be given if the child is at least 16 years old. If the child is below the age of 16 years, such processing requires that the consent is given or authorized by the holder of parental responsibility over the child. However, Member States may lower the age of child's consent for those purposes as long as the age of consent is at least 13 years (GDPR, art 8, 2021). For instance, in both Finland and Estonia the age limit is 13 years (www.tietosuoja.fi,

2020; www.dataguidance.com, 2020). When discussing child's consent the data processor shall make reasonable efforts to verify that the consent is given or authorized by the holder of parental responsibility over the child (GDPR, art. 8, 2018).

4.4 Processing of special categories of personal data

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, as well as information regarding health or person's sex life or sexual orientation are considered sensitive in nature. This sensitivity grants them a special status concerning data processing. The processing of these special categories of data requires certain conditions to be met according to the GDPR. Recital 51 (2018) of the GDPR argues that "personal data which are particularly sensitive in relation fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms of the data subject."

A notable mention is that processing of photographs of individuals are not considered to be processing of special categories of data. They can be considered as biometric data only when processed through specific technical means allowing identification or authentication of a natural person. Special categories of personal data should not be processed unless certain conditions hold (GDPR, Recital 51, 2018). Article 9. of the GDPR lists these conditions regarding processing of special categories of data and I have assembled them in table 9. Additionally, Member State may provide additional protection over special categories of data (GDPR, Recital 51, 2018). In addition to the special conditions below, the special categories of data also merit the protection of the general principles and other rules of data protection introduced in the GDPR, particularly the conditions for lawful processing mentioned above. The GDPR sets derogations from the general prohibition of processing special categories of data, for instance when the data subject gives their explicit consent or if the processing is carried out for specific needs through legitimate activities by certain associations or foundations (GDPR, Recital 51, 2018).

In the following table I have assembled the conditions that allow derogations regarding processing of special categories of data. "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's

sex life or sexual orientation shall be prohibited unless one of the following applies:" (GDPR, art. 9, 2018).

Table 11. Processing of special categories of data

1.	The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred above may not be lifted by the data subject.
2.	Processing is necessary for the purposes of carrying out out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorized by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
3.	Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
4.	Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit body with a political, philosophical or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.
5.	Processing relates to personal data which are manifestly made public by the data subject.
6.	Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
7.	Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
8.	Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards of a professional secrecy under Union or Member State law or rules established by national competent bodies.
9.	Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
10.	Processing is necessary for archiving purposes in the public interest, scientific or or historical research purposes or statistical purposes in accordance with with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

(GDPR, art. 9, 2018)

Member States may also maintain or introduce further conditions or limitations regarding processing of genetic data, biometric data, or data concerning health (GDPR, art. 9, 2018).

4.5 Rights of the data subject under GDPR

In this chapter I am introducing and discussing the rights of the data subject. These are highly relevant for European smart city initiatives such as FINEST Twins, as the providers of the digital services should be aware of the broad rights of the data subject under GDPR. First and foremost, the data subjects enjoy the right to transparency (GDPR, Recital 58, 2021). The principle of transparency requires that any information addressed to the public should be concise, easily accessible and understandable. This requires the use of clear language and when appropriate even visualization (GDPR, Recital 58, 2021). The service provider should pay attention especially when the manufacturing services for children as children merit specific protection in data protection under GDPR. In a situation where the processing is addressed to a child, should also the language be plain and easy enough for a child to understand (GDPR, Recital 58, 2021).

When collecting data from data subjects, the controller is obliged to provide certain information regarding the data collection. Article 13. of the GDPR (2018) provides a list of information that the data collector should provide:

Table 12. Information provided where personal data are collected from the data subject

1.	The identity and the contact details of the controller and, where applicable, of the controller's representative.
2.	The contact details of the data protection officer, where applicable.
3.	The purposes of the processing for which the personal data are intended as well as the legal basis for the processing.
4.	Where the processing is based on legitimate interests of the controller or a third party, the legitimate interests pursued by the controller or a third party.
5.	The recipients or categories of recipients of the personal data, if any.
6.	Where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

(GDPR, Art. 13, 2018)

In addition, the controller shall provide further information to ensure fair and transparent processing. The controller should determine and inform the time period for which the data are to be stored. If the controller cannot determine a specific time period, they should inform the criteria by which the time period is determined (GDPR, Art. 13, 2018). The controller should also remind the data subject of the right to request access, rectification, erasure and restriction of processing as well as the right to portability of the data regarding the data subject (GDPR, Art. 13, 2018). If the processing is based on data subject's consent, the data controller should also inform that the data subject is free to withdraw their consent of the data processing at any time without affecting the lawfulness of processing based on consent before its withdrawal. The data subject must be also reminded of the right to lodge a complaint with a supervisory authority (GDPR, Art. 13, 2018).

Furthermore, the data subject should be informed whether the provision of personal data is a statutory or contractual requirement. If the personal data is required in order to enter into a contract, the data subject should be made aware of the possible consequences if the data is not provided (GDPR, Art. 13, 2018). If the personal data is used for automated processing such as profiling or other automated decision-making, the data collector has to provide meaningful information about the logic involved, as well as the significance and the consequences of such processing for the data subject (GDPR, Art. 13, 2018).

Finally, if the data collector intends to use the data for other purposes than for which it was initially collected, the data collector should inform the data subject of such usage before the processing (GDPR, Art. 13, 2018). All of the above applies also if the data has not been obtained from the data subject. In such cases the data collector has to also point out the source from which the personal data originates, and if applicable, whether it came from publicly accessible sources (GDPR, Art. 14, 2018). When the data has been obtained from other sources than the data subject, the data collector should inform the data subject of the data collection and related rights within a reasonable period after obtaining the personal data, at the latest within one month (GDPR, Art. 14, 2018). If the personal data is used to contact the data subject, the above information about data collection and related rights should be provided as the contact is made. Also, if the data is disclosed to another recipient, the subject should be informed as soon as the data is first disclosed (GDPR, Art. 14, 2018).

The GDPR sets exceptions to these rules in certain situations. I have assembled the exceptions to the regulations regarding informing the data subject about data collection in table 11 below. It is notable that these exceptions only apply when the data is collected from

other sources than the data subject. If the data is collected from the subject, the above regulation still applies (GDPR, Art 13; GDPR, Art. 14, 2018):

Table 13. The exceptions of informing the data subject

	The regulations regarding informing the data subject about data collection do not apply insofar as:
1.	The data subject already has the information
2.	The provision of such information proves impossible or would involve a disproprtionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or in so far as the obligation to inform the data subject is likely to render impossible or seriously impair the achievement of the objectives of processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.
3.	Obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests.
4.	When the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

(GDPR, Art. 14, 2018)

The GDPR grants the data subjects the right to access to the personal data which have been collected concerning them. That right can be exercised at reasonable intervals and the access should be made easy (GDPR, Recital 63, 2018). The right to access exists for data subject's to be aware of and verify the lawfulness of processing. Data subjects have also the right to know and obtain information of the purposes which the data are processed, and the time period of the processing as well as the recipients of the data and the logic behind any automatic data processing.

When profiling the data subjects have right to know the consequences of such processing (GDPR, Recital 63, 2018). In practice, the data controller should be able to provide remote access to a secure system which would provide the data subject with direct access to their personal data (GDPR, Recital 63, 2018). Also, the data controller needs to ensure that these actions do not infringe rights or freedoms of others, including trade secrets or intellectual property rights. However, the protection of other entities and stakeholders should not be a refusal to provide all information to the data subject (GDPR, Recital 63, 2018).

Article 15 of the GDPR discussed data subject's right of access and it introduces the information that the controller is obliged to provide upon request from the data subject. First,

"the data subject shall have the right to obtain confirmation from the controller as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the information assembled in the following table" (GDPR, Art. 15, 2018).

Table 14. Information to be given to a data subject upon request

1.	The purposes of processing.
2.	The categories of personal data concerned.
3.	The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations.
4.	Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
5.	The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.
6.	The right to lodge a complaint with a supervisory authority.
7.	Where the personal data are not collected from the data subject, any available information as to their source.
8.	The existence of automated decision-making, including profiling, and, at least in the case of profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing.

(GDPR, Art. 15, 2018)

If the personal data are transferred to a third country or to an international organization, the data processor should inform the data subject of appropriate safeguards relating to the transfer (GDPR, Art. 15, 2018). The controller is obliged to provide a copy of the personal data that is being processed. However, if the data subject further requests copies of the personal data after receiving them once, the controller could set a fee based on administrative costs of the data handling and the data handling should not infringe the rights and freedoms of others (GDPR, Art. 15, 2018). These data are most often provided in electronic format to the data subjects (GDPR, Art. 15, 2021).

A data subject has also rights to rectification and erasure of their personal data. Meaning that the data subject has the right to have their inaccurate or incomplete data rectified or completed (GDPR, Art. 16, 2018). The right of rectification or the "right to be forgotten" determines that the "data subject should have right to have their personal data erased and no longer processed when the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has

withdrawn their consent or objects to the processing of personal data concerning them, or where the processing of their personal data does not otherwise comply with the GDPR" (GDPR, Recital 65, 2018).

Article 17 of the GDPR discusses the right to erasure and according to the article "the data subject shall have the right to obtain from the controller the erasure of personal data concerning them without undue delay and the controller shall have the obligation to erase personal data without undue delay when one of the following grounds applies:" (GDPR, Art. 16, 2018)

Table 15. Right to be forgotten

1.	The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.
2.	The data subject withdraws consent on which the processng is based, and where there is no other legal ground for the processing.
3.	The data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing.
4.	The personal data have been unlawfully processed.
5.	The personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.
6.	The personal data have been collected in relation to the offer of information society services directly to a child.

(GDPR, Art. 16, 2018)

Also, if the controller has made the personal data public, and is obliged under some of the conditions introduced in table 13 to erase the personal data, the controller should take reasonable steps, considering the available technology and the cost of implementation, to inform controllers that are processing the data about the request to erasure (GDPR, Art 17, 2018). However, the conditions mentioned here and in table 13 shall not apply if the processing is necessary for exercising the right of freedom of expression. Another exception is if the data are used for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (GDPR, Art. 17, 2018). Also, if the data is collected for reasons of public interest in the area of public health such in purposes of preventive or occupational medicine, for the assessment of the working capacity of an employee or for example if the data is necessary for protecting against serious cross-border threats to health (GDPR, Art. 9; GDPR, Art. 17,

2018). Furthermore, if the data is being used for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, the rights to be forgotten do not apply in so far as the right to be forgotten would seriously impair or render impossible the achievement of the objectives of that processing (GDPR, Art. 17, 2018). Finally, the right to be forgotten is overwritten if the data is used for establishment, exercise or defense of legal claims (GDPR, Art. 17, 2018).

In certain conditions, the data subject might have also a right to restrict processing of their data. The right to restriction of processing is discussed in the Article 18 of the GDPR. According to the article the data subject shall have the right to obtain from the controller restriction of processing when one of the following applies:

Table 16. Restriction of processing

1.	The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data.
2.	The processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead.
3.	The controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defense of legal claims.
4.	The data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

(GDPR, Art. 18, 2018)

If the processing has been restricted under circumstances introduced in table 14, "such personal data shall, except for storage, only be processed with the data subject's consent or for the establishment, exercise, or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or a Member State (GDPR, Art 18, 2018). Upon lifting of the restriction, the data processor shall inform the data subject before the restriction of processing is lifted (GDPR, Art 18, 2018). The concrete methods for restriction of processing include, among others, temporarily moving the selected data to another processing system, or making the data unavailable to users. The data controller can also temporarily remove the data from their website (GDPR, Recital 67, 2018).

If the system in which the data is processed is automated, the restriction should be prioritized through technical means in such a manner that the personal data are not subject to further processing and cannot be altered (GDPR, Recital 67, 2018). Also, the restriction

of data should be clearly indicated in the system (GDPR, Recital 67, 2018). Finally, the controller is responsible of communicating any rectification, erasure or restriction of processing concerning personal data to the recipient to whom the personal data have been disclosed (GDPR, Art. 19, 2018). The controller is relieved from this obligation only if the communicating proves to impossible or involves disproportionate effort. The controller should also inform the data subject about those recipients if the data subject requests it (GDPR, Art. 19, 2018).

Article 20 of the GDPR discusses data subject's rights to data portability. This means that the data subject has the right to receive the personal data concerning them from the data controller which they have provided (GDPR, Art. 20, 2018). These data should be given in a structured, commonly used, and in machine-readable format (GDPR, Art. 20, 2018). The data subject can also if desired, to move these data to another controller without hindrance from the previous controller if only technically feasible (GDPR, Art. 20, 2018). Again, this right to data portability should however not adversely affect the rights and freedoms of others (GDPR, Art. 20, 2018).

The right to object, which is introduced in GDPR Article 21, occurs "where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to their particular situation" (GDPR, Recital 69, 2018). The controller is always responsible to demonstrate the legitimacy of overriding the fundamental rights and freedoms of the data subject (GDPR, Recital 69, 2018). I have assembled the fundamentals of right to object in table 15 below.

Table 17. Right to object

1.	The data subject shall have the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning them, including profiling based on those data. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.
2.	Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning them for such marketing, which includes profiling to the extent that it is related to such direct marketing.
3.	Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
4.	At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.
5.	In the context of the use of information society services, the data subject may exercise their right to object by automated means using technical specifications.
6.	Where personal data are processed for scientific or historical research purposes, the data subject, on grounds relating to their particular situation, shall have the right to object to processing of personal data concerning them, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

(GDPR, Art. 21, 2018)

Article 22 of the GDPR discusses automated individual decision-making, including profiling. The article dictates that "the data subject shall have the right not to be subjected to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them" (GDPR, Art. 22, 2018). Profiling here means any automated processing measuring the data subject's aspects, for instance work performance, health, personal preferences, or economic situation, which produce legal effects (GDPR, Recital 71, 2018). Thus, the data subject has a right to have human interaction included in certain processes where personal aspects are measured, for example when applying for a job (GDPR, Recital 71, 2018). Some exceptions exist, for instance "automated processing shall be sufficient if it is necessary for entering into, or performance of, a contract between the data subject and a data controller" (GDPR, Art. 22, 2018). Furthermore, human intervention is not required if "the decision is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests" (GDPR, Art. 22, 2018). Finally, the automated decision making is sufficient if explicit consent towards it has been given by the data subject (GDPR, Art. 22, 2018). However, in cases where the automated is based on contractual performance between the

data subject and controller or on explicit consent, the controller should implement suitable measures to safeguard the data subject's rights at least in the form of possible human intervention from the data controller's side and to contest the decision (GDPR, Art. 22, 2018).

The regulatory requirements set by the GDPR of using cross-border open data in a smart city initiative are divided into principles relating to processing of personal data and the rights of the data subject. The principles relating to processing of personal data are lawfulness, fairness and transparency, data minimization, accuracy, storage limitation, integrity and confidentiality as well as accountability (GDPR art. 5, 2018). The rights of the data subject are extrinsic and revolve around informing the data subject of the usage of the data and ensuring their consent (GDPR art. 7, 8, 9, 13, 14, 15, 2018). The data subject has also other several rights such as right to be forgotten (GDPR art. 16, 2018), right to restrict the processing of data (GDPR art. 17, 2018) and right to object the processing of their personal data (GDPR art. 21, 2018). In addition, cross-border open data obligates the data processor to ensure that data is transferred to a country or third party that in turn ensures adequate level of protection evaluated by the European Commission (GDPR art. 45, 2018). In conclusion, the rights of the data subject are various and strong under the regulatory framework of the GDPR, and the data controllers, in this case the digital service providers, should comply very carefully with the regulation. Special attention should be given to sensitive data as well as children as a data subject as these data subject's merit special safeguards.

5 Survey on citizen's attitudes towards data processing

5.1 Survey development

In this section I'm introducing my survey of citizen's attitudes towards data processing. I explain how the questionnaire has been developed and provide the rationale behind choosing the survey questions. The survey is based on the GDPR and Technology Acceptance Model (TAM). The GDPR provides base for the attributes regarding privacy issues in terms of its seven principles and TAM compliments the attributes with five items relating to user experience. TAM is an information systems theory that aims to explain how users come to accept and use technology, thus, I used it to accommodate attributes relating user experience. These twelve attributes are then evaluated with each other by the respondents via best-worst scaling. Best-worst scaling is a method of data collection in which the respondents are asked to rank certain items in a survey. The respondents are shown various (in this case three) items in a list, and then they are asked to rank the top and bottom options of those items. The items are shown in rotation until all the items have been ranked with each other, providing a preference list of the respondent. The survey consisted of three categories of questions. Questions related to demographic background, questions about respondent's digital orientation, and questions abouts respondents' preferences regarding smart city services. Questions are presented as either Likert scale questions or best-worst scaling questions. Likert scale questions are used to divide the respondents into different segments by their demographics and digital orientation to identify whether there are differences in the preferences between demographics or engagement with technology.

Finally, the respondents were asked to rate the principles of GDPR (lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, accountability) with the attributes of TAM, 'perceived ease of use' (Venkatesh & Davis, 2000), 'perceived usefulness' (Venkatesh & Davis, 2000), 'self-efficacy' (Karimi & Niknami, 2011), 'cost reduction' (Roca et al., 2006) and 'time saving' (Roca et al., 2006) with the best-worst scaling model with twelve attributes: seven principles of GDPR and five characteristics of TAM. This allowed me to gain insightful data about respondents' preferences about privacy issues when mirroring those issues against attributes that increase user experience.

The principles and characteristics were presented to the respondents equally in a hypothetical scenario and the goal was to find out which attributes were the most valued by

the respondents. The scenario was that the cities of Helsinki and Tallinn launched a new cross-border journey planner application, which could be used within either of these cities or while travelling between the cities. The imaginary mobile application would use respondents' data such as location, address, and national security number to improve the user experience. The respondents were then asked if it were most important for them to for example that the data is processes with appropriate security measures (integrity & confidentiality) or if the journey planner would be easy and effortless to use (perceived ease of use) or if perhaps only relevant data of respondent is being collected (purpose limitation). The principles of GDPR and the TAM elements are veiled in the questions to make the questionnaire more comprehensible for the respondents.

5.2 Testing the survey

I started pilot testing for the survey 27.11.2020. On that Friday I distributed the link for my survey to some of my peers in university as well as my academic instructors responsible for my thesis work. During that weekend, ten people completed the survey and gave me feedback on it. The feedback was mainly positive i.e., no need for adjustments, but some commented on the length of the texts in for example GDPR sections of the survey which I then shortened to reduce respondent fatigue.

Another pain point was the best-worst scaling part in which the respondents had to choose the most important and least important attribute of the journey planner application. As the respondents had to read and weigh the same attributes with each other several times, many respondents thought it was burdensome to answer that part. However, as that is the nature of best-worst scaling I had little choice but to adjust the number of questions in total or the number of items per question. After discussing with professor Merja Halme (2020) about my survey, I settled in twelve questions and three items per question. The survey was open to public from 30.11.2020 to 11.1.2021. I targeted Finnish and Estonian respondents via social media and e-mail. I shared the survey on my Facebook page and asked my friends to share it further to gain a broader audience.

In the next chapter I will go through my questionnaire with to show you how this survey was conducted. I will provide screen shots of the actual survey as it is the most effective way to introduce the survey to you.

5.3 Introducing the survey

In this section I am briefly introducing the survey. The full survey can be found in the appendix section. On the first page of the survey, I explain that the goal of the survey is to capture the attitudes of citizens towards data processing in digital services and that the survey is based on the GDPR. The first questions in the survey are about the respondents' demographics. The respondents are asked to state their gender, location (whether it be Finland or Estonia), age and educational background. I did this to perceive whether there are any significant differences in the preferences between different demographic groups.

After the demographic questions I wanted to find out the respondent's digital orientation and views on data collection. I started by asking the respondents what digital applications they use and how often. I provided examples of the most common ones such as social media, food delivery and ride hailing applications, but there was also "other" option for other digital applications. I also wanted to know if the respondents were at all concerned about the collection and use of their data and the security of these services, and if that would affect their preferences. Thus, I asked about their privacy and security concerns regarding the data collection of the services they use. I used Likert scaling method for this part. Next, I wanted to give the respondents some information about the GDPR and its principles. I also asked if the respondents were familiar with the regulation and its principles, again using Likert scaling.

Finally, the best-worst scaling starts. There are twelve variables that appear in nine different scenarios and the respondent had to rank the most important and the least important attribute every time. This would then create a preference order for the attributes. There was a preparation for the best-worst scaling part of the survey. I stated that the respondent is asked their opinion on data processing done by digital smart city services. I used a hypothetical city bike scenario in which the cities of Helsinki and Tallinn would launch a new cross-border journey planner application, which could be used within either of these cities or while travelling between them. The imaginary mobile application would use data such as location, name, date of birth, national security number, phone number and address, to recommend the best mode of transportation. Then I gave the GDPR principles and TAM elements for the respondents to rank and asked which of the characteristics would be the most important and least important to the respondent in this scenario.

5.4 Results of the survey

When I closed the survey, I had collected in total 122 responses of which 112 were complete. Furthermore, 98 (84%) responses of the completed ones were from Finland and 18 (16%) were from Estonia. To get a thorough view of the respondents in general I'm introducing some demographics of the respondents. As the sample size is rather small, I think it is important to note if some demographic segment is overrepresented as it would affect my conclusions and add implications for future research.

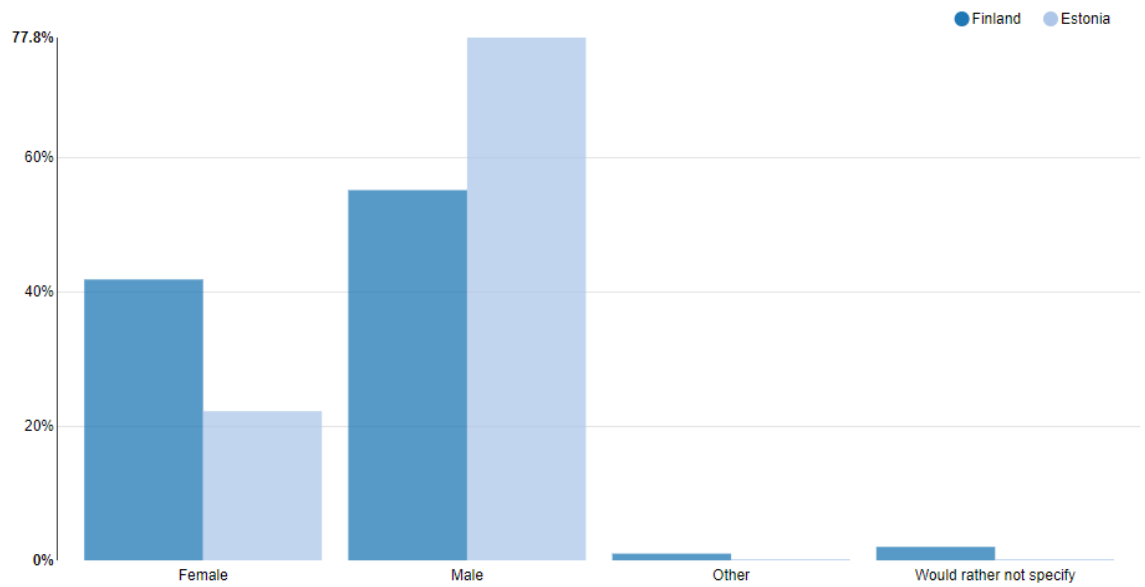


Figure 8. Gender by location

As figure 8 shows, 58,6% of the respondents were male, 38,8% female, 0,9% other and 1,7% would rather not specify. As you can see 41,8% of the Finnish respondents were female and 55,1% were male, respectively. 1% identified as other and 2% would rather not specify their gender. In Estonia most of the respondents were male, as 77,8% of the Estonian respondents were male. The remainder 22,2% were female and no Estonian respondent identified as other or would not specify their gender. So, in general there were slightly more male respondents than female. However, the difference is not too significant in my opinion as the overall distribution was 58,6% and 38,8%

When observing the variable age, we can see that the vast majority (69,8%) of the respondents were 18-30 years old. Another large segment was 31-40 this segment concluded 15,5% of the respondents. The 41-50 segment totalled 6,9% and the 51-60 segment 3,4%. The 61-70 segment was slightly bigger, 4,3%. Unfortunately, I did not get any responses

from neither under 18 years old nor older than 70 years old. In figure 9. I have assembled the age distribution by country.

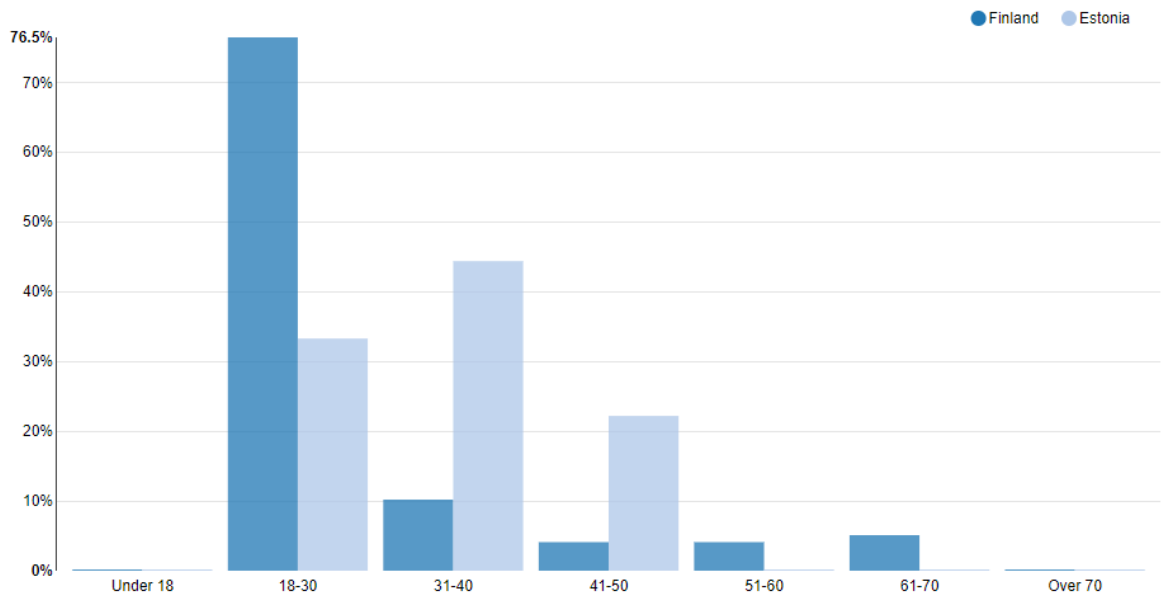


Figure 9. Age by location

Next, I am addressing the educational background of the respondents. As previously, I have assembled the educational background by location in the following figure.

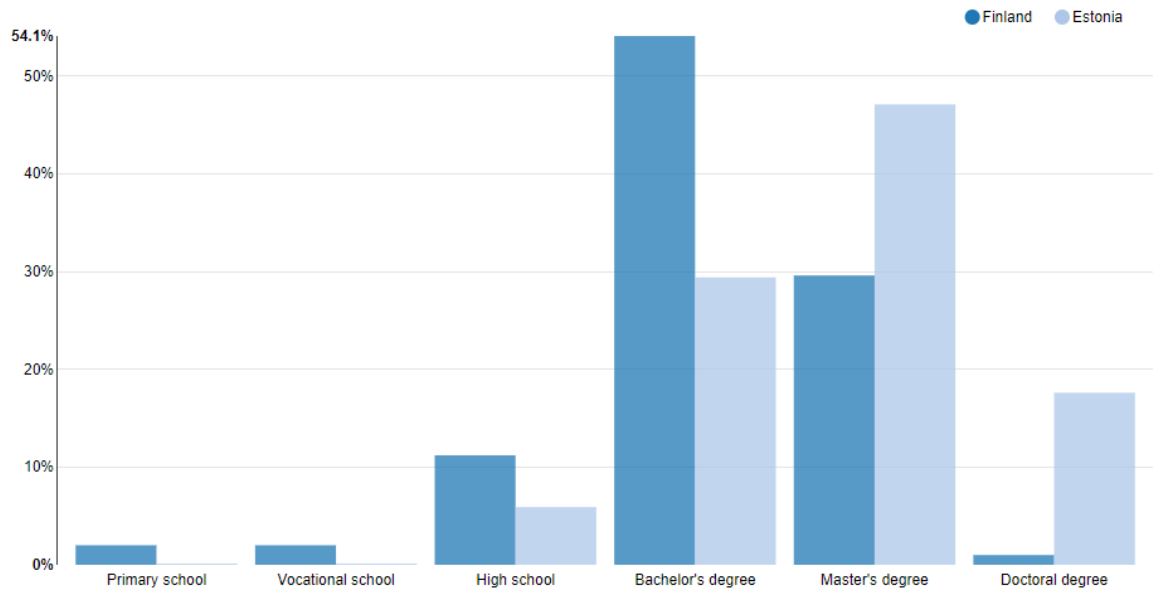


Figure 10. Education by location

Merely primary school graduated respondents totalled 1,7% of the respondents of which all were from Finland. Similarly, 1,7% of the respondents answered to be graduated from vocational school, again solely from Finland. Respondents with high school degree concluded 10,4% of the respondents. From Finnish respondents, 11,2% marked high school as their highest completed level of education and from Estonia 5,9% respectively.

Bachelor's degree seemed to be the most represented educational level among the respondents as 50,4% of the respondents reported bachelor's degree as their highest educational level. 54,1% of the Finnish respondents had bachelor's degree as their highest level of completed education and 29,4% of the Estonian respondents, respectively.

As for master's degree, in total 32,2% of the respondents had completed master's degree. 29,6% of the Finnish respondents and 47,1% of the Estonian respondents. Finally, respondents with doctoral degree totalled 3,5% of the overall respondents. 1% of the Finnish respondents had doctoral degree and 17,6% of the Estonian respondents had doctoral degree.

5.5 Digital orientation

In this chapter I am going to review the digital orientation of the respondents in the form of engagement of digital applications and services. I am also addressing respondents concerns regarding privacy and security of the applications as well as their familiarity with the GDPR. As I am going through these results, I am going to review if there are any significant differences between the results in the two countries in question. Finally, I am going to study how the privacy and security concerns are related with respondent's familiarity with the GDPR.

My first question regarding digital orientation asked the respondents about their social media engagement. Not surprisingly, most of the respondents admitted engaging daily with social media, totalling 90,4% of the respondents. 92,9% of the Finnish and 75% of the Estonian respondents used social media daily. In total, 4,4% of the respondents used social media 5-6 times per week, 1,8% used 3-4 times per week, 0,9% used 1-2 times per week, only 2,6% reported that they used social media less than once per week. The regional distribution of social media engagement is illustrated in the following figure.

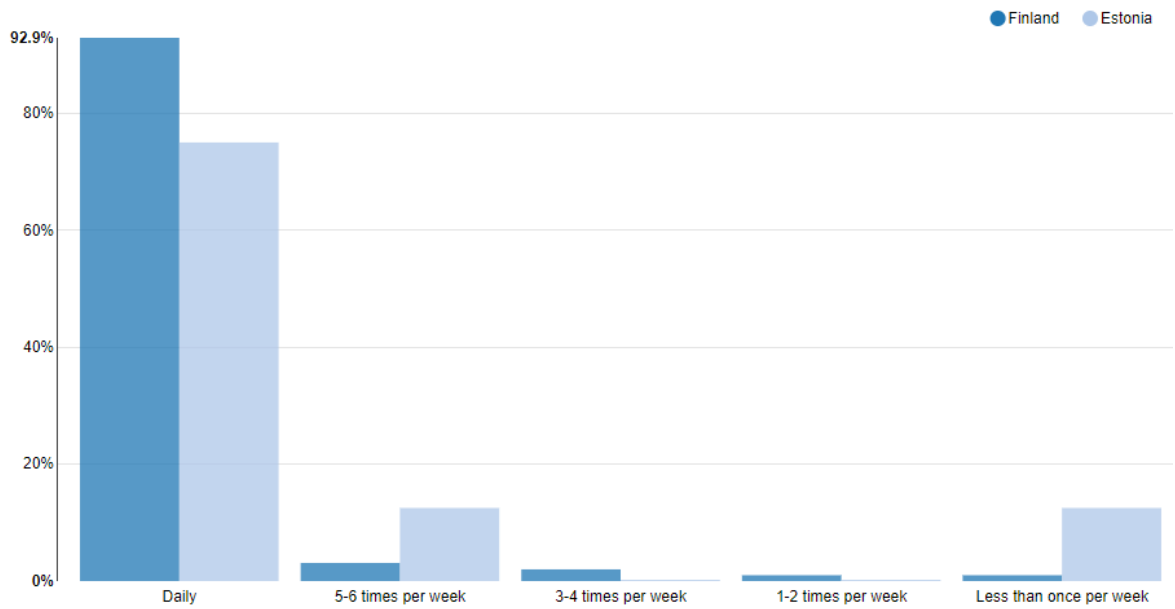


Figure 11. Social media engagement

The second question regarding digital orientation was measuring engagement of digital application complimenting commute transport such as journey planner applications and online tracking for commute transport vehicles. In total, 16,7% of the respondents reported to engage daily with these applications. 14,9% said they use these applications 5-6 times per week, 14,9% used 3-4 times per week, 20,2% used 1-2 times per week and 33,3% used less than once per week. The regional distribution is again illustrated in the following figure.

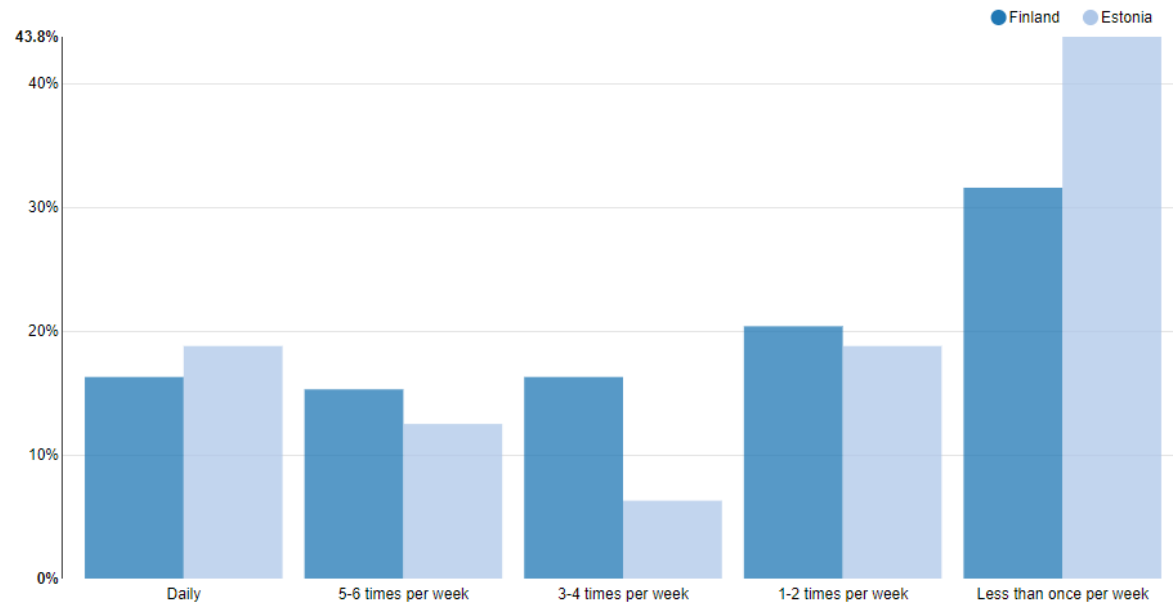


Figure 12. Engagement with commute transport applications

The third question regarding digital orientation was about city bikes or scooters. Only 1,8% of the respondents said to use city bikes or scooters daily. 1,8% reported to use them 5-6 times per week, 10,5% used them 3-4 times per week, 14,9% used them 1-2 times per week, and the majority of 71,1% reported to use them less than once per week. The regional distribution is illustrated below.

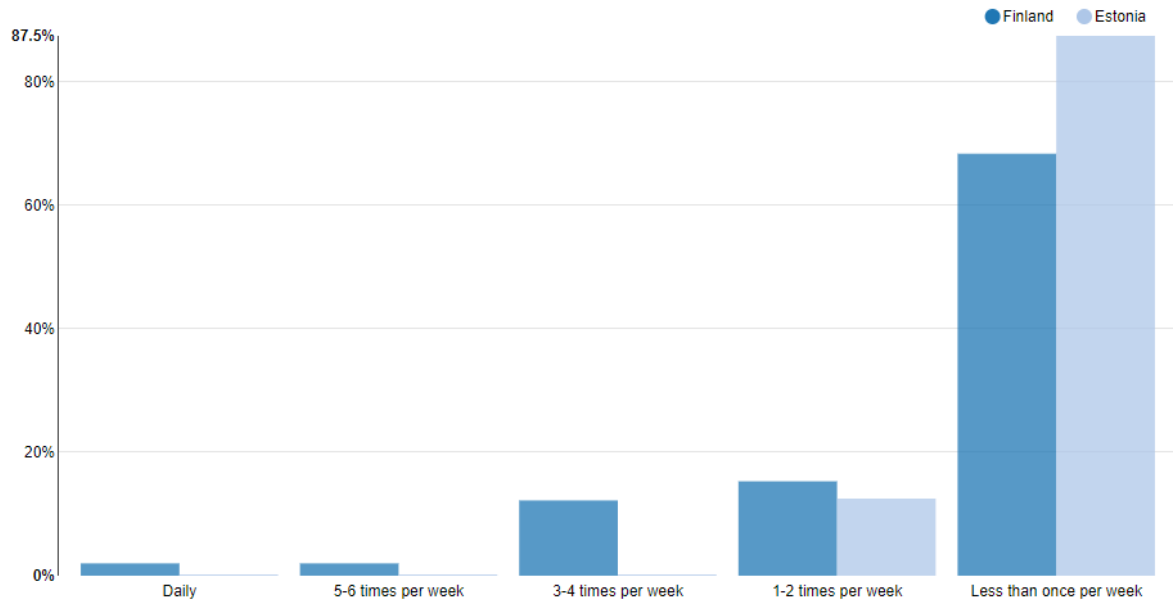


Figure 13. City bike or scooter usage

Also raid hailing applications seemed to be less frequently used by the respondents as you can see in the below figure.

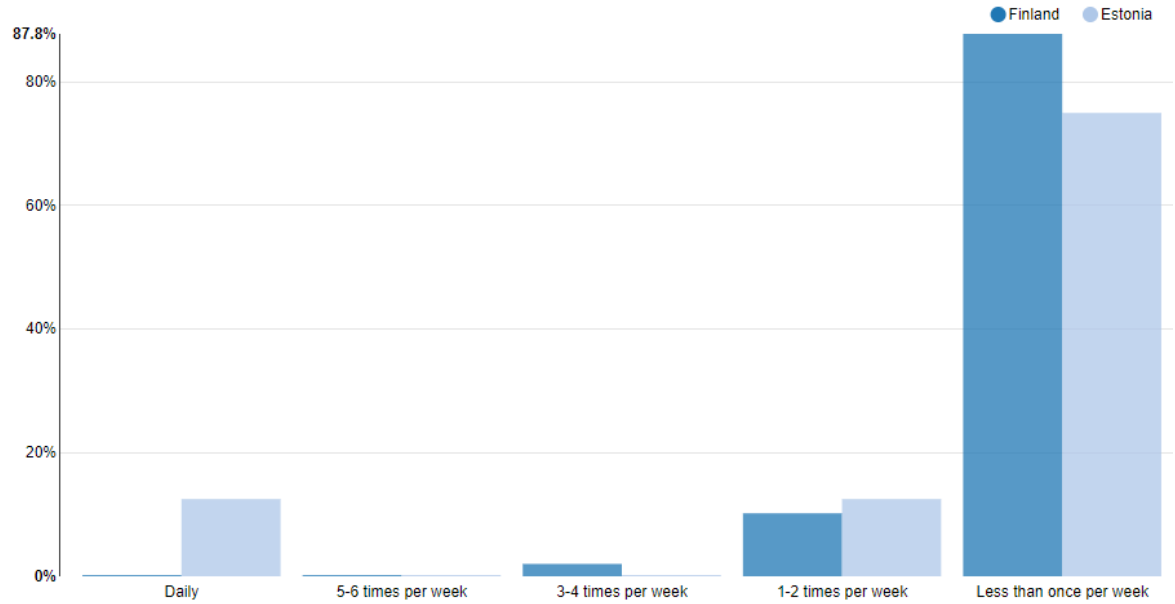


Figure 14. Engagement with ride hailing applications

Only 1,8% of the respondents said to use raid hailing applications daily. Not one of the respondents reported to use ride hailing applications 5-6 times per week. 1,8% said to use them 3-4 times per week and 10,5% said to use them 1-2 times per week. Most of the respondents, 86% reported to use ride hailing applications less than once per week.

Food delivery applications such as Wolt or Foodora were slightly more popular than ride hailing apps. However, frequent daily users were still scarce as only 1,8% of the respondents said to use these applications daily. Again, none of the respondents said to use these applications 5-6 times per week. 6,1% of the respondents used food delivery applications 3-4 times per week and 32,5 said to use them 1-2 times pre week. Here again however the majority of 59,6% said to use food delivery applications less than once per week. The regional distribution is again illustrated in the below figure.

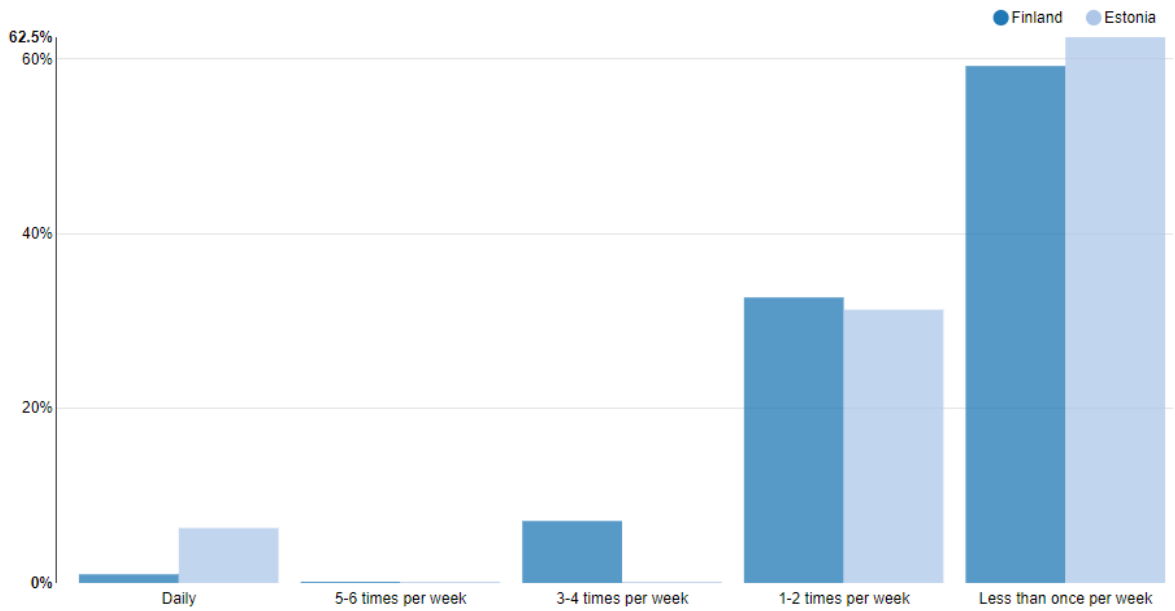


Figure 15. Engagement with food delivery applications

The next segment of digital orientation was mobile banking, and the question was similar to other questions of engagement with such services. As opposed to couple previous digital services, the majority of respondents used mobile banking applications daily, totalling 28,9% of the respondents. 15,8% of the respondents used mobile banking applications 5-6 times per week and 23,7% of the respondents used them 3-4 times per week. 19,3% of the respondents used mobile banking applications 1-2 times per week and finally, 12,3% used them less than once per week. As previously the regional distribution between Finland and Estonia is presented in the following figure.

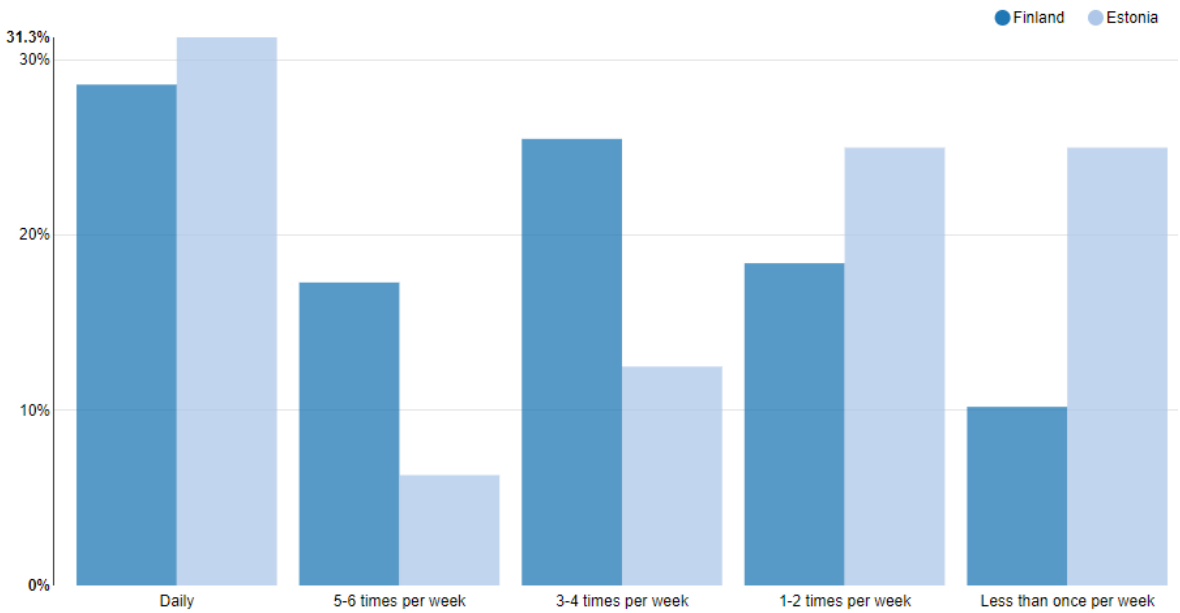


Figure 16. Engagement with mobile banking applications

The seventh segment of digital applications were the conference call applications such as Zoom and Skype. I assume that covid-19 affects these results a lot, leading to more people engaging with these applications daily. In total, 32,5% of the respondents said to engage daily with conference call applications. 20,2% said to engage with them 5-6 times per week and 19,3% said to use them 3-4 times per week. 13,2% reported to use conference call applications 1-2 times per week and 14,9% said to use them less than once per week. The regional distribution is presented in the below figure.

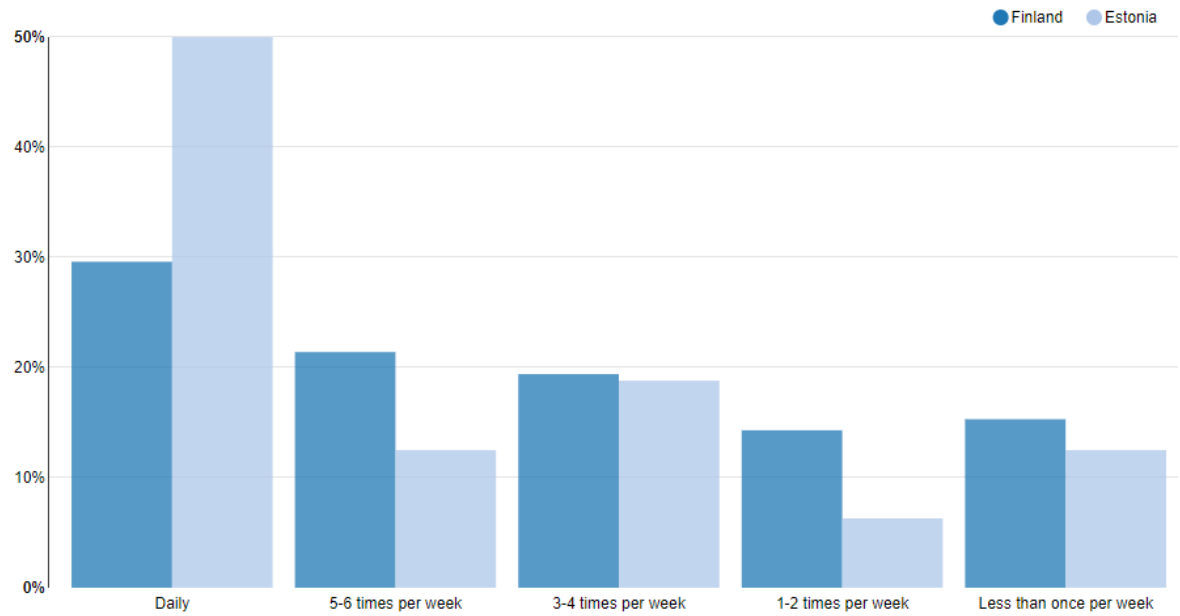


Figure 17. Engagement with conference call applications

The next question in the survey measured the respondent's engagement with streaming services such as Netflix or Twitch. The majority of 37,7% reported to use streaming services daily. 18,4% said to use them 5-6 times per week and 21,1% said to use them 3-4 times per week. Only 6,1% reported to use streaming services 1-2 times per week and 16,7% said to use them less than once per week. The regional distribution is illustrated below.

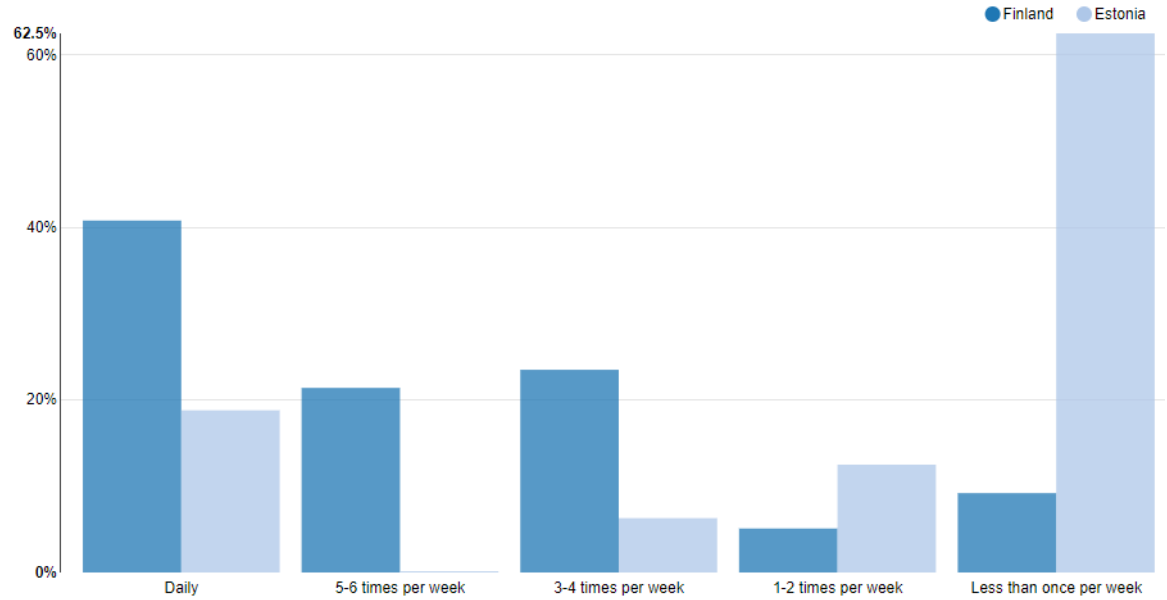


Figure 18. Engagement with streaming services

The ninth question regarding digital orientation was about smart car parks. The engagement with these applications was very low in both regions as you can see in the below figure.

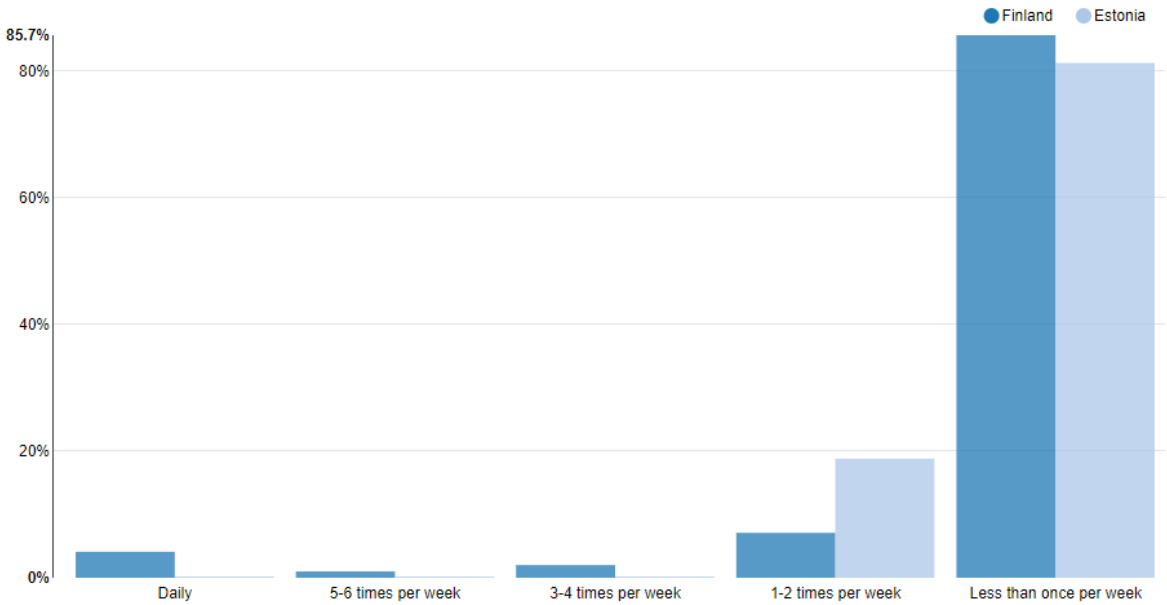


Figure 19. Engagement with smart car parks

The daily users were only 3,5% of the respondents and 0,9% of the respondents said to use smart car parks 5-6 times per week. 1,8% reported to use them 3-4 times per week and 8,8% said to use them 1-2 times per week. The majority of 85,1% reported to use smart car parks less than once per week.

The final segment of digital orientation was just other digital applications. In total 65,8% of the respondents reported to use other digital applications daily. 7,9% said to use them 5-6 times per week and 7% said to use them 3-4 times per week. 11,4% said to use other digital applications 1-2 times per week and 7,9% said to use them less than once per week. The regional distribution is once again presented below.

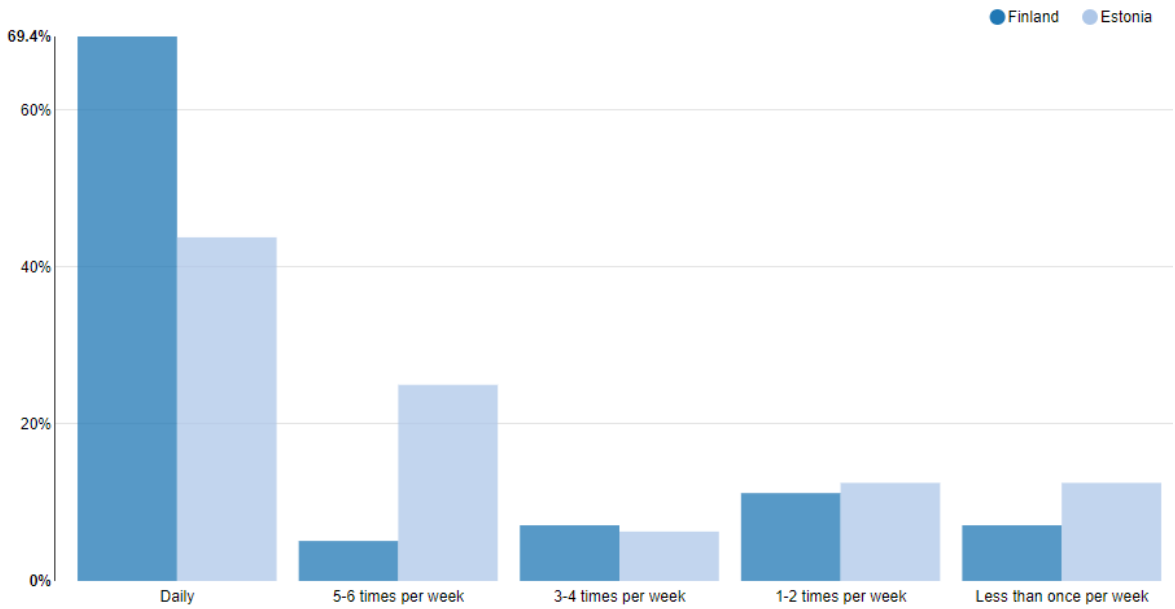


Figure 20. Engagement with other digital applications

In conclusion, the results between Finnish and Estonian respondents seem to be similar. There are no great differences in digital orientation between Finns and Estonians as the figures show. To smart city development, even though Finland and Estonia are different countries, the cross-border smart city initiative seems feasible in terms of citizens' digital orientation. There needs not to be distinctive services for the countries, but rather the smart city services could be developed for a unified group of consumers, rather than for Finns and for Estonians.

5.6 Privacy concerns

Next, I am going to review respondents concerns regarding privacy and security regarding data collection as well as their familiarity with the GDPR. Similarly, to the previous figures, I will present the regional distribution in each parameter and additionally I will present the concerns related to respondents' familiarity with the GDPR. Starting off with privacy concerns, only 5,3% of the respondents said that they are not at all concerned of the privacy issues of the data collection made by digital service providers. 29,8% of the respondents said to be not too concerned of the privacy issues of the data collection and 26,3% were neutral on the manner. The majority of 32,5% reported to be concerned about the privacy issues of the data collection by service providers. However, only 6,1% of the respondents said to be extremely concerned of the privacy issues of the data collection. The regional distribution of privacy concerns by country is illustrated in the figure below.

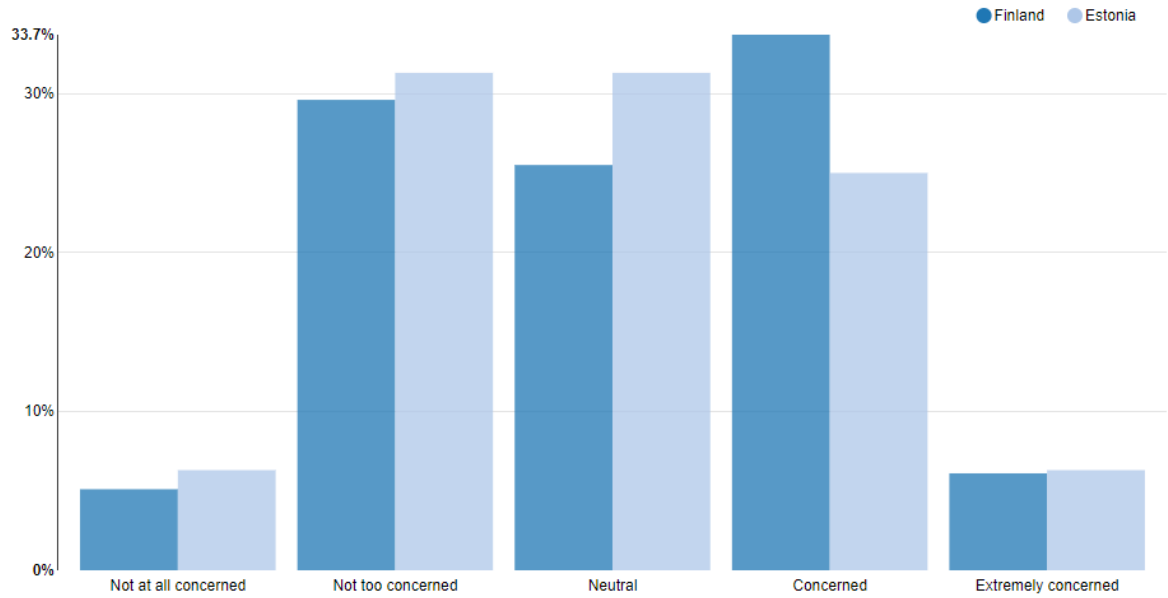


Figure 21. Privacy concerns regarding data collection

As expected, the results regarding respondents' concern towards security of data collection of digital services follow somewhat similar distribution as the privacy concern.

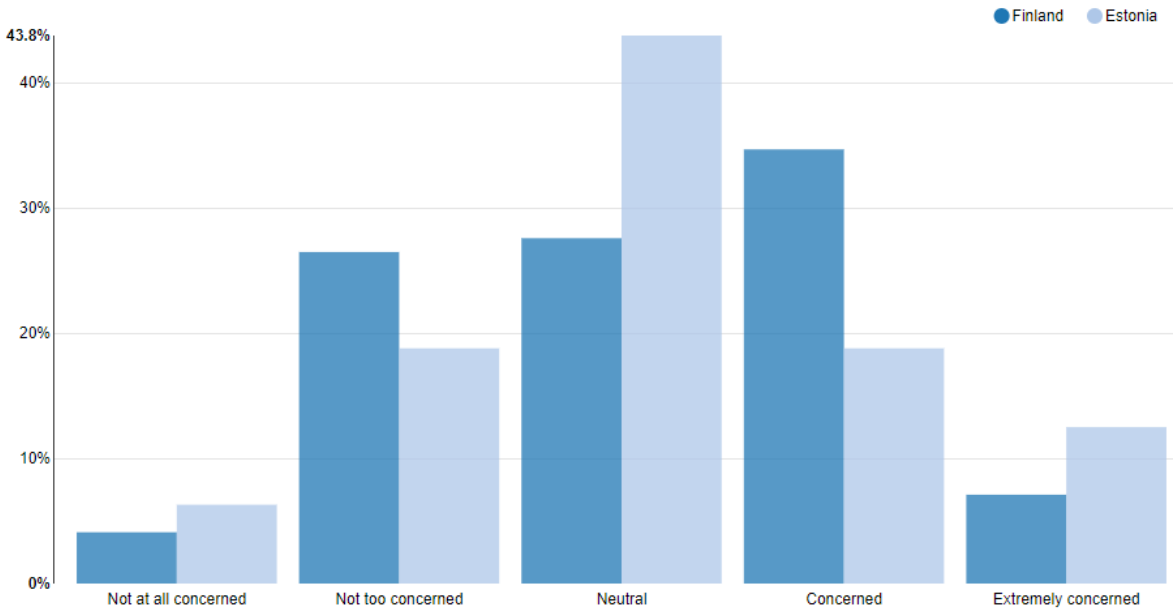


Figure 22. Security concerns regarding data collection

In total, 4,4% of the respondents stated that they are not at all concerned about the security of data collector. 25,4% of the total respondents said they are not too concerned about the security of the data collection of digital services and 29,8% were neutral on the matter. Again, the majority of 32,5% of the total respondents were concerned of the security of their data and 7,9% were extremely concerned.

The survey also measured if the respondents were at all familiar with the GDPR. In the below figure I have assembled the regional results of the GDPR familiarity item of the survey.

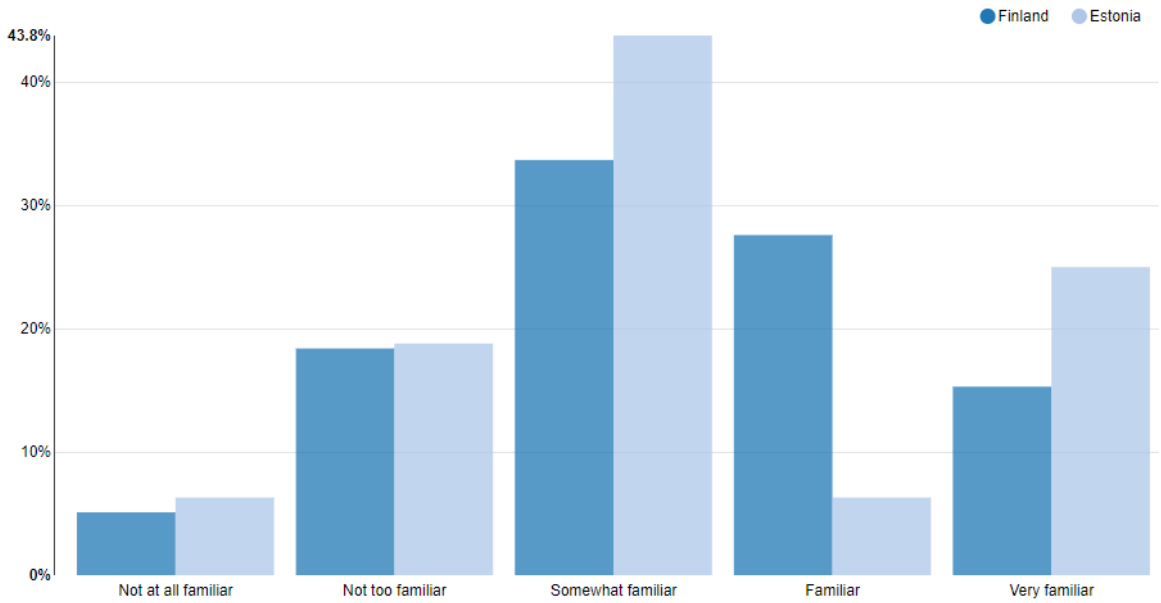


Figure 23. Familiarity with the GDPR

In total, only 5,3% of the respondents reported to be not at all familiar with the GDPR. 18,4% were not too familiar and 35,1 said to be somewhat familiar. 24,6 of the total respondents were familiar with the GDPR and 16,7% of the respondents were very familiar with the regulation.

To conclude this section, I have assembled a figure that represents citizens' concerns regarding security and privacy, but the sample is distributed by the GDPR familiarity item. I did this to see if the familiarity with the regulation would increase or decrease citizens' concerns regarding data collection and privacy. The first figure represents privacy concerns and GDPR familiarity, and the second figure represents security concerns and GDPR familiarity.

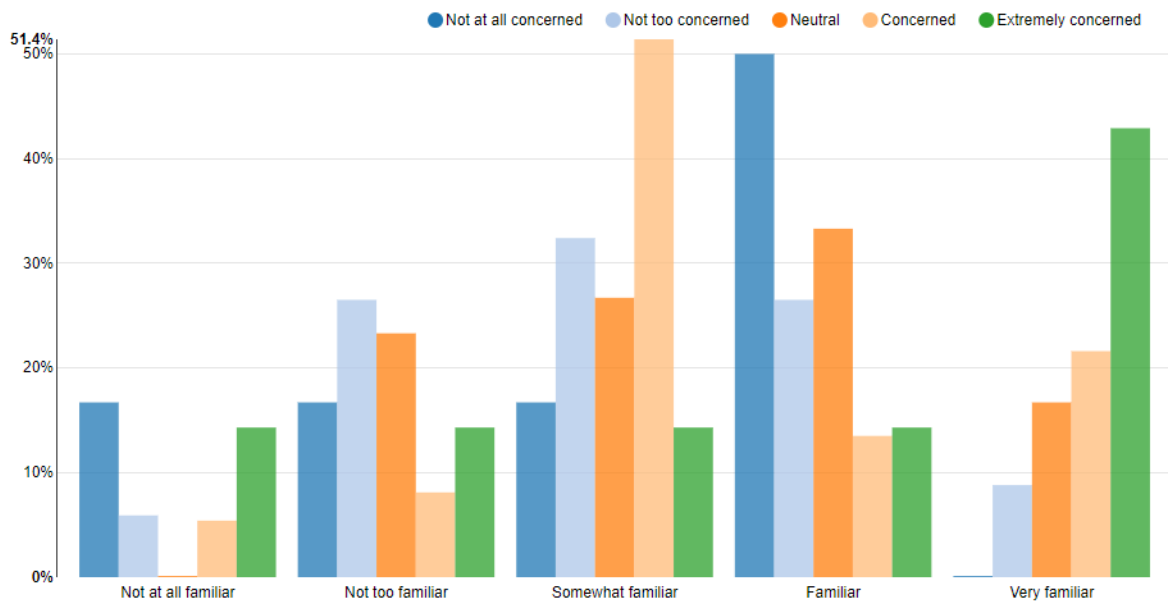


Figure 24. Privacy concern and GDPR familiarity

I am going to break this off by starting with the respondents who were not at all concerned by the privacy of the data collector. Of these respondents, 16,7% were not at all familiar with the GDPR. 16,7% were not too familiar with the GDPR and again 16,7% were somewhat familiar with GDPR. 50% were familiar and none were very familiar with the GDPR. The respondents that said not to be too concerned by the privacy issues of the data collector were distributed a bit more evenly. 5,9% were not at all familiar with the GDPR and 26,5% were not too familiar with the GDPR. 32,4% were somewhat familiar and 26,5 were familiar with the GDPR. 8,8 of the respondents were very familiar with the GDPR.

Of the respondents with neutral attitude towards privacy issues of the data collector none were not at all familiar with the GDPR and 23,3% were not too familiar with the GDPR. 26,7% of the respondents with neutral attitude were somewhat familiar with the GDPR and 33,3 were familiar with the regulation. 16,7% of the respondents with neutral attitude were very familiar with the GDPR.

Of the respondents that said to be concerned with the privacy issues of the data collector 5,4% were not at all familiar with the GDPR and 8,1% were not too familiar with it. Of the concerned respondents 51,4% said to be somewhat familiar with the GDPR and 13,5% were familiar. 21,6% of the concerned respondents were very familiar with the GDPR.

Of the extremely concerned respondents 14,3% were not at all familiar with the GDPR and 14,3 were not too familiar. 14,3% were also somewhat familiar and 14,3% were

familiar with the GDPR. 42,9% of the extremely concerned respondents were very familiar with the GDPR.

I have assembled similar diagram to illustrate respondent's security concerns with their familiarity towards GDPR. It can be seen below.

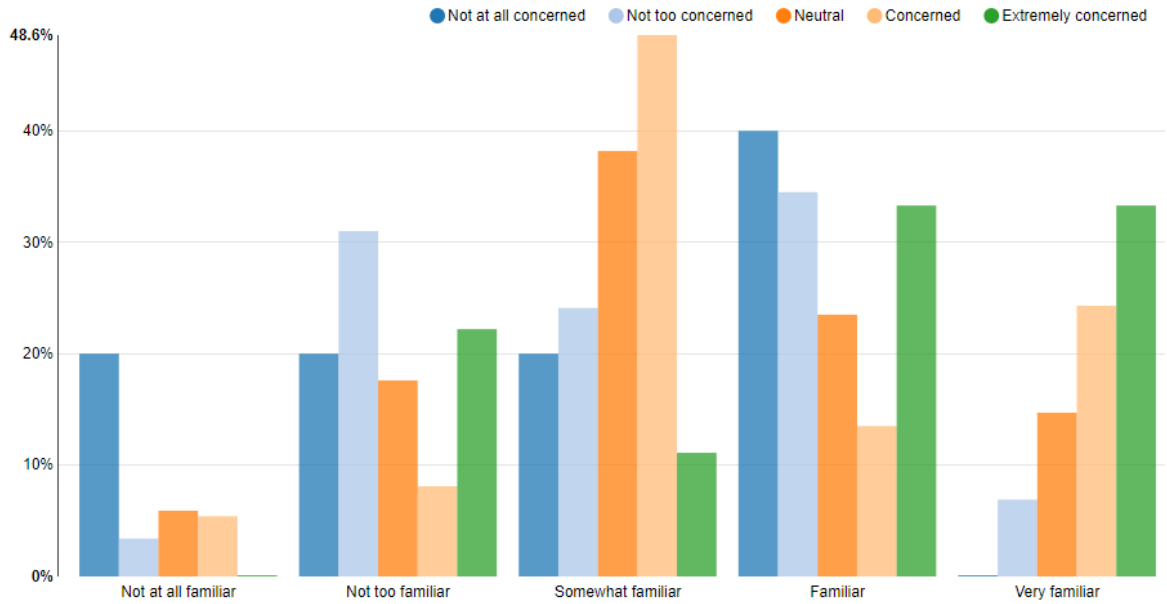


Figure 25. Security concern and GDPR familiarity

Of the respondents that said to be not at all concerned with the security issues of the data collector 20% were not at all familiar with the GDPR. Similarly, 20% were not too familiar and 20% somewhat familiar with the regulation. 40% were familiar and none were very familiar with the GDPR.

Of the respondents that said to be not too concerned of the security issues of the data collector 3,4% were not at all familiar with the GDPR and 31% were not too familiar. 24,1% of these respondents were somewhat familiar and 34,5% were familiar with the GDPR. 6,9% of the not too concerned respondents were very familiar with the GDPR.

As figure 25 shows, 5,9% of the respondents with neutral attitude towards security issues of the data collector were not at all familiar with the GDPR and 17,6% were not too familiar. Of the neutral respondents 38,2% were somewhat familiar and 23,5% were familiar with the GDPR. 14,7% of the neutral respondents were very familiar with the GDPR.

Of the respondents that were concerned towards security issues of the data collector 5,4% were not at all familiar with the GDPR and 8,1% were not too familiar. 48,6% of the

concerned respondents were somewhat familiar and 13,5% said to be familiar with the regulation. 24,3% of the concerned respondents were very familiar with the GDPR.

Finally, of the extremely concerned respondents none said to not at all familiar with the GDPR and 22,2% were not too familiar. 11,1% of the extremely concerned respondents were somewhat familiar with the GDPR and 33,3% were familiar. 33,3% were also very familiar with the regulation. The detailed distribution of respondents towards privacy and security concerns is provided in the appendixes.

When it comes to the security and privacy concerns of the respondents, the Estonian respondents were more neutral and not as concerned regarding privacy issues than the Finnish respondents. The Estonians reported also to be 'very familiar' and 'somewhat familiar' with the GDPR more than the Finnish respondents. The Finnish respondents were again dominantly more 'familiar' with the GDPR, so it is hard to draw conclusions here whether the GDPR familiarity affected the privacy and security concerns. However, figures 24 and 25 show that those that were 'very familiar' with the GDPR were also the most concerned by both privacy and security issues of the data collector. Interestingly, most of the respondents that said to be 'familiar' with the GDPR in turn were 'not at all concerned' by either privacy or security issues of the data collector. This makes the conclusion drawing even trickier and I would suggest that research on the topic should be done with a larger sample size to grasp a clearer view of the possible link between GDPR familiarity and privacy and security concerns. Overall, most of the respondents did not feel strongly about security and privacy issues as the 'not at all concerned' and 'extremely concerned' items had the lowest representation in both security and privacy issues, by both Finnish and Estonian respondents.

5.7 Citizens' preferences in smart city applications

In this chapter I will review the preferences of the respondents regarding GDPR principles and the attributes borrowed from the technology acceptance model. The respondents were shown these attributes in different combinations of attributes and they were asked to mark the most important and least important attribute in twelve different scenarios. Discover software then ranked the attributes and gave them utility scores depending on their popularity in the survey using empirical Bayes model. The score ranges from 0 to 100 for each item and the scores sum to 100 across the items. Higher score implies higher importance

among the respondents and lower scored items were least important. The scores are ratio scaled meaning that an item with a score of 10 is twice as important as an item with a score of 5. As the utility scores are developed based on relative comparisons among the items in the study, there is no information available whether the items are all very much liked or very much disliked by an individual.

The GDPR principles displayed together with the TAM model attributes in many scenarios, hence they were not separate entities in this survey but merely attributes for the respondents to rank. The TAM attributes compared are 'perceived ease of use', 'perceived usefulness', 'self-efficacy', 'cost reduction' and 'time saving'. The GDPR principles compared were 'data minimization', 'accuracy', 'storage limitation', 'lawfulness, fairness and transparency', 'integrity and confidentiality', 'purpose limitation' and 'accountability'. The overall rankings among all respondents are shown in the below figure. Note that the detailed descriptions of the GDPR principles can be found in table 1.

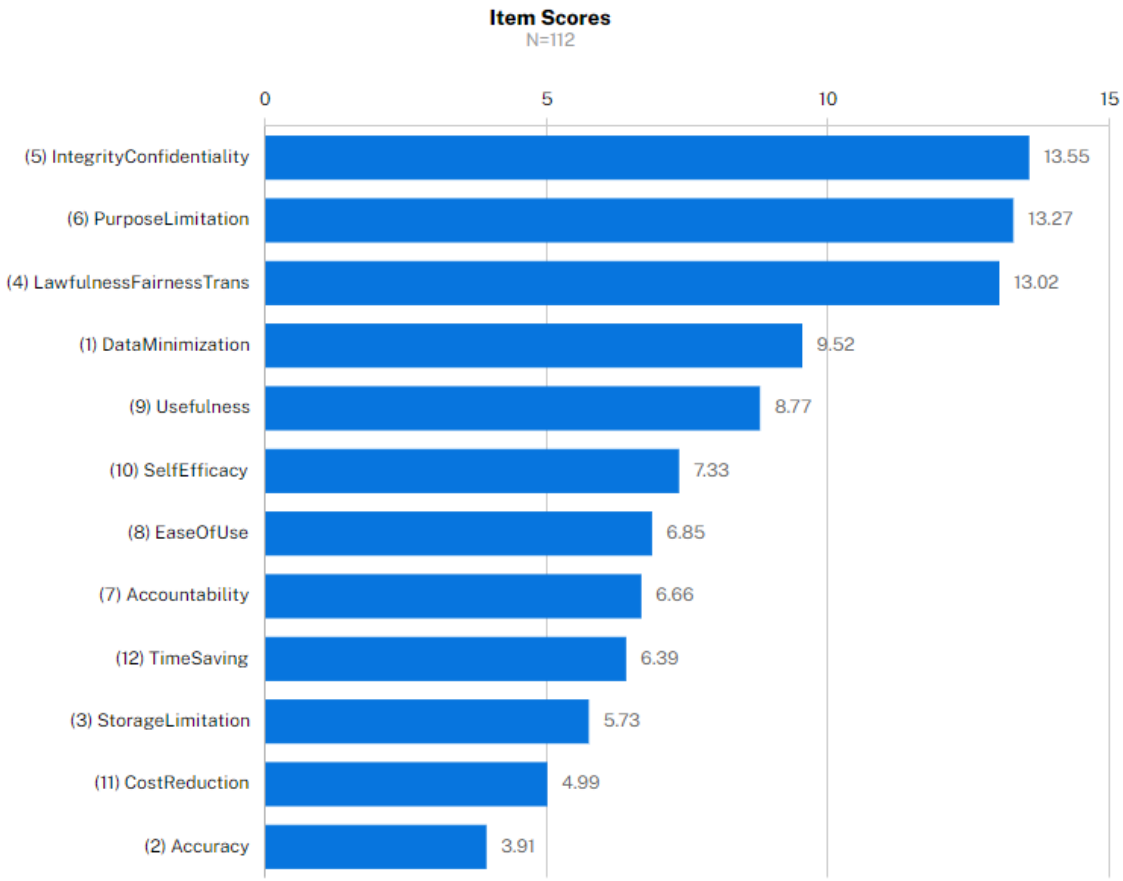


Figure 26. Overall utility scoring

Although the respondents did not feel strongly about security and privacy issues of the data collector, the GDPR principles were rated as more important than the TAM elements, indicating that security and privacy issues are more important than user experience. As the figure shows, 'integrity and confidentiality' were the most important attributes for the respondents with a utility score of 13,55 with 'purpose limitation' as close second with a utility score of 13,27. Third place goes to 'lawfulness, fairness and transparency' with a utility score of 13,02. These three items are very close to each other and hence were seen as the most important factors for the respondents regarding digital services. Notably, the top four items are all solely GDPR principles as 'data minimization' is on the fourth place with a utility score of 9,52.

On the fifth place we have our first TAM element, 'usefulness' with a utility score of 8,77 and on the sixth place we have our second TAM element, 'self-efficacy'. The seventh most important attribute was 'ease of use' with a utility score of 6,85 and not far behind we have our next GDPR item 'accountability' with a utility score of 6,66. On the ninth place we have yet another TAM item, 'time saving' with a utility score of 6,39 and on the tenth place we have a GDPR item 'storage limitation' with a utility score of 5,73. Second to last place in importance goes to TAM element 'cost reduction' with a utility score of 4,99 and the last place goes to GDPR attribute 'accuracy' with a utility score of 3,91.

5.7.1 Preferences by demographics

Next, I will provide tables in which I demonstrate the preferences of each demographic group by showing each group's utility scoring for each item. The preferences by gender and their utility scoring are shown in the table below:

Table 18. Preferences by gender

Item	Label	Total N=112	Female N=42	Male N=67	Other N=1	Would Rather Not Specify N=2
5	IntegrityConfidentiality	13.55	13.94	13.24	9.52	18.15
6	PurposeLimitation	13.27	13.45	13.11	12.74	14.90
4	LawfulnessFairnessTrans	13.02	13.44	12.81	7.80	14.02
1	DataMinimization	9.52	8.99	9.81	3.07	14.21
9	Usefulness	8.77	8.55	9.04	4.52	6.55
10	SelfEfficacy	7.33	7.99	6.90	16.26	3.68
8	EaseOfUse	6.85	6.99	6.66	11.97	8.10
7	Accountability	6.66	6.56	6.68	4.30	9.13
12	TimeSaving	6.39	6.42	6.46	4.26	4.35
3	StorageLimitation	5.73	5.51	5.96	3.09	3.92
11	CostReduction	4.99	4.75	5.08	18.09	0.40
2	Accuracy	3.91	3.41	4.26	4.38	2.60

As the table shows, the utility scorings of both male and female respondents follow closely the overall utilities of the total population. Hence, gender does not seem to affect the utility scores of the respondents, at least not dramatically. The respondents that identified themselves as ‘other’ or ‘would rather not specify’ were so scarce that it is not feasible to draw conclusions based on those respondents.

When observing the preferences by location, the Finnish population follows closely to the total population of the respondents. As for the Estonian respondents there is way more variation in the preferences when compared to the total population, however, the Estonian respondents were rather scarce as well totalling only 15 respondents so it is possible that total preferences would look different with more equal distribution between the countries. With such scarce respondents it is hard to say if the Estonian respondents vary from the total population or from the Finnish population. To find out we would need to conduct the survey with more Estonian respondents. Interestingly, in the Estonian population the item ‘usefulness’ reached a utility score of 12,20 which is relatively high and close second to the highest utility scoring of 12,33 in the same group which was ‘purpose limitation’. This is

notable as usually the GDPR elements were rated as more important than the TAM elements. This could be explained by the rather small sample size from Estonia meaning that individual preferences were more highlighted than the overall preferences of the population.

Table 19. Preferences by location

Item	Label	Total N=112	Finland N=97	Estonia N=15
5	IntegrityConfidentiality	13.55	14.06	10.31
6	PurposeLimitation	13.27	13.41	12.33
4	LawfulnessFairnessTrans	13.02	13.61	9.24
1	DataMinimization	9.52	9.69	8.42
9	Usefulness	8.77	8.24	12.20
10	SelfEfficacy	7.33	6.98	9.60
8	EaseOfUse	6.85	6.86	6.84
7	Accountability	6.66	6.70	6.36
12	TimeSaving	6.39	5.83	10.00
3	StorageLimitation	5.73	5.78	5.38
11	CostReduction	4.99	4.94	5.29
2	Accuracy	3.91	3.89	4.05

Moving on to the age variable we face similar difficulties with the results. The 18-31 bracket follows closely to the overall population, but also 71% of the respondents fall into this bracket. Notably, in all age groups however, at least one or more GDPR principles were rated with highest utility scoring, above the TAM elements. ‘Integrity and confidentiality’ was rated as the highest utility item in three different age group: 18-30, 41-50 and 51-60. In the 31-40 bracket ‘lawfulness, fairness and transparency’ -item was rated with the highest utility. In the 61-70 bracket the ‘data minimization’ -item reached the highest utility score. Notably, in this age group also the ‘ease of use’ item had relatively high utility score compared to other age groups.

Table 20. Preferences by age

Item	Label	Total N=112	18-30 N=80	31-40 N=15	41-50 N=8	51-60 N=4	61-70 N=5
5	IntegrityConfidentiality	13.55	14.59	9.09	13.34	17.04	7.89
6	PurposeLimitation	13.27	13.77	11.83	10.93	15.59	11.41
4	LawfulnessFairnessTrans	13.02	13.24	11.95	12.08	17.29	10.78
1	DataMinimization	9.52	9.06	8.69	12.77	12.86	11.51
9	Usefulness	8.77	8.78	10.87	7.69	5.33	6.83
10	SelfEfficacy	7.33	6.82	9.77	7.20	6.24	9.30
8	EaseOfUse	6.85	6.57	8.79	5.79	3.32	10.16
7	Accountability	6.66	6.96	6.51	5.98	2.96	6.37
12	TimeSaving	6.39	6.18	7.73	7.83	2.83	6.33
3	StorageLimitation	5.73	5.52	6.51	6.15	6.69	5.33
11	CostReduction	4.99	5.24	3.94	5.17	3.01	5.35
2	Accuracy	3.91	3.27	4.33	5.06	6.83	8.74

Table 21. Preferences by education

Item	Label	Total N=112	Primary School N=2	Vocational School N=2	High School N=11	Bachelor's Degree N=58	Master's Degree N=35	Doctoral Degree N=4
5	IntegrityConfidentiality	13.55	9.55	11.01	14.76	14.36	13.29	4.10
6	PurposeLimitation	13.27	9.28	15.80	14.85	13.10	13.68	8.47
4	LawfulnessFairnessTrans	13.02	7.71	19.83	13.29	12.93	13.42	9.39
1	DataMinimization	9.52	12.16	12.23	11.40	8.90	9.78	8.33
9	Usefulness	8.77	6.14	1.57	7.23	9.13	8.18	17.92
10	SelfEfficacy	7.33	8.65	6.15	5.79	6.43	9.02	9.91
8	EaseOfUse	6.85	9.33	4.36	5.90	6.57	7.48	8.18
7	Accountability	6.66	8.88	9.94	4.44	7.62	5.84	3.24
12	TimeSaving	6.39	4.06	1.78	3.74	6.51	6.40	15.31
3	StorageLimitation	5.73	10.41	9.39	8.17	5.55	4.86	5.02
11	CostReduction	4.99	5.74	3.23	5.92	5.20	4.34	5.66
2	Accuracy	3.91	8.09	4.71	4.51	3.71	3.72	4.46

When addressing preferences by education, we face similar constraints as with other demographic groups as the vast majority of respondents are from two educational group ‘bachelor’s degree’ and ‘master’s degree’. These two groups combined constitute 83% of

the respondents. Hence, the other group's statistical significance is somewhat negligible. However, these two groups follow closely to the total population's distribution of utility scoring and there are no significant outliers in either of these groups.

5.7.2 Preferences by concern and GDPR familiarity

Next, I will address the utility scorings and privacy concerns. Not surprisingly, the respondents that reported to be 'not at all concerned' by the data collector's privacy issues rated the TAM elements higher than the GDPR elements, 'self-efficacy', 'time saving' and 'usefulness' scoring the highest utilities. 'Cost reduction' scored slightly lower in this group and notably is still higher than the highest GDPR element 'integrity and confidentiality'. Even though all the TAM elements were rated higher than the GDPR elements in this group, the most important item overall, 'integrity and confidentiality' scored highest in this group too when compared to other GDPR items. Interestingly, respondents that said to be 'not too concerned' about the privacy issues of the data collector did not rate the TAM elements above GDPR principles, but rather the utility scorings of this group follow the total distribution of preferences.

Table 22. Preferences by privacy concern

Item	Label	Total N=112	Not At All Concerned N=6	Not Too Concerned N=34	Neutral N=30	Concerned N=35	Extremely Concerned N=7
5	IntegrityConfidentiality	13.55	8.24	13.36	13.20	15.00	13.31
6	PurposeLimitation	13.27	7.90	13.27	12.85	14.61	12.94
4	LawfulnessFairnessTrans	13.02	6.72	13.22	13.10	13.74	13.56
1	DataMinimization	9.52	6.92	9.59	8.79	10.40	10.10
9	Usefulness	8.77	11.37	9.48	9.13	7.56	7.61
10	SelfEfficacy	7.33	12.73	6.93	6.99	6.85	8.60
8	EaseOfUse	6.85	11.37	7.68	6.03	6.17	5.94
7	Accountability	6.66	4.45	6.28	7.27	6.67	7.68
12	TimeSaving	6.39	11.55	6.62	5.99	5.74	5.82
3	StorageLimitation	5.73	2.36	5.05	6.45	6.23	6.26
11	CostReduction	4.99	9.56	5.24	4.74	4.23	4.68
2	Accuracy	3.91	6.84	3.28	5.45	2.80	3.49

Apart from the 'not at all concerned' -group all the respondents rated the three top GDPR principles as the most important in regarding privacy issues of the data collector. Hence, following the total distribution of utility scores in the survey.

The utility scorings and security concerns follow a similar pattern as with privacy concerns. The respondents that said to be ‘not at all concerned’ by the security issues of the data collector rated most of the TAM elements higher than GDPR principles. However, they rated ‘purpose limitation’ and ‘integrity and confidentiality’ higher than ‘cost reduction’. In other segments the three top GDPR principles dominate the utility scorings once again.

Table 23. Preferences by security concern

Item	Label	Total N=112	Not At All Concerned N=5	Not Too Concerned N=29	Neutral N=34	Concerned N=35	Extremely Concerned N=9
5	IntegrityConfidentiality	13.55	9.12	12.24	13.26	15.36	14.36
6	PurposeLimitation	13.27	9.58	13.17	12.41	14.56	13.83
4	LawfulnessFairnessTrans	13.02	6.56	12.70	12.79	14.21	13.89
1	DataMinimization	9.52	6.33	10.61	7.18	10.99	10.91
9	Usefulness	8.77	11.86	8.72	10.74	6.99	6.69
10	SelfEfficacy	7.33	9.73	7.43	7.98	6.31	7.24
8	EaseOfUse	6.85	12.00	7.53	7.16	5.71	5.10
7	Accountability	6.66	6.41	5.82	6.07	7.75	7.45
12	TimeSaving	6.39	11.04	6.49	7.98	4.49	4.88
3	StorageLimitation	5.73	2.26	5.65	5.14	6.25	8.15
11	CostReduction	4.99	8.77	5.79	5.25	3.90	3.58
2	Accuracy	3.91	6.33	3.85	4.04	3.49	3.91

Finally, let us observe the utility scorings related to GDPR familiarity. First, the respondents that were ‘not at all familiar’ with the GDPR rated TAM elements as their top priority, with ‘usefulness’ reaching the highest utility score of 12,75. ‘Ease of use’ being the close second with a utility scoring of 12,31. The third place in this segment goes to ‘self-efficacy’ with 11,90 utility scoring, but the GDPR principles ‘integrity and confidentiality’ is almost on par with ‘self-efficacy’, reaching a utility score of 11,86. As for the other groups of this segment the distribution of utility scoring is the usual. Three top GDPR principles ‘integrity and confidentiality’, ‘purpose limitation’ and ‘lawfulness, fairness and transparency’ having the greatest importance over everything else. For respondents that were ‘not too familiar’ with the GDPR and for those that were ‘very familiar’ ‘purpose limitation’ was the top priority. For the other groups of this segment ‘integrity and confidentiality’ was paramount.

Table 24. Preferences by GDPR familiarity

Item	Label	Total N=112	Not At All Familiar N=6	Not Too Familiar N=21	Somewhat Familiar N=38	Familiar N=28	Very Familiar N=19
5	IntegrityConfidentiality	13.55	11.86	12.41	14.00	13.44	14.63
6	PurposeLimitation	13.27	9.62	12.88	12.80	13.39	15.59
4	LawfulnessFairnessTrans	13.02	10.86	11.37	12.53	14.06	14.99
1	DataMinimization	9.52	6.47	8.17	10.49	9.60	9.91
9	Usefulness	8.77	12.75	9.74	8.71	9.33	5.75
10	SelfEfficacy	7.33	11.90	8.26	7.45	6.58	5.75
8	EaseOfUse	6.85	12.31	7.24	6.72	6.38	5.68
7	Accountability	6.66	2.09	6.78	6.29	6.93	8.31
12	TimeSaving	6.39	9.21	7.55	6.28	6.46	4.34
3	StorageLimitation	5.73	5.14	5.16	5.67	5.00	7.72
11	CostReduction	4.99	4.16	6.26	5.52	4.65	3.29
2	Accuracy	3.91	3.63	4.19	3.55	4.18	4.04

In conclusion, the GDPR principles were more important to the respondents that the TAM elements indicating that the security and privacy issues are more important to the citizens than user experience. The smart city administration should bear this in mind when developing digital applications for smart city initiatives.

6 Conclusions

In this section I am going to conclude the findings of my thesis as well as reflect my initial hypothesis of higher focus of human value related items being more important to respondents. I am addressing each of my research question in the order they appeared in the thesis starting off the possibilities of how open data could be used for developing digital services in cross-border smart cities. Open data enables various smart city services through sensors, citizens, and smart devices within the city. The main contributor for emergence of these services are the enabling technologies such as ubiquitous connectivity, sensor networks, autonomous systems, smart cards, wearable devices, intelligent vehicles, open data, IoT and cloud computing (Eckoff & Wagner, 2017). The smart city services can be further divided to subgroups of services, smart people, smart living, smart environment, smart governance, smart economy and smart mobility.

The regulatory requirements set by the GDPR of using cross-border open data in a smart city initiative are divided into principles relating to processing of personal data and the rights of the data subject. The principles relating to processing of personal data are lawfulness, fairness and transparency, data minimization, accuracy, storage limitation, integrity and confidentiality as well as accountability (GDPR art. 5, 2021). The rights of the data subject are extrinsic and revolve around informing the data subject of the usage of the data and ensuring their consent (GDPR art. 7, 8 , 9, 13, 14, 15, 2021). The data subject has also other several rights such as right to be forgotten (GDPR art. 16, 2021), right to restrict the processing of data (GDPR art. 17, 2021) and right to object the processing of their personal data (GDPR art. 21, 2021). In addition, cross-border open data obligates the data processor to ensure that data is transferred to a country or third party that in turn ensures adequate level of protection evaluated by the European Commission (GDPR art. 45, 2021). In conclusion, the rights of the data subject are various and strong under the regulatory framework of the GDPR, and the data controllers, in this case the digital service providers, should comply very carefully with the regulation. Special attention should be given to sensitive data as well as children as a data subject as these data subject's merit special safeguards.

Finally, the attitudes and privacy concerns of citizens regarding data processing in smart city context. First, let us address the overall results of the survey. Overall, the GDPR items were seen as more important as the TAM items as the first four most important items are all GDPR attributes and the first TAM item 'usefulness' is on the fifth place. The three

most important items were ‘integrity and confidentiality’, ‘purpose limitation’ and ‘lawfulness, fairness and transparency’. All these three items have a utility score above 13 and they are almost level when assessing importance with each other by the respondents. The respondents rated ‘integrity and confidentiality’ as the most important attribute among the items, meaning that for most respondents, it is paramount that their data is processed in a manner that ensures appropriate security measures. It also natural that the respondents want to limit the purposes of using their data to only for the purposes they have given their blessing on, hence the high importance of ‘purpose limitation’ attribute. Similarly, lawful, fair and transparent use of data is seen as very important as these values greatly contribute to safe handling of personal data. ‘Data minimization’ was rated as the fourth important attribute, with a utility scoring of 9,52 which is substantially lower than the top three attributes. Yeh (2017) states that in his study surveying Taiwanese cities reveal that “citizens are willing to accept and use ICT-based smart city services if the services are designed with innovative concepts that secure their privacy and offer a high quality of services”. The findings in this thesis support this statement as the citizens rated the privacy elements with high importance. In addition to Yeh’s statement I would state that securing citizens’ privacy is even more important than offering high quality of services.

In contrary to my initial hypothesis, the most important attribute ‘integrity and confidentiality’ has little connections with Schwartz’s human values. As ‘integrity and confidentiality’ attribute has only one implicit link to ‘security – personal’ human value, it is one of the vaguest connections between GDPR attributes and Schwartz’s human values. Similarly, ‘purpose limitation’ the second most important attribute according to the survey, has only one implicit link to ‘self-direction – action’ human value. Of the top three attributes, only ‘lawfulness, fairness and transparency’ had several explicit and implicit links to Schwartz’s human values. As these attributes had highly varying connections to human values, I have to reject my initial hypothesis of higher focus of human value related items being more important to the public.

The highest utility TAM item was ‘usefulness’ on the fifth place with a utility scoring of 8,77. As expected, usefulness is very valued attribute considering digital applications and unsurprisingly highest of the TAM elements. ‘Self-efficacy’ and ‘ease of use’ follow closely with utility scores of 7,33 and 6,85 respectively. After these TAM elements we have ‘accountability’ with a utility score of 6,66 which was again a GDPR item. ‘Accountability’ in this case means that mishandling of data by the service provider will be sanctioned. So, it seems it is somewhat important that the service provider is accountable of mishandling of

data, however it is not nearly as important as the previous GDPR elements. I believe this is due to the reactive nature of the 'accountability' attribute. People want the service provider to be sanctioned of mishandling their data but prefer that the data is handled properly in the first place. For example, 'integrity and confidentiality' was twice as important as 'accountability' in terms of utility scorings in this survey.

The next item on the list is 'time saving' with a utility score of 6,39. Time saving was surprisingly insignificant among the respondents. However, we must remember that this survey does not measure whether an attribute is important or not, it scales these attributes against one another, not to some external level of importance. Hence, even the attributes with low utility scores could be important by the respondents as well. The ones with higher utility scores are just more important compared to lesser scores.

The three bottom attributes are 'storage limitation', 'cost reduction' and 'accuracy' meaning that they were the three least important attributes for the respondents overall. Storage limitation was highest of the bottom three, reaching utility score of 5,73 this attribute meant that user's data would be deleted from the database after processing. Surprisingly, 'cost reduction' reached a utility score of only 4,99 meaning that it was the lowest overall TAM element and one of the lowest attributes overall, it seems that people are willing to pay premium for careful processing of their data as well as for functional services. The least important attribute was 'accuracy' reaching utility score of 3,91 meaning that the respondents do not find it very important that their data is correct and accurate.

Next, I am going to assess some preferences on different demographic groups and present the main take-aways of the demographic groups. According to the survey, gender has little importance when assessing these utilities. The genders follow closely the utility scorings of the overall population and there are no significant anomalies among the utility scorings of the attributes. When addressing locational differences however the results were not as uniform. The Finnish population followed closely to the results of the overall population, but there was some variation between the Estonian respondents when compared to the overall population. For example, among the Estonian population, the attribute 'purpose limitation' with a utility score of 12,33 was rated as the most important attribute and 'usefulness' was rated as the second highest with a utility score of 12,20. This is notable as this varies largely from the overall population. However, the responses from Estonia were rather scarce, only 15 respondents, so it is hard to draw conclusions from such a small sample size.

The ‘age’ demographic faces similar difficulties when assessing the results, as most of the respondents were 18-31 years old. This age group totaled 71% of the respondents. In all age groups, at least one or more GDPR principle were rated as the most important attribute, above the TAM elements. It is perhaps notable that in the senior age group (61-70 years old) had rated the ‘ease of use’ attribute relatively high compared to other age groups. In the senior group ‘ease of use’ reached a utility scoring of 10,16 whereas it only reached 6,85 scoring in the overall population. To conclude the demographical section the ‘education’ demographic was also strongly focused on two demographic groups, ‘bachelor’s degree’ and ‘master’s degree’ constituted 83% of the respondents. These two groups follow closely to the overall population’s preferences and as they are quite similar groups, both academic but on different levels, it is difficult to draw conclusions if education affects these preferences as I would have needed more non-academic respondents.

Next, I am going to conclude the relation between security and privacy concerns as well as GDPR familiarity and attitudes towards data collection. Let us first assess the privacy and security issues in data collection. Unsurprisingly, the respondents that said to be ‘not at all concerned’ of the privacy and security issues of the data collector rated TAM elements higher than GDPR attributes. In these groups, all the TAM elements surpass the GDPR attributes in terms of utility scoring. Interestingly, even though GDPR attributes were below the TAM elements in this group, ‘integrity and confidentiality’ was still the highest rated GDPR element in these groups as well. All the other respondent groups rated the GDPR attributes above the TAM elements however, and generally follow the overall distribution of preferences, even those who said to be ‘not too concerned’.

Interestingly, the respondents that were ‘not at all familiar’ with the GDPR rated TAM elements as their top priority, whereas in other groups the GDPR attributes were seen as top priority. So, the GDPR attributes were seen as the most important element even in the group which was ‘not too familiar’ with the GDPR, only those who were not at all familiar rated TAM elements as their top priority. To conclude, it seems like the subgroups followed the overall distribution rather closely with some exceptions. For example, in the last section where GDPR familiarity and concerns are assessed, those with more careless attitudes towards these issues rated TAM elements above GDPR elements, but the general attitude seems to favor GDPR attributes above TAM elements.

6.1 Limitations and suggestions for future research

Finally, I am addressing the limitations of my thesis and some suggestions for future research. The main limitation for my thesis is the rather small sample size of my survey. Especially the number of Estonian respondents (only 18) does not give coherent implication of the population as a whole. My first suggestion would be that if there should be a similar survey of citizens' attitudes towards privacy issues in digital services, the sample size of the respondents should be higher to achieve a broader perspective on these issues.

Another limitation is that although I gained a comprehensive list of preferences between the GDPR principles and TAM elements, I do not know how important the citizens view these attributes compared to other basic needs. I would thus suggest that these attributes would be valued against some other attributes not related to data security and privacy or user experience of digital services, but rather to some other activities and even basic needs. This would allow us to perceive how important these attributes are overall, not just the relative importance of the attributes with each other.

Finally, as my survey only had one hypothetical situation of data collection (the city bike example) it does not take into consideration the situational importance of each attribute. For example, if the city bike example would be replaced with some healthcare application that possible prevents serious diseases, would the importance of these attributes shift?

References

Agrawal, D., Kettinger, W., & Zhang, C. (2014). The Openness Challenge: Why Some Cities Take It On and Others Don't. Proceedings of the 20th Americas Conference on Information Systems (AMCIS), Savannah.

Almirall, E. and Wareham, J., 2008. Living labs and open innovation: Roles and applicability. *eJOV: The Electronic Journal for Virtual Organization & Networks*, *10*.

Angelidou, M., 2014. Smart city policies: A spatial approach. *Cities*, *41*, pp. S3-S11.

Anthopoulos, L., 2015, August. Defining smart city architecture for sustainability. In *proceedings of 14th electronic government and 7th electronic participation conference (IFIP2015)* (pp. 140-147).

Anttiroiko A-V (2012) The role of new technologies in reshaping governance platforms. Int J Inf Commun Technol Hum Dev 4(3):1–13

Anttiroiko, A.V., Valkama, P. and Bailey, S.J., 2014. Smart cities in the new service economy: building platforms for smart services. *AI & society*, *29*(3), pp.323-334.

Bakici, T., Almirall, E., Wareham, J. (2013), A smart city initiative: The case of Barcelona. Journal of Knowledge Economy, 4(2), 135-148.

Balakrishna, C., 2012, September. Enabling technologies for smart city services and applications. In *2012 sixth international conference on next generation mobile applications, services and technologies* (pp. 223-227). IEEE.

Belanche-Gracia, D., Casaló-Ariño, L.V. and Pérez-Rueda, A., 2015. Determinants of multi-service smartcard success for smart cities development: A study based on citizens' privacy and security perceptions. *Government information quarterly*, *32*(2), pp.154-163.

Benevolo, C., Dameri, R.P. and D'auria, B., 2016. Smart mobility in smart city. In *Empowering organizations* (pp. 13-28). Springer, Cham.

Bessant J, Tidd J (2007) Innovation and entrepreneurship. Wiley, Chichester

Bleier, A., Goldfarb, A., Tucker C. (2020). Consumer Privacy and the Future of Data-Based Innovation and Marketing. International Journal of Research in Marketing, 4/2020.

Bonina, C.M., 2013. New business models and the value of open data: definitions, challenges and opportunities. *NEMODE–3K Small Grants Call*.

Bruneckiene, J., Sinkiene, J. (2014), Critical Analysis of Approaches to Smart Economy. 8 International Scientific Conference "Business and Management 2014" May 15-16, 2014, Vilnius, LITHUANIA. Section: Smart Development.

Buera, F.J. and Kaboski, J.P., 2012. The rise of the service economy. *American Economic Review*, *102*(6), pp.2540-69.

Bu-Pasha, S., 2017. Cross-border issues under EU data protection law with regards to personal data protection. *Information & Communications Technology Law*, *26*(3), pp.213-228.

Burange, A.W. and Misalkar, H.D., 2015, March. Review of Internet of Things in development of smart cities with data management & privacy. In *2015 International Conference on Advances in Computer Engineering and Applications* (pp. 189-195). IEEE.

Caragliu A., De Bo C., Nijcamp P. (2009), "Smart city in Europe", 3rd Central European Conference in Regional Science.

Carillo FJ (ed) (2006) Knowledge cities. Approaches, experiences, and perspectives. Elsevier, Amsterdam

Carlsen, L.H., 2014. *The Location of Privacy-A Case Study of Copenhagen Connecting's Smart City* (Doctoral dissertation, Master Thesis, Roskilde University Communication Studies, Roskilde).

Castro, D., Atkinson, R.D. and Ezell, S.J., 2010. Embracing the self-service economy. *Available at SSRN 1590982*.

Cilliers, L. and Flowerday, S., 2014. Information privacy concerns in a participatory crowdsourcing smart city project. *Journal of Internet Technology and Secured Transactions*, *3*(3), pp.208-87.

Crump C, Harwood M. 2014 Invasion of the data snatchers: big data and the internet of things means the surveillance of everything. ACLU, 25 March 2014.

Dais A, Nikolaidou M, Alexopoulou N, Anagnostopoulous D (2008) Introducing a public agency networking platform towards supporting connected governance. In: Wimmer MA, Scholl HJ, Ferro E (eds) EGOV 2008. LNCS 5184. Springer-Verlag, Berlin, pp 375–387

Dameri R.P. (2012), "Defining an evaluation framework for digital cities implementation", IEEE International Conference on Information Society (i-Society).

Dameri, R.P. and Cocchia, A., 2013, December. Smart city and digital city: twenty years of terminology evolution. In *X Conference of the Italian Chapter of AIS, ITAIS* (pp. 1-8).

de Man A-P (2004) The network economy. Strategy, structure and management. Edward Elgar, Cheltenham

Eckhoff, D. and Wagner, I., 2017. Privacy in the smart city—applications, technologies, challenges, and solutions. *IEEE Communications Surveys & Tutorials*, *20*(1), pp.489-516.

Edwards, L., 2016. Privacy, security and data protection in smart cities: A critical EU law perspective. *Eur. Data Prot. L. Rev.*, *2*, p.28.

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

Elwood S, Leszczynski A. 2011 Privacy reconsidered: new representations, data practices, and the geoweb. Geoforum 42, 6–15.

Eriksson-Zetterquist U, Mu¨llern T, Styhre A (2011) Organisation theory. A practice-based approach. Oxford University Press, Oxford

Fagnant, D.J. and Kockelman, K.M., 2014. The travel and environmental implications of shared autonomous vehicles, using agent-based model scenarios. *Transportation Research Part C: Emerging Technologies*, *40*, pp.1-13.

Furubotn EG, Richter R (2005) Institutions & economic theory. The contribution of the new institutional economics. Economics, cognition and society, 2nd edn. The University of Michigan Press, Ann Arbor

Gallaher MP, Link AN, Petrusa JE (2006) Innovation in the US service sector. Routledge, Abingdon

Garvin DA (1993) Building a learning organization. Harv Bus Rev 71(4):78–91

Giffinger R. (2007), Smart Cities: Ranking of European medium-sized cities, Centre of Regional Science, Vienna.

Gonzalez-Zapata, F., & Heeks, R. (2015). The multiple meanings of open government data: understanding different stakeholders and their perspectives. Government Information Quarterly.

Gretzel, U., Sigala, M., Xiang, Z. and Koo, C., 2015. Smart tourism: foundations and developments. *Electronic Markets*, *25*(3), pp.179-188.

Hall P. (2000), "Creative cities and economic development", Urban Studies, Volume 37, Issue 4, pp. 633-649.

Helbig, N., Gil-García, J. R., & Ferro, E. (2009). Understanding the complexity of electronic government: implications from the digital divide literature. Government Information Quarterly, 26(1), 89–97.

Hielkema, H. and Hongisto, P., 2013. Developing the Helsinki smart city: The role of competitions for open data applications. *Journal of the Knowledge Economy*, *4*(2), pp.190-204.

Hoffman, D. L., & Novak, T. P. (2018). Consumer and object experience in the internet of things: An assemblage theory approach. Journal of Consumer Research, 44(6), 1178–1204.

Hollands, R. G. (2008). Will the Real Smart City Please Stand Up?: Intelligent, Progressive or Entrepreneurial? 12/2008.

Irani, Z., Love, P., & Montazemi, A. (2007). E-government: past, present and future. European Journal of Information Systems, 16(2), 103.

Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2012). Benefits, adoption barriers and myths of open data and open government. Information Systems Management, 29(4), 258–268

Jo, H.C., Kim, S. and Joo, S.K., 2013. Smart heating and air conditioning scheduling method incorporating customer convenience for home energy management system. *IEEE transactions on consumer electronics*, *59*(2), pp.316-322.

Jorgenson DW, Wessner CW (2007) Measuring and sustaining the new economy. enhancing productivity growth in the information age. National Research Council of National Academies. The National Academic Press, Washington

Karimi, M. and Niknami, S., 2011. Self-efficacy and perceived benefits/barriers on the AIDS preventive behaviors. *Journal of Kermanshah University of Medical Sciences*, *15*(5), pp.384-92.

Kastner, W., Neugschwandtner, G., Soucek, S. and Newman, H.M., 2005. Communication systems for building automation and control. *Proceedings of the IEEE*, *93*(6), pp.1178-1203.

Katzy, B. and Klein, S., 2008. Editorial introduction: special issue on living labs. *The Electronic Journal for Virtual Organizations and Networks*, *10*(1), pp.2-6.

Kelli, A., Lindén, K., Vider, K., Kamocki, P., Birštonas, R., Calamai, S., Labropoulou, P., Gavriilidou, M. and Stranák, P., 2019, May. Processing personal data without the consent of the data subject for the development and use of language resources. In *Selected papers from the CLARIN Annual Conference 2018, Pisa, 8-10 October 2018*. Linköping University Electronic Press.

Kushida KE, Zysman J (2009) The services transformation and network policy: the new logic of value creation. Rev Policy Res 26:173–194

Kyriazis, D., Varvarigou, T., White, D., Rossi, A. and Cooper, J., 2013, June. Sustainable smart city IoT applications: Heat and electricity management & Eco-conscious cruise control for public transportation. In *2013 IEEE 14th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)* (pp. 1-5). IEEE.

Lopez de Avila, A. (2015). Smart Destinations: XXI Century Tourism. Presented at the ENTER2015 Conference on Information and Communication Technologies in Tourism, Lugano, Switzerland, February 4-6, 2015.

Louviere, J.J., Flynn, T.N. and Marley, A.A.J., 2015. *Best-worst scaling: Theory, methods and applications*. Cambridge University Press.

Lynch, J.P. and Loh, K.J., 2006. A summary review of wireless sensors and sensor networks for structural health monitoring. *Shock and Vibration Digest*, *38*(2), pp.91-130.

Martin, T., Jovanov, E. and Raskovic, D., 2000, October. Issues in wearable computing for medical monitoring applications: a case study of a wearable ECG monitoring device. In *Digest of Papers. Fourth International Symposium on Wearable Computers* (pp. 43-49). IEEE.

Nuortio, T., Kytöjoki, J., Niska, H. and Bräysy, O., 2006. Improved route planning and scheduling of waste collection and transport. *Expert systems with applications*, *30*(2), pp.223-232.

Paton RA, McLaughlin SA (2008) Service innovation: knowledge transfer and the supply chain. Eur Manag J 26:77–83

Pereira, G.V., Macadar, M.A., Luciano, E.M. and Testa, M.G., 2017. Delivering public value through open government data initiatives in a Smart City context. *Information Systems Frontiers*, *19*(2), pp.213-229.

Perera, H., Hussain, W., Mougouei, D., Shams, R.A., Nurwidyantoro, A. and Whittle, J., 2019, September. Towards integrating human values into software: Mapping principles and rights of gdpr to values. In *2019 IEEE 27th International Requirements Engineering Conference (RE)* (pp. 404-409). IEEE.

Phan, R.W. and Mohammed, L.A., 2003, September. On the security & design of MyKad. In *9th Asia-Pacific Conference on Communications (IEEE Cat. No. 03EX732)* (Vol. 2, pp. 721-724). IEEE.

Porter, M. E., & Heppelmann, J. E. (2014). How smart, connected products are transforming competition. Harvard Business Review, 92(11), 64–88.

Rial, A. and Danezis, G., 2011, October. Privacy-preserving smart metering. In *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society* (pp. 49-60).

Roca, J.C., Chiu, C.M. and Martínez, F.J., 2006. Understanding e-learning continuance intention: An extension of the Technology Acceptance Model. *International Journal of human-computer studies*, *64*(8), pp.683-696.

Rose, K., Eldridge, S. and Chapin, L., 2015. The internet of things: An overview. *The Internet Society (ISOC)*, *80*, pp.1-50.

Rubinstein IS. 2013 Big data: the end of privacy or a new beginning? Int. Data Privacy Law 3, 74–87.

Rutherford D (2002) Routledge dictionary of economics, 2nd edn. Routledge, London

Schaffers, H., Cordoba, M.G., Hongisto, P., Kallai, T., Merz, C. and Van Rensburg, J., 2007, June. Exploring business models for open innovation in rural living labs. In *2007 IEEE International Technology Management Conference (ICE)* (pp. 1-8). IEEE.

Schwartz, S.H., 2012. An overview of the Schwartz theory of basic values. *Online readings in Psychology and Culture*, *2*(1), pp.2307-0919.

Soe, R.-M. (2017). FINEST Twins: platform for cross-border smart city solutions. *dg.o '17: Proceedings of the 18th Annual International Conference on Digital Government Research.* Ed. Hinnant, C. C.; Ojo, A. ACM, 352−357.

Solove D. 2006 A taxonomy of privacy. Univ. Penn. Law Rev. 154, 477–560.

Solove D. 2013 Privacy management and the consent dilemma. Harvard Law Rev. 126, 1880– 1903.

Su K., Li J., Fu H. (2011), "Smart City and the applications", IEEE International Conference on Electronics, Communications and Control (ICECC), pp. 1028-1031.

Takabi, H., Joshi, J.B. and Ahn, G.J., 2010. Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, *8*(6), pp.24-31.

Tien JM (2007) Services innovation: decision attributes, innovation enablers, and innovation drives. In: Hsu C (ed) Service enterprise integration. An enterprise engineering perspective. Springer, New York, pp 39–76

UN (2011) The state of world population 2011. United Nations Population Fund (UNFPA), New York

Vargo SL, Maglio PP, Akaka MA (2008) On value and value cocreation: a service systems and service logic perspective. Eur Manag J 26:145–152

Venkatesh, V., 2000. Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information systems research*, *11*(4), pp.342-365.

Washburn, D., Sindhu, U., Balaouras, S., Dines, R.A., Hayes, N. and Nelson, L.E., 2009. Helping CIOs understand "smart city" initiatives. *Growth*, *17*(2), pp.1-17.

Webster, J. and Watson, R.T., 2002. Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, pp.xiii-xxiii.

Woods, E., Alexander, D., Labastida, R. and Watson, R., 2016. *UK Smart Cities Index, Assessment of Strategy and Execution for 10 Cities*. Technical Report.

Wölfl, A., 2005. *The service economy in OECD countries* (pp. 27-63). Paris: OECD.

Xue, Q., 2010. Smart Healthcare: Applications of the Internet of Things in Medical Treatment and Health. *Information Construction*, *5*, pp.56-58.

Yeh, H., 2017. The effects of successful ICT-based smart city services: From citizens' perspectives. *Government Information Quarterly*, *34*(3), pp.556-565.

Zanella, A., Bui, N., Castellani, A., Vangelista, L. and Zorzi, M., 2014. Internet of things for smart cities. *IEEE Internet of Things journal*, *1*(1), pp.22-32.

Zang J, Dummit K, Graves J, Lisker P, Sweeney L. 2015 Who knows what about me? A survey of behind the scenes personal data sharing to third parties by mobile apps. Technology Science, 30 October 2015.

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J. and Shen, X.S., 2017. Security and privacy in smart city applications: Challenges and solutions. *IEEE Communications Magazine*, *55*(1), pp.122-129.

Zysman J (2004) Finland in a digital era: how do wealthy nations stay wealthy? Prime Minister's Office: Publications 25/2004. Edita, Helsinki

Interviews

Name of the interviewee, job, company, place and time

Raivio Riku, Director, Company XYZ, Espoo, 12.10.2001.

Internet-references

Article 29 Data Protection Working Party. 2014 Opinion 8/2014 on the recent developments on the internet of things. See http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

Befriending UK´s official web-page (2020), https://www.befriending.co.uk/about/what-is-befriending/

https://www.dataguidance.com/notes/estonia-national-gdpr-implementation-overview (accessed 3.9.2020)

EMT Madrid (2020), https://www.emtmadrid.es/Home?lang=es-ES

Energyhive platform (2020), http://www.energyhive.com

European Commission´s official web-page (2020), https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market#:~:text=A%20Digital%20Single%20Market%20(DSM,personal%20data%20protection%2C%20irrespective%20of

General Data Protection Regulation (GDPR). 2018. *General Data Protection Regulation (GDPR)*. [online] Available at: <https://gdpr-info.eu/> [Accessed 13 May 2021].

European Data Protection Supervisor, (2014). Privacy and competitiveness in the age of big data: the interplay between data protection, competition law and consumer protection in the digital economy. See http://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf

Forum Virium (2020), https://forumvirium.fi/projektit/

Open definition website (2020):
https://opendefinition.org/

Setis-Eu (2012), setis.ec.europa.eu/implementation/technology-roadmap/

Sporat Kartalla (2020), www.sporat.fi

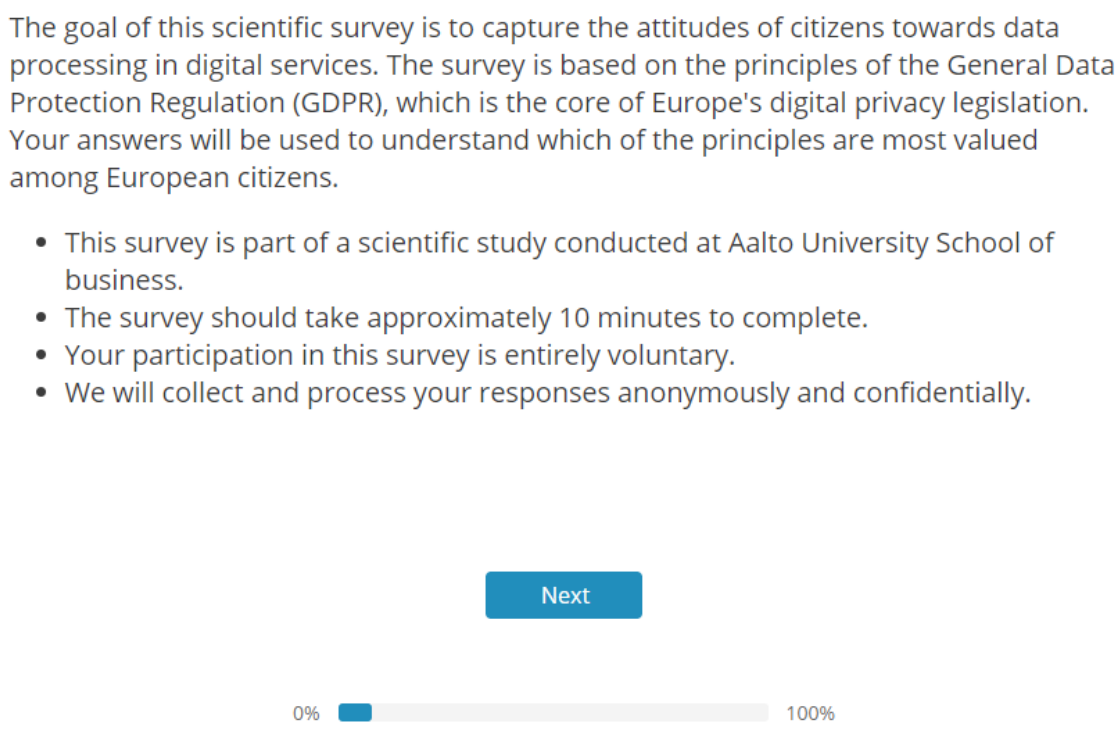
https://tietosuoja.fi/en/consent-of-the-data-subject

Appendix

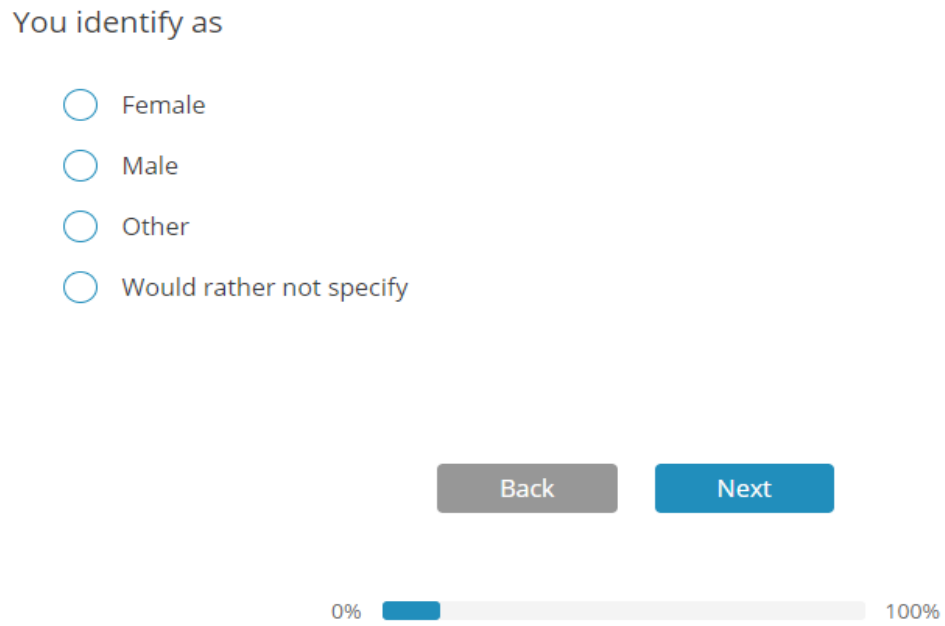
Appendix a. Privacy and security concern distribution

Value	Label	Total	Question: PrivacyConcern					Question: SecurityConcern				
			1 Not at all concerned	2 Not too concerned	3 Neutral	4 Concerned	5 Extremely concerned	1 Not at all concerned	2 Not too concerned	3 Neutral	4 Concerned	5 Extremely concerned
1	Not at all familiar	6 5.3%	1 16.7%	2 5.9%		2 5.4%	1 14.3%	1 20.0%	1 3.4%	2 5.9%	2 5.4%	
2	Not too familiar	21 18.4%	1 16.7%	9 26.5%	7 23.3%	3 8.1%	1 14.3%	1 20.0%	9 31.0%	6 17.6%	3 8.1%	2 22.2%
3	Somewhat familiar	40 35.1%	1 16.7%	11 32.4%	8 26.7%	19 51.4%	1 14.3%	1 20.0%	7 24.1%	13 38.2%	18 48.6%	1 11.1%
4	Familiar	28 24.6%	3 50.0%	9 26.5%	10 33.3%	5 13.5%	1 14.3%	2 40.0%	10 34.5%	8 23.5%	5 13.5%	3 33.3%
5	Very familiar	19 16.7%		3 8.8%	5 16.7%	8 21.6%	3 42.9%		2 6.9%	5 14.7%	9 24.3%	3 33.3%
	Summary:	N: 114 Min: 1 Max: 5 Mean: 3.29	N: 6 Min: 1 Max: 4 Mean: 3.00	N: 34 Min: 1 Max: 5 Mean: 3.06	N: 30 Min: 2 Max: 5 Mean: 3.43	N: 37 Min: 1 Max: 5 Mean: 3.38	N: 7 Min: 1 Max: 5 Mean: 3.57	N: 5 Min: 1 Max: 4 Mean: 2.80	N: 29 Min: 1 Max: 5 Mean: 3.10	N: 34 Min: 1 Max: 5 Mean: 3.24	N: 37 Min: 1 Max: 5 Mean: 3.43	N: 9 Min: 2 Max: 5 Mean: 3.78

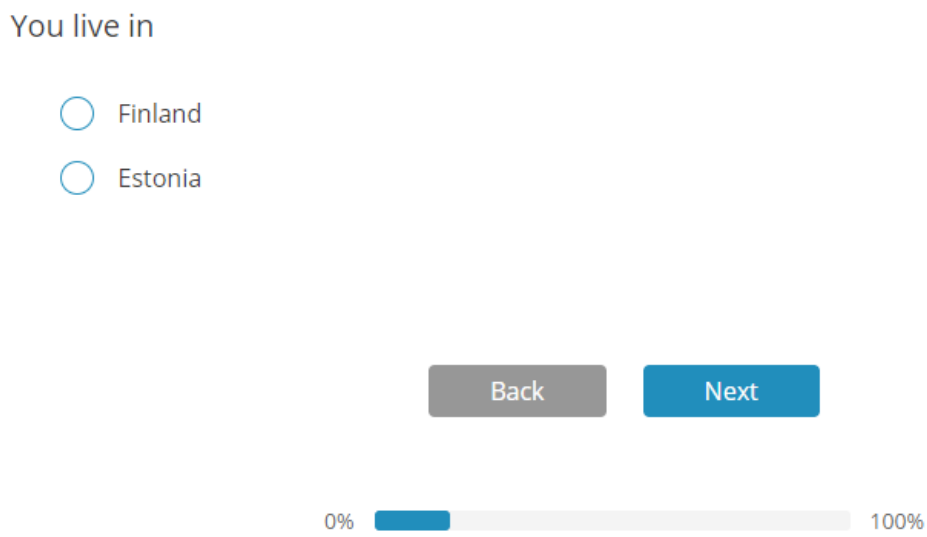
Appendix b. Survey of citizens' attitudes towards data processing



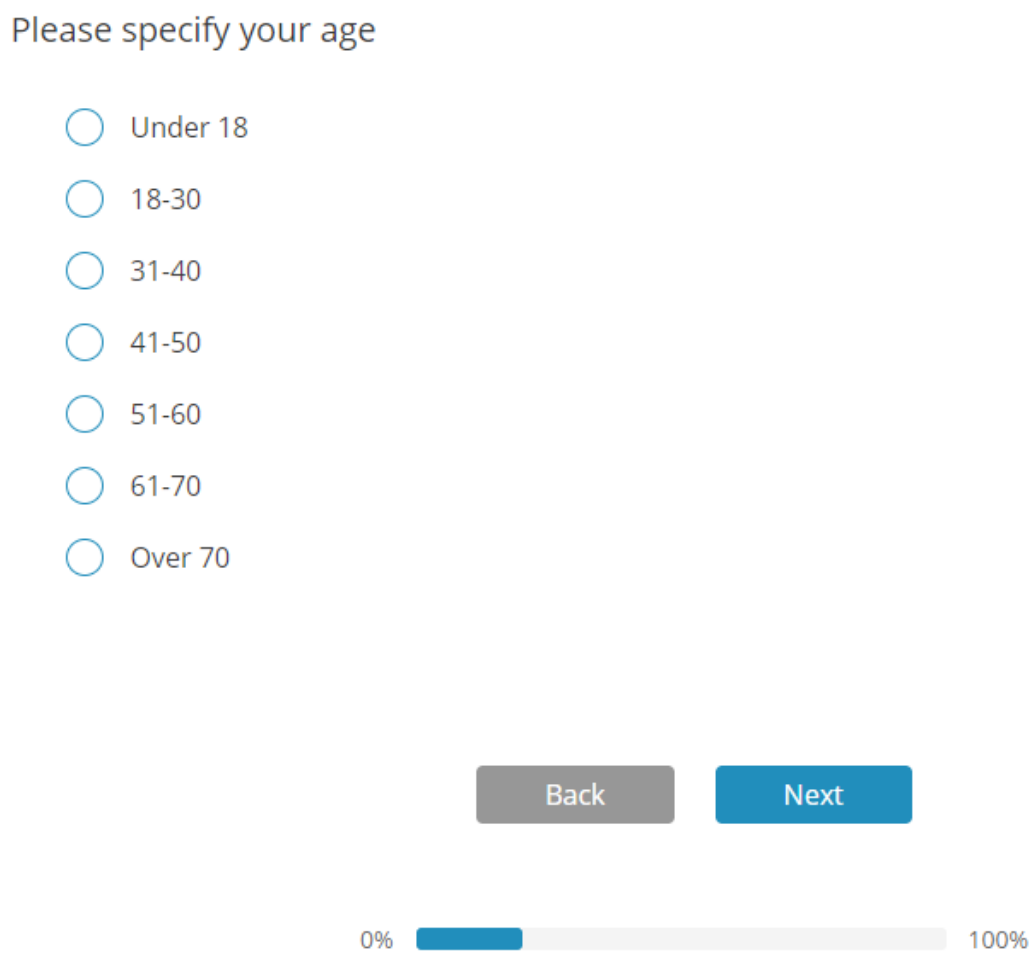
In the next page the respondent is asked to state their gender.



The next demographic question regards the respondent's location, whether its Finland or Estonia.



The third demographic question is about age.



I also wanted to know if the respondent's educational background affected their preferences. This was the last question concerning respondent demographics.

What is the highest level or degree of education you have completed?

- ◯ Primary school
- ◯ Vocational school
- ◯ High school
- ◯ Bachelor's degree
- ◯ Master's degree
- ◯ Doctoral degree

Back Next

0% 100%

How often do you use the following digital applications or services? We provide some examples in the parenthesis but other applications of the same category count as well.

	Daily	5-6 times per week	3-4 times per week	1-2 times per week	Less than once per week
Social media (Facebook, Instagram, Tiktok)	○	○	○	○	○
Journey planner or online tracking for commute transport (Reittiopas, Sõiduplaanid, Sporat.fi)	○	○	○	○	○
City bikes or scooters (Alepa bike, Tier, Voi)	○	○	○	○	○
Ride hailing applications (Uber, Yango, Lyft)	○	○	○	○	○
Food delivery applications (Wolt, Foodora, ResQ)	○	○	○	○	○
Mobile banking (Mobilepay, Nordea mobile)	○	○	○	○	○
Conference call apps (Zoom, Skype, Discord)	○	○	○	○	○
Streaming services (Netflix, Twitch)	○	○	○	○	○
Smart car parks (EasyPark, eParking.fi, ParkMan)	○	○	○	○	○

How concerned are you about the collection and use of your data by these services?

- ◯ Not at all concerned
- ◯ Not too concerned
- ◯ Neutral
- ◯ Concerned
- ◯ Extremely concerned

Back Next

0% 100%

How concerned are you about the security of these services?

- ◯ Not at all concerned
- ◯ Not too concerned
- ◯ Neutral
- ◯ Concerned
- ◯ Extremely concerned

Back Next

0% 100%

All the digital services we use collect different kinds of information about us. Therefore, it is crucial to have a regulatory body that protects our privacy and sets rules for the processing of the information collected. General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union. The regulation is based on the following seven essential principles of data protection.

1. *Lawfulness, fairness and transparency.* Personal data shall be processed lawfully, fairly and in transparent manner in relation to the data subject.
2. *Purpose limitation.* Data shall be collected for specified, explicit and legitimate purposes and not further processed.
3. *Data minimization.* Data shall be adequate and limited to what is necessary for the processing.
4. *Accuracy.* Data shall be accurate and up to date.
5. *Storage limitation.* Data shall be kept in form which permits identification of data subjects for no longer than is necessary for the processing.
6. *Integrity and confidentiality (security).* Appropriate security measures are used when processing the data.
7. *Accountability.* The data controller shall be responsible for, and be able to demonstrate compliance with these principles.

How familiar are you with the GDPR and its principles?

- ◯ Not at all familiar
- ◯ Not too familiar
- ◯ Somewhat familiar
- ◯ Familiar
- ◯ Very familiar

Next, we would like to ask you about your opinion about how your data are collected and processed by a digital applications and services. You are presented with a scenario multiple times. Each time you should select the data protection principle, which is the most important to you as well as the least important to you relating to that scenario.

Please note that "your data" refers to all the personal data (e.g. name, age and home address) about you that is being collected and processed by the service provider.

Back Next

0% 100%

Imagine that the City of Helsinki and City of Tallinn launch a new cross-border journey planner application, which can be used within either of these cities or while travelling between the cities. This mobile application uses your data (e.g. location, name, date of birth, national security number, phone number, and address) to recommend you the best mode of transportation (e.g. public transport, city bikes, taxi) and the best route (e.g. shortest, cheapest, fastest). The application also enables you to buy tickets or pay for your journey on a figure tip.

Which of the following characteristics would be the most important and the least important to you?

1 / 12

The most important	Characteristic	The least important
○	Your data is processed with appropriate security measures	○
○	The service provider will be sanctioned for mishandling your data	○
○	The journey planner application would be easy and effortless to use	○

Back Next

0% 100%

2 / 12

The most important	Characteristic	The least important
○	You would save transportation time by using the journey planner application	○
○	Your data is used only for the purposes you agreed on	○
○	You could use the journey planner application successfully and efficiently	○

3 / 12

The most important	Characteristic	The least important
○	Your data is correct and accurate	○
○	Your data is processed lawfully, fairly and in a transparent manner	○
○	Only relevant data about you is being collected	○

4 / 12

The most important	Characteristic	The least important
○	The journey planner application would be useful and improve your transportation	○
○	Your data is deleted from the database after processing	○
○	You would save transportation costs by using the journey planner application	○

5 / 12

The most important	Characteristic	The least important
○	Your data is correct and accurate	○
○	You would save transportation time by using the journey planner application	○
○	Your data is processed with appropriate security measures	○

6 / 12

The most important	Characteristic	The least important
○	The journey planner application would be easy and effortless to use	○
○	You would save transportation costs by using the journey planner application	○
○	Your data is processed lawfully, fairly and in a transparent manner	○

7 / 12

The most important	Characteristic	The least important
◯	You could use the journey planner application successfully and efficiently	◯
◯	Only relevant data about you is being collected	◯
◯	Your data is deleted from the database after processing	◯

8 / 12

The most important	Characteristic	The least important
◯	Your data is used only for the purposes you agreed on	◯
◯	The journey planner application would be useful and improve your transportation	◯
◯	The service provider will be sanctioned for mishandling your data	◯

9 / 12

The most important	Characteristic	The least important
◯	The service provider will be sanctioned for mishandling your data	◯
◯	You could use the journey planner application successfully and efficiently	◯
◯	Your data is correct and accurate	◯

10 / 12

The most important	Characteristic	The least important
◯	Your data is processed lawfully, fairly and in a transparent manner	◯
◯	Your data is processed with appropriate security measures	◯
◯	The journey planner application would be useful and improve your transportation	◯

11 / 12

The most important	Characteristic	The least important
○	Only relevant data about you is being collected	○
○	You would save transportation costs by using the journey planner application	○
○	Your data is used only for the purposes you agreed on	○

12 / 12

The most important	Characteristic	The least important
○	Your data is deleted from the database after processing	○
○	The journey planner application would be easy and effortless to use	○
○	You would save transportation time by using the journey planner application	○

The survey is complete. Thank you for participation!