TALLINN UNIVERISTY OF TECHNOLOGY
School of Business and Governance
Department of Law

Elsa-Maria Tropp

OPEN DATA: A STEPCHILD IN E-ESTONIA'S DATA MANAGEMENT STRATEGY?

Master's thesis
Law, Law and Technology

Supervisor: Thomas Hoffmann, PhD
Co-supervisor: Archil Chocia, PhD

Tallinn 2022

I declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is 7558 words from the introduction to the end of summary.

Elsa-Maria Tropp ……
(signature, date)
Student code: 212122HAJM
Student e-mail address: eltrop@taltech.ee

Supervisor: Thomas Hoffmann, PhD:
The paper conforms to requirements in force

……
(signature, date)

Co-supervisor: Archil Chocia, Phd:
The paper conforms to requirements in force
……
(signature, date)

Chairman of the Defence Committee:
Permitted to the defence
……
(name, signature, date)

ABSTRACT

The European Convention on Human Rights implies in its Article 10 that the state has an obligation to guarantee the right to seek or obtain information. This approach was confirmed already in 1982 by the Committee of Ministers' Declaration on the Freedom of Expression and Information and is regulated on the EU level by Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public sector information. The European Commission considered that action at Union level was necessary to address barriers to a wide reuse of public sector and publicly funded information across the Union, to bring the legislative framework up to date with the advances in digital technologies and to further stimulate digital innovation. However, the availability of open data has increased dramatically both domestically and EU-wide. This paper analyses the importance of open data, the problem of the lack of open data policies, provide an overview of existing systems used by the governance of Estonia to ensure access to open information, and make proposals on how to improve open data disclosure practices in Estonia.

Qualitative research methods are used to write this paper. Secondary data will be used through literature reviews and articles composed by other authors.

Keywords: access to information, data protection, Estonia, GDPR, open data, open data policies

INTRODUCTION

Following master thesis is formatted as an article. This article has been pubilshed in the TalTech Journal of European Studies (ISSN 2228-0596) in May 2022. The article is published in co-authorship of the master student Elsa-Maria Tropp and supervisors Dr. Thomas Hoffmann and Dr. Archil Chochia. The master student is the first author and conducted the main part of the research guided by supervisors.

The European Convention on Human Rights implies in its article 10 that the state has an obligation to guarantee the right to seek or obtain information. This approach was confirmed already in 1982 by the Committee of Ministers' Declaration on the Freedom of Expression and Information and finally regulated on the EU level by Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public sector information. The European Commission considered that action at Union level was necessary to address the remaining and emerging barriers to a wide reuse of public sector and publicly funded information across the Union, to bring the legislative framework up to date with the advances in digital technologies and to further stimulate digital innovation.

However, the current usage of open data published by the governments is falling behind expectations. Datasets are being released on different platforms with the assumption that these datasets are meant to be used for any purpose and the users will benefit from them regardless of their intentions. This assumption may impair the reuse of open data, as there might not be a connection between context-specific user and data provision. States do not have a clear strategy about what should be published and how it should be published. There are currently a variety of open data policies and regulations at various levels of government, but little to no systematic and structured study has been conducted on the issues covered by open data policies, their goal, and their actual impact. Most research in this area has consisted of conceptual papers, descriptions of the empirical uses of open data or the design of technology and systems for harnessing the power of open data.

The aim to be achieved with the article is to contributie to fill earlier mentioned problem. This article identifies the significance of open data and the resulting challenges imposed by the widespread lack of specific open data policies. The artcile also provides an explanation of the existing systems used in Estonian governance to ensure access to open information, but also highlights the shortcomings, before it finally makes proposals on how to improve open data disclosure practices in Estonia.

The hypothesis for this article is that governments need to disclose via platforms its open data to ensure its transparency to its citizens.

In this article, document analysis is used as a method of collecting qualitative data. Secondary data will be used through literature reviews and articles composed by other authors.

This article consists of four main chapters and in addition a chapter with proposals. First chapter explains the importance of open data policies. The main importance of open data is the fact that it helps to ensure the long-term transparency of government information.

The second chapter will introduce different legislations that obliges Estonian governemnt to publish collected open data are introduced. This obligation derives from Directive 2019/1024 of the European Parliament and of the Council on open data and the reuse of public sector information. On national level, Estonia has established an explicit constitutional right to full transparency about the use of personal and public right (Article 44 of Estonian Constitution). In addition, the Amendment Act of Estonian Public Information Act entered into force on 10 December 2021 and had the objective to bring the Estonian Public Information Act in line with Directive 2019/1024 on open data. The new Estonian Public Information Act intends to solve practical bottlenecks that have arisen in the interpretation of the definition of open data and the principles related to reuse provided in the earlier law.

The third chapter will give an overview of different data platform tools that are used in Estonia – x-road, eesti.ee portal, avaandmed.eesti.ee and riigiteataja.ee. In addition, overview of how once-only principle is used in Estonia is given. This chapter has multiple subsections, each one is dedicated to earlier menntioned platform or principle.

The fourth chapter explains relationship between open data and personal data protection (GDPR). Open data policies may not be in conflict with the individual's right to privacy protected by GDPR. When disclosing open data, the authority must be 100% sure that the data disclosed are in no way personal data or that they can be linked in any way to a specific person, as this would constitute an infringement that could result in a fine of up to 20 million euros

In the last chapter, three proposals are made based on the analysis and case studies to further improve open data accessibility:

Open Data: A Stepchild in e-Estonia's Data Management Strategy?

Elsa-Maria Tropp
Thomas Hoffmann
Archil Chochia

Department of Law
Tallinn University of Technology
Ehitajate tee 5
Tallinn 19086, Estonia
Email: eltrop@taltech.ee
Email: thomas.hoffmann@taltech.ee
Email: archil.chochia@taltech.ee

Abstract: The availability of open data has increased dramatically, partly in reaction to several types of government agencies publishing their raw data. Access to and use of open data is not only essential for the development of public policy and delivery of various services, but it is also of eminent value for private (and often economic) purposes. To meet these demands, the availability of open data has increased dramatically both domestically and EU-wide. Nevertheless, it is still access to and use of personal data which is usually in the spotlight of public—and also legal—debates. Contributing to fill this gap, this paper analyses the significance of open data and the resulting challenges imposed by the widespread lack of specific open data policies. The paper also provides an overview of the existing systems used in Estonian governance to ensure access to open information, but also highlights the shortcomings, before it finally makes proposals on how to improve open data disclosure practices in Estonia.

Keywords: *access to information, data protection, Estonia, GDPR, open data, open data policies*

1. Introduction

The European Convention on Human Rights implies in its Article 10 that the state has an obligation to guarantee the right to seek or obtain information. This approach was confirmed already in 1982 by the Committee of Ministers' Declaration on the Freedom of Expression and Information and finally regulated on the EU level by Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public sector information. The European Commission considered that action at Union level was necessary to address the remaining and emerging barriers to a wide reuse of public sector and publicly funded information across the Union, to bring the legislative framework up to date with the advances in digital technologies and to further stimulate digital innovation.

The availability of open data has increased dramatically, with pressure being put on several types of government agencies to publish their raw data. Open data is frequently required for the development of public policy and the delivery of services, but it can also be useful for other purposes, such as traffic statistics. The traditional separation between public entities and users is overcome through open data (Janssen, Charalabidis & Zuiderwijk, 2012, p. 258). In many different domains, public agencies are among the major creators and collectors of data. These data categories include anything from traffic, environmental, geographical, and tourism information to statistics, business, public sector budgets, and performance levels, as well as policy and inspection data (food, safety, education quality, etc.).

Open data may be used to establish public policy (Napoli & Karaganis, 2010, p. 385) as well as to gain insight into and provide solutions to social issues (Janssen, 2011, p. 45). Open data—i.e., non-personal data generated by public entities—should be opened for all to reuse, free of charge, and without discrimination concern all data which (when published) does not violate the fundamental rights of individuals. Even though states must publish open data, not much of it is being published. The current usage of open data published by the governments is falling behind expectations. Datasets are being released on different platforms with the assumption that these datasets are meant to be used for any purpose and the users will benefit from them regardless of their intentions (Janssen, 2011, p. 45). This assumption may impair the reuse of open data, as there might not be a connection between context-specific user requirements and data provision (Ruijer *et al.*, 2017, p. 471). States do not have a clear strategy about what should be published and how it should be published. There are currently a variety of open data policies and regulations at various levels of government, but little to no systematic and structured study has been conducted

on the issues covered by open data policies, their goal, and their actual impact (see, e.g., Nyman-Metcalf & Papageorgiou, 2018; Hamuľák, Kocharyan & Kerikmäe, 2020; Kerikmäe & Nyman-Metcalf, 2020a; 2020b). Most research in this area has consisted of conceptual papers, descriptions of the empirical uses of open data or the design of technology and systems for harnessing the power of open data (Janssen, Charalabidis & Zuiderwijk, 2012, pp. 258–259). Furthermore, as open data as a concept is a new phenomenon and still in its early stages of growth, there is no proper framework for comparing open data policies on a broad range of aspects (Zuiderwijk & Janssen, 2013, p. 17).

This article will analyse the importance of open data, the problem of the lack of open data policies, provide an overview of existing systems used by the governance of Estonia to ensure access to open information, and make proposals on how to improve open data disclosure practices in Estonia.

2. The importance of open data policies

Governments should adopt open data policies aiming to encourage and guide the disclosure of government data and to derive benefits from its use. Even though different open data policies are in place at various levels of government, little systematic research has been done on the topic of open data policies. Open data policies are thus fragmented, and it is considered a challenge to create a coherent system between government agencies. There is a need to start comparing these public data policies to create a unified system for opening open data. Comparing open data policies across different parts and levels of government is essential for achieving a better understanding of the common and distinctive elements in the policies, as well as identifying the factors that determine policy variation and impact. This knowledge could help in the formulation of new open data policies as well as the enhancement of existing ones (Zuiderwijk & Janssen, 2013, p. 18).

Open data policies ensure the long-term transparency of government information. For that, government information must be preserved in an accessible manner and location (Jaeger & Bertot, 2010, p. 373). However, effective and efficient e-governance requires a high degree of trust in government information systems (Saxena, 2005, p. 505). If this trust is lacking, citizens are reluctant to provide their personal data to be processed by government systems, and the intended benefits from efficient and effective administration and governance is not generated in the first place (Priisalu & Ottis, 2017, p. 450). In order to ensure democratic governance and freedom of

information, information controllers should therefore be prepared to disclose open data collected in the course of their work (Bertot *et al*., 2010, p. 264). This is a very important aspect for democratic countries, including Estonia, because in this way the whole process of governing the country can be more transparent for the citizens. Transparency is an issue that considers not only short-term considerations (for example, citizens do have to have access to information they need), but also long-term ones (Halachmi & Greiling, 2013, pp. 574–576). As mentioned above, for long-term transparency, governments additionally have to be prepared to preserve the information in an accessible format and location for maintenance (McDermott, 2010, p. 405). As the information is stored in publicly accessible format, the citizens can access the data (at any time), which helps to ensure the transparency of government as people can find the information and thus potentially comprehend the reasons behind the decisions made by the government. This process leads to a more transparent government as citizens can also examine which data the government has been collecting.

Transparency is today regarded as an integral part of democratic governance. Democracies are considered to be more transparent by design, but, in fact, they simply tend to generate much more information than authoritarian systems (Jaeger & Bertot, 2010, p. 372). Disclosure of data raises two main preconditions for democratic governance: First, it assumes that public agencies are prepared for an open process that values influence, discourses, and exchanges as constructive and welcomes competing viewpoints and ideas (Lindstedt & Naurin, 2010, p. 310). Second, it leads to the expectation that the government will relinquish authority, at least to some level, necessitating significant changes in the public sector. Users can examine and verify whether the conclusions drawn from the data are valid and supported by opening the data, and they can study previously collected information to narrow the policy-making focus on a broad range of aspects (Zuiderwijk & Janssen, 2013, p. 18). Open data should result in open government, in which the government acts as an open system and interacts with its surroundings, rather than reinforcing current procedures. The release of data is expected to have several advantages, including boosting innovation and fostering economic growth. Not only should data be made public, but it should also be actively searched for feedback on how to improve government (Janssen, Charalabidis & Zuiderwijk, 2012, p. 260).

3. The obligation to disclose open data in Estonian law

Estonia is among the leading countries in the world in the field of e-governance (Kerikmäe & Nyman-Metcalf, 2020b, p. 31; Salumaa-Lepik, Kerikmäe & Nisu, 2021). A friendly political and economic environment that has been created in Estonia for ICT entrepreneurs—whether they are seeking commercial profit, developing technological innovations, advancing knowledge, or promoting civil initiatives—is one of the key drivers that helps Estonia advance in developing and launching different open government projects (Hoffmann, 2020a; Kassen, 2019, p. 569; Kerikmäe, Hoffmann & Chochia, 2018; Kerikmäe, Mölder & Chochia, 2019).

As a developed e-state, Estonia has been collecting and continues to collect an abundant amount of data about its citizens. Data is collected in a variety of places, and it is used by a variety of institutions and organizations in their everyday work to improve public services. In particular, the state publishes the data necessary for the provision of various public and proactive services, the latter in the form of direct public services, provided by an institution on its own initiative, on the basis of the presumed intent of persons and on the basis of data from databases belonging to the state information system (see Principles for Managing Services and Governing Information, Art. 3(2)). These services have been designed and improved in such a way that algorithms or artificial intelligence-driven functions, added in the information system, analyse already existing information in various databases and identify situations when a person acquires a certain right or benefit. In the case of a proactive service, the citizen does not have to apply for the service, but the local government offers the service to the corresponding target group, using the information available in public databases. When a right or obligation arises, the information system provides the service automatically or asks for the person's consent (and subsequently offers the service). One example of providing a proactive service at the birth of a child is when a medical professional makes an entry in the population register about the birth of a child and the new-born child automatically receives health insurance and is registered in the patient list of the mother's general practitioner. In this example, proactivity signifies that an entry in the population register for a born child activates the following services without the parent having to apply for it.

Estonia is obliged to publish the collected open data according to both EU and national law: Directive 2019/1024 of the European Parliament and of the Council on open data and the reuse of public sector information is the central directive for open data, establishing a minimum harmonization of national rules and practices on the reuse of publicly funded information with the

objective to support the smooth functioning of the internal market and the development of the information society in the EU. Specifically, Directive 2019/1024 sets the following rules:

- All public sector content that can be accessed under the rules of national access to documents is in principle freely available for reuse. With this Directive, public sector bodies are not able to charge more than the marginal cost for the reuse of their data, except in very limited cases.
- A particular focus is placed on high-value datasets, such as statistics or geospatial data. These datasets have high commercial potential as they can speed up the emergence of a wide variety of value-added information products and services.
- Public undertakings in the transport and utilities sector generate valuable data when providing services in the general interest that will enter into the scope of the Open Data and Public Sector Information Directive. Once the public undertakings make such data available, they will have to comply with the principles of transparency, non-discrimination and non-exclusivity set out in the Directive and ensure the use of appropriate data formats and dissemination methods.
- Some public bodies strike complex data deals with private companies, which can potentially lead to public sector information being "locked in". Safeguards are put in place to reinforce transparency and to limit the conclusion of agreements which could lead to exclusive reuse of public sector data by private partners.
- More real-time data, available via APIs (Application Programming Interface) can allow companies, especially start-ups, to develop innovative products and services, such as mobility apps. EU countries are required to develop policies for open access to publicly funded research data.

However, in contrast to many other EU Member States, Estonia has also on national level established an explicit right to full transparency about the use of both personal and public data—a right which is even constitutionally protected. Namely, Article 44 of the Constitution of the Republic of Estonia protects in its first paragraph the right to "freely receive information disseminated for public use", which is further supported by a duty imposed by paragraph 2 on "all state agencies, municipalities and their officials" to provide information about their activities, pursuant to a procedure provided by a law, to Estonian citizens at their request. The access to personal data is guaranteed in paragraph 2, according to which "Estonian citizens have the right to access information about themselves held in state agencies and municipalities and in state and municipal archives.

Other EU Member States usually do not guarantee these rights on a constitutional level and additionally to a much less extent. For instance, Article 5 of the German Basic Law only grants the right “to inform oneself without hindrance from generally accessible sources”, and also the details regulated in the Act on the Regulation of Access to Federal Information provide a much more limited access than guaranteed by the Estonian constitution.

Information published as open data involves information related to legislation, various economic, traffic, and weather data. In fact, the state still has collected beyond that a wealth of more data which could be published to different target groups who would be able to generate value out of the usage of this data, providing benefits to both the national economy and the quality of governance. The Amendment Act of Estonian Public Information Act entered into force on 10 December 2021 and had the objective to bring the Estonian Public Information Act in line with Directive 2019/1024 on open data and, according to the Explanatory Memorandum to the Public Information Act, the reuse of public sector information and to increase the availability and reusability of open data to foster innovation and the economy, the smoother functioning of the internal market and the information society. The Explanatory Memorandum to the Public Information Act also describes how allowing the reuse of data held by a public sector body provides added value for reusers, end-users, and the society, and often for the public authority concerned, as it promotes transparency and accountability. The amendments give effect to the requirements of Directive 2019/1024 of the European Parliament and of the Council on the reuse of public data and public sector information. The Commission shall evaluate the application of this Directive no earlier than on 17 July 2025, so even though Member States had to bring into force the laws, regulations, and administrative provisions necessary to comply with this Directive by 17 July 2021 at the latest, many states have not yet established comprehensive open data policies since last summer.

The new Estonian Public Information Act intends to solve practical bottlenecks that have arisen in the interpretation of the definition of open data and the principles related to reuse provided in the current law. For instance, paragraph 31, Section 83 of the Estonian Public Information Act establishes the obligation to make such open data that are updated frequently or in real time because they change continuously or expire rapidly available for reuse through the Application Programming Interface and, where appropriate, as bulk downloads immediately after collection or in the case of manual updates. If this is considered too “burdensome for the holder”, the data shall be made available in the shortest possible time and with technical constraints that do not unduly prejudice the economic and social potential of the data. According to Section 9 of the same

paragraph, open data shall, as a rule, be released for reuse without conditions. Where the imposition of conditions for reuse is necessary in the public interest, such conditions shall be objective, proportionate, and non-discriminatory, and conditions for recovery shall be available in machine-readable form and in an open format.

This is the first time the Estonian government has regulated the obligation to publish open data at the level of law. Until this amendment of the Estonian Public Information Act, *id est* under the previous version of the Act (which entered into force on 1 April 2019), the obligation to publish open data was merely established as a general duty; the obligation was to disclose open data where possible and appropriate and does not infringe the rights of the data subject. This change of the new version of Estonian Public Information Act, which entered into force on 10 December 2021, is indeed significant as it imposes a real obligation to disclose open data. This is the first time in Estonian history that private entities have to start publishing data they have collected as far as it qualifies as open data in order to be in compliance with the law. This amendment to the law potentially necessitates the convening of an expert group to develop guidelines at Estonian level on which data are included in the open data and on what timeframe and on what platform they should be published.

4. Data platform tools in Estonia

Unless there is a central platform where open data is published, there can be impairment of transparency, as a lot of open data is published without a clear structure (Conradie & Choenni, 2014, p. 11). In other words, the mere abundance of data and information made available at some point may impair transparency, as users may be unable to locate data searched for, even though the respective data exist and are made public (Jaeger & Bertot, 2010, p. 372). This can be the case if government agencies do not have a central environment in which disclosures are uploaded, or if these environments are existing, but are not designed as user-friendly, which means that it is difficult for users, or citizens, to navigate these environments. Governments mostly make their data available through platforms. A key benefit of their platforms is that if all government agencies use the same platform, i.e., all information is available from one environment, then it is easier for citizens to seek and obtain information as well as interact with public administrators (Wijnhoven, Ehrenhard & Kuhn, 2015, p. 30). Platforms for open government data are a relatively new phenomenon, which has emerged in the last decade and which also has been the object of scholarly research in terms of their potential to enable improved public service innovation, increase

transparency, and provide broader social benefits (Bonina & Eaton, 2020, p. 1). Another benefit of open data platforms is that they offer users the possibility to provide feedback to the policy decision-makers, to gain insight and knowledge, and to overall participation (Ruijer *et al*., 2017, p. 477)—an architecture which thus additionally strengthens the basic human right to seek and obtain information according to the above-mentioned Article 10 of the European Convention of Human Rights. To accomplish open data innovation, platform governance must be used to develop an ecosystem of active actors on both the demand and supply sides of an open government data platform (Bonina & Eaton, 2020, p. 3). Ease of access is crucial for making users use the platform.

4.1 The X-Road

X-tee ('The X-road'), the "backbone" of governmental data (Paide *et al*., 2018, p. 34), is used for secure data exchange and interoperability in the public and private sector (Saputro *et al*., 2020, p. 216). The X-road is a data exchange layer for information systems which forms the heart of Estonian digital services, as it links the different databases and information systems, allowing fast and secure data exchange between these databases (Tupay, 2020). The X-road is accessed via the eesti.ee main governance website or other authorities' websites; any data that originates from other databases or, conversely, needs to be added to a database, passes through the X-Road platform. The members of the X-road are primarily various public authorities, but also private companies, such as banks or telecommunications companies (Republic of Estonia Information System Authority, 2021a). The government's vision behind the creation of the X-road was to keep databases available seven days a week and 24 hours a day (Republic of Estonia Information System Authority, 2021b). All those granted access to the X-road can use the services and data of other members to improve their own business processes (even though an explicit prior consent is required for private entities to access personal data). For instance, when local police tries to check a driver's license in the event of a real-live incident, the Estonian driver will no longer need to carry a physical driver's license, as the police officer will be able to make an operative inquiry on the spot, via the X-road, in the database of the Republic of Estonia Road Administration, using an identification document to control driver's licenses. The Tax and Customs Board has a similar data service that allows checking tax arrears of private or legal persons (Republic of Estonia Information System Authority, 2021b). Another example is the service where, upon registration of a child's birth in the population register, the child is automatically added to the list of his or her mother's family medicine centre.

4.2 The once-only principle

Another feature of the X-road is the 'once-only principle' (OOP). By means of the OOP, which is anchored in Estonian law (Estonian Law on Public Information, Art. 43(3)), personal data is made available to the state by the person concerned only once; public authorities must contact this body (and not the person concerned again) for future data processing operations.

The Estonian data protection framework is in this context remarkable as it involves a special approach to take care of the data subject's actual protection interests: While at first (and perhaps even at second) sight, the X-Road and the OOP may seem to violate the GDPR's principle of purpose limitation (Martini & Wenzel, 2017, pp. 749–758), the data subject's interests are nevertheless taken into account, as a neglect of the data subject's consent at the access level is compensated by comprehensive transparency at the processing level. If the person concerned is really seriously interested in who has accessed which personal data, based on what authorization and for what specific purpose, and how they have processed it, the state portal provides, upon request, exhaustive (and untamperable) information in real time on that portal via a "data tracker". When an authority assesses an individual's data, it leaves a digital footprint displayed in real time to the respective data, subject upon request, indicating which authority viewed the data at what time, and an explanation on the entity's access to these data and the respective justification for exercising this right.

Less transparency in the consent stage is therefore compensated by maximum transparency in the data processing stage (Hoffmann, 2020b). If one now takes into account that a growing proportion of the consents in everyday digital practice are granted with little or none consideration at all, as the user is usually primarily interested in the specific application, and less in her data, this architecture serves the actual interests of the data subject much better, as the data subject is only confronted with information that provides transparency if the subject actually requests it—and then receives it immediately and in full and to the desired extent.

Access to any of these personal data can be traced directly, and in case of doubt, the Estonian data protection inspector is available for assistance. Obviously, the data tracker supports the data subject's interest only after the (possibly unlawful) access has already taken place, but the drastic sanctions (up to 1 year imprisonment, according to §157 II of the Estonian Criminal Code) for the unlawful access to personal data has an enormous preventative effect (Kerikmäe & Nyman-Metcalf, 2020b, p. 47). The system is very popular in Estonia; the data-tracker has over 30,000 uses per month. One of the aspects of the X-road in Estonia is that individuals (citizens and

residents of Estonia) can quickly examine what data the authorities have on them by going to one website (www.eesti.ee), which links to all public services and databases (Kerikmäe & Nyman-Metcalf, 2020b, p. 47). All of the previously mentioned will reduce the possibility of data breaches, which is one of the most likely issues with data transfer. The data exchange layer of the X-road has the potential to play an important role also for the disclosure of non-personal data, as data could be aggregated through this platform and published, for example, on the eesti.ee website.

4.3 The eesti.ee state portal

In Estonia, the government uses the website eesti.ee as a central website for every public service. Eesti.ee is a state-maintained portal and functions as the e-Estonian information gateway: The portal is used by the authorities to publish information, allow access to electronic services, and forward documents and notifications. All governmental services are linked to that website. The Estonian state and all stakeholders in the public, private and third sector offer their public services through the portal eesti.ee pursuant to the legal acts valid in the Republic of Estonia.

4.4 Avaandmed.eesti.ee—the official Estonian open data portal

This portal is explicitly designed for open data and provides everyone the opportunity to access and visualize open data, including usage stories that are based on open data. In April 2022, it included 879 datasets by 2,212 publishers, which are all freely accessible. Open data on this portal is published by the public, private or third sector, which means that every sector is able to upload their open data to be accessed. Users can see different datasets, specified according to categories, specifically Population and Society, Energy, Education, Culture and Sport, Environment, Economy and Finance, Science and Technology, Region and Cities, Agriculture, Fisheries, Forestry and Food, Health, Transport, Government and Public Sector, Justice, Legal System and Public Safety.

4.5 Riigiteataja.ee—laws and regulations

Another platform through which the Estonian government releases open data to its citizens is *Riigi Teataja*, Estonia's official state gazette. *Riigi Teataja* employs ICT resources to provide more convenient and wider access to the information it actually requires by law. It also provides easy-to-handle mechanisms to compare current and previous versions of laws, government rules, and other documents. These few examples appear to be a natural component of the government's and parliament's (*Riigikogu*) operations in terms of transparency, but a comparison with other

countries reveals that such openness is not yet universal. Returning to the example of *Riigi Teataja*, a lot of open data have already provided value by helping in the prevention of various evils today, and it is possible that no one was aware of the change in the law in time. This has potentially saved public money, as people are aware of the changes in the law and can therefore avoid illegal behaviour or refrain from illegal activities.

5. Open data and data protection

The European data protection framework acknowledges two categories of data: personal and non-personal data. The latter can be subdivided into data that is always non-personal (as it is never related to an identified or identifiable natural person), and there is also data that is not personal any more, as the linkage to a natural person has been removed (Finck & Pallas, 2020, p. 13). Open data policies may, nevertheless, be in conflict with the individual's right to information privacy as protected by the GDPR (Kulk & Loenen, 2012, pp. 196–197), as there is also a data protection risk when publishing open data in those cases where differentiation between personal and non-personal data or, which will be more and more the case in the future, e.g., with ubiquitous data collection/surveillance in smart cities, where the entanglement of individually non-personal data leads to patterns which allow for the identification of individual data. When disclosing open data, the authority must be 100% sure that the data disclosed are in no way personal data or that they can be linked in any way to a specific person, as this would constitute an infringement that could result in a fine of up to 20 million euros. Although many governmental organizations might be willing to open up their data, they lack the guiding principles derived from practical case studies that help them in doing this. Practical frameworks need to be created that would support agencies to decide whether a dataset is eligible to release or not (Zuiderwijk *et al*., 2012, p. 91).

Even though the X-tee service renders the possibility of data breaches low, as the data is moved in a controlled manner and the person can control who has processed their data and when, it does not eliminate the possibility in general. Beyond legal constraints, such as the GDPR, there are also several ethical concepts to consider when exchanging data from human individuals, including de-identification (Forero, Curioso & Patrinos, 2021, p. 2). Users of open data should not be able to identify persons by using a dataset, which the controller should prevent by respective technical mechanisms (Janssen, 2011, p. 451). In specific cases of highly sensitive information, such as information about health data or data revealing racial or ethnic origin, there is the option for the submission of processed data, such as summary statistics (Forero, Curioso & Patrinos, 2021, p. 2).

The GDPR comprises the right to access and rectify data about oneself and the need for control by an independent authority (Nyman-Metcalf, 2014, p. 41). As it comes to publishing data, a considerable amount of personal data could be impersonalized either by anonymization or pseudonymization, and therefore this data could be used and published as open data.

In Estonia, there has been a successful prototype of this GDPR-compliant pseudonymization, when the governmental agency (here the Estonian Road Administration) cooperated with a private entity (the telecommunication company Telia) in granting access to the anonymous movement data of individual passengers and thus rendered their work processes and trajectories more efficient. The Estonian Transport Administration received from Telia data which indicates the number of people moving on specific road sections with an accuracy of up to an hour. The data, which were originally derived from the individual passenger's personal data from positioning their phone, were anonymized to the level that merely the number of passengers on a specific road section remained detectable. Neither the Transport Administration nor Telia knew or collected the name, gender, age, or other personally identifiable information of the passengers (Pau, 2021).

This is a good example of how collection of personal data could be "downgraded" to open data, which can be openly disclosed in a subsequent step and consecutively enable government administrations to work more efficiently. A similarly successful collaboration was conducted during the first Covid-19 wave in Estonia in spring 2020, when telecommunication companies collected and analysed impersonal data about the location of people obliged to stay in quarantine at home. No data other than the location data of otherwise anonymous members of this group were collected in this study, keeping the procedure GDPR compliant.

6. Proposals

Based on these analysis and case studies, the following proposals can be made in order to further improve open data accessibility:

6.1 Development and publication of a framework comparing open data policies

For the time being, national open data policies are fragmented both at national level and the EU level, even though the Directive calls for harmonization. Public data policies should be the object of intensified comparative research, which would essentially facilitate the creation of a unified

system for disclosing open data. Without a central framework, which maybe should be published on the EU level, it is difficult to create a coherent system. With the EU level framework, the Member States could create a similar system for disclosing open data that could later be accessed by users, which could be beneficial on different levels, including economic. This framework could also establish guidelines on how and to which extent personal data ought to be anonymized before publishing.

6.2 Increasing the number and the extent of citizens' access to databases

Currently there are different and partly overlapping databases granting access to open data. Supplementing the first proposal, and assuming the successful establishment of a framework binding all EU Member States, a next step would be enhancing the structures of databases. The Estonian example could serve as a functioning model for a central platform for open data disclosure, enabling citizens locate data more easily. Also, that central platform could be provided with a guide about the different types of datasets each database contains, i.e., if the user has a general idea where to look for the data, it would be easier for the user to navigate through the database. The current Estonian official open data portal avaandmed.eesti.ee would be suitable to serve as such a central platform for Estonia; however, for the time being, the webpage is not designed as user-friendly, as there are over 800 data sets without an overarching system organizing these data. In addition, a central database could be established also for EU-related datasets.

6.3 Publishing open data that is actually useful

Estonia ranks only 24th out of 32 countries in the OECD (2019) Open, Useful and Re-usable data (OURdata) Index in 2019, i.e., even though Estonia's governmental agencies have gathered a wealth of different information, they still struggle to publish OURdata. The issue has not been researched or evaluated in further detail since 2019, but taking into account that the Estonian Public Information Act was amended only in December 2021, and that the purpose of the latest amendment was to increase the availability and reusability of open data, it is very likely that Estonia still ranks in the lower part of the OURdata index. However, as by now Directive 2019/1024 has been transposed into the new Public Information Act, which has been amended, which means that there are steps that Estonia has taken in regard to disclosing open data, we should wait and see where Estonia ranks the next time OURdata index is concluded. There is potential to rise in the rankings as there are now better legal requirements that should make the

reused data held by a public sector or public authority itself more useful as the new amendment on Public Information Act promotes transparency and accountability, which means that the disclosed data should be of better quality, in the sense of its usefulness, compared to the data that was published in 2019.

If the disclosed open data remains ranking low on the OURdata index, then the disclosing of open data is only formal and only done to be technically compliant with law. As mentioned above, the purpose of both the EU directives and Estonian law is to add value for reusers, end-users, the society, and often for the public authority concerned, as the goal for open data is to promote transparency and accountability.

7. Conclusion

In conclusion, governments are obliged to publish open data for the sake of transparency and to guarantee their citizens the right to obtain information. This right derives from multiple different legislations, most notably the European Convention on Human Rights. Unfortunately, there has been a lack of central guidelines for publishing open data. Directive (EU) 2019/1024 orders Member States to publish open data, but as the Commission will not evaluate this Directive earlier than on 17 July 2025, there are three and a half years of uncertainty on the strategy ahead. As of now, open data policies are fragmented, and no coherent system enables smooth cooperation in open data exchange between government agencies. This situation could be solved by establishing detailed, yet comprehensive, guidelines, which would instruct governments on how, where, and under which legal requirements are open data to be published.

The disclosure of open data is expected to have several advantages, including boosting innovation and fostering economic growth. Another benefit of open data platforms is that they offer users affordances to inform the policy process, gaining insight and knowledge, and overall participation. Additionally, the disclosure of open data can ensure the long-term transparency of government information. Information controllers should be prepared to release open data obtained in the course of their tasks in order to support democratic governance and freedom of information.

The obligation for Estonian agencies to publish the collected open data derives both from the EU and the national legislature—Directive 2019/1024 on the EU level and the Estonian Public Information Act on the national level. Making open data public for citizens can be smoothly achieved via central governmental platforms. One of the major advantages of these platforms is

synergy, i.e., if all government agencies use the same platform, all information is accessible from a single location, making it easier for individuals to search and get information as well as communicate with public officials. For example, the Estonian government uses platforms such as eesti.ee, which is used by the authorities to publish information, allow access to electronic services, and forward documents and notifications, riigiteataja.ee to publish legal acts, and Avaandmed.eesti.ee as an explicit, yet slightly unorganized central platform for open data.

Before any open data is published on the above-mentioned websites, the authority has to verify that the data disclosed is not (or no longer) personal data and that they can neither by the mere interaction with other datasets "crystallize" it into personal data, as this data would then have to be processed as GDPR compliant. Many government agencies would be prepared to share their data but often lack guidelines. Practical guidelines must be developed to assist agencies in determining whether a dataset is eligible for release. Guidelines could provide instructions on how and to which extent personal data can be sufficiently impersonalized before public disclosure. Personal data can be impersonalized either by anonymization or pseudonymization, and therefore this data could be used and published as open data.

Elsa-Maria Tropp acquired a bachelor's degree in law from the University of Tartu. She is currently enrolled as a master's student in the Law and Technology program at Tallinn University of Technology.

Dr. **Thomas Hoffmann** is a tenured assistant professor of private law at the Department of Law (TalTech Law School) of Tallinn University of Technology, Estonia. He graduated (in 2005) and also obtained his PhD in law at the University of Heidelberg (in 2006). Thomas' research focuses on comparative private law, here especially on insolvency law, private international law, contracts in digital environments, and consumer law. He has provided comprehensive research on Estonian, German, and international law to various stakeholders within numerous EC tenders. Thomas keeps track with forensic issues by serving as Of Counsel for the bnt Attorneys-at-Law firm in Tallinn. A list of his publications is available at http://bit.ly/1fz4RkT.

Dr. **Archil Chochia** is a senior researcher at TalTech Law School of Tallinn University of Technology. Archil obtained his doctoral degree from TalTech in 2013. His academic publications include the books *Political and Legal Perspectives of the EU Eastern Partnership Policy* (Springer, 2016), *Brexit: History, Reasoning and Perspectives* (Springer, 2018) and *Russian Federation in the Global Knowledge Warfare: Influence Operations in*

Europe and Its Neighbourhood (Springer, 2021). Archil is a senior fellow of Weinstein International Foundation.

References

Bertot, J. C.; Jaeger, P. T. & Grimes, J. M. (2010), 'Using ICTs to create a culture of transparency: E-government and social media as openness and anticorruption tools for societies,' *Government Information Quarterly*, vol. 27, no. 3, pp. 264–271. https://doi.org/10.1016/j.giq.2010.03.001

Bonina, C. & Eateon, B. (2020), 'Cultivating open government data platform ecosystems through governance: Lessons from Buenos Aires, Mexico City and Montevideo,' *Government Information Quarterly*, vol. 25, no. 3. https://doi. org/10.1016/j.giq.2020.101479

Conradie, P. & Choenni, S. (2014), 'On the barriers for local government releasing open data,' *Government Information Quarterly*, vol. 31(1), pp. 10–17. https://doi. org/10.1016/j.giq.2014.01.003

Council of Europe Committee of Ministers Recommendation No. R (97) 20 of the Committee of Ministers to Member States on "hate speech", 30.10.1997.

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public sector information, *OJ* L 172, 26.6.2019, pp. 56–83.

Estonian Public Information Act, *Riigi Teataja* I, 30.11.2021, 17.

European Convention on Human Rights, 4.11.1950. Retrieved from https://www. echr.coe.int/documents/convention_eng.pdf [accessed Apr 2022]

Finck, M. & Pallas, F. (2020), 'They who must not be identified—distinguishing personal from non-personal data under the GDPR,' *International Data Privacy Law*, vol. 10, no. 1, pp. 11–36. https://doi.org/10.1093/idpl/ipz026

Forero, D. A.; Curioso, W. H. & Patrinos, G. P. (2021), 'The importance of adherence to international standards for depositing open data in public repositories,' *BMC Res Notes*, vol. 14, no. 1, art. 405. https://doi.org/10.1186/ s13104-021-05817-z

German Basic Law (*Grundgesetz*), Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 u. 2 Satz 2 des Gesetzes vom 29. September 2020 (BGBl. I S. 2048) geändert worden ist.

Halachmi, A. & Greiling, D. (2013), 'Transparency, e-Government, and accountability,' *Public Performance & Management Review*, vol. 36, no. 4, pp. 562–584. https://doi.org/10.2753/PMR1530-9576360404

Hamuľák, O.; Kocharyan, H. & Kerikmäe, T. (2020), 'The contemporary issues of post-mortem personal data protection in the EU after GDPR entering into force,' *Czech Yearbook of Public and Private International Law*, vol. 11, pp. 225−238.

Hoffmann, T. (2020a), 'Schutz oder Beschränkung der Privatautonomie durch den digitalen Staat: Eine Untersuchung am estnischen Beispiel,' in T. Zarandia, E. Kurzynsky-Singer & L. Shatberashvili (eds.) *Private Autonomy as a Fundamental Principle of Civil Law*, Tbilisi: Ivane Javakhishvili Tbilisi State University, pp. 116−119.

Hoffmann, T. (2020b), 'The impact of digital autonomous tools on private autonomy,' *Baltic Yearbook of International Law Online*, vol. 18, pp. 18−31.

Jaeger, P. T. & Bertot, J. C. (2010), 'Transparency and technological change: Ensuring equal and sustained public access to government information,' *Government Information Quarterly*, vol. 27, no. 4, pp. 371–376. https://doi.org/10.1016/j.giq.2010.05.003

Janssen, K. (2011), 'The influence of the PSI directive on open government data: An overview of recent developments,' *Government Information Quarterly*, vol. 28, no. 4, pp. 446–456. https://doi.org/10.1016/j.giq.2011.01.004

Janssen, M.; Charalabidis, Y. & Zuiderwijk, A. (2012), 'Benefits, adoption barriers and myths of open data and open government,' *Information Systems Management*, vol. 29, no. 4, pp. 258–268. https://doi.org/10.1080/10580530.2012.716740

Kassen, M. (2019), 'Open data and e-government—related or competing ecosystems: a paradox of open government and promise of civic engagement in Estonia,' *Information Technology for Development*, vol. 25, no. 3, pp. 552–578. https://doi.org/10.1080/02681102.2017.1412289

Kerikmäe, T.; Hoffmann, T. & Chochia, A. (2018), 'Legal technology for law firms: Determining roadmaps for innovation,' *Croatian International Relations Review*, vol. 24, no. 81, pp. 91−112. https://doi.org/10.2478/cirr-2018-0005

Kerikmäe, T.; Mölder, H. & Chochia, A. (2019), 'Estonia and the European Union,' in F. Laursen (ed.) *Encyclopedia of European Union Politics*, Oxford: Oxford University Press, pp. 1−18. https://doi.org/10.1093/acrefore/9780190228637.013.1105

Kerikmäe, T. & Nyman-Metcalf, K. (2020a), 'Machines are taking over—are we ready? Law and artificial intelligence,' *Singapore Academy of Law Journal*, vol. 33, pp. 24–49.

Kerikmäe, T. & Nyman-Metcalf, K. (2020b), 'The rule of law and the protection of fundamental human rights in an era of automation,' in J.-S. Gordon (ed.) *Smart Technologies and Fundamental Rights*, Philosophy and Human Rights, Leiden: Brill, pp. 221−239. https://doi.org/10.1163/9789004437876_011

Kulk, S. & Loenen, B. (2012), 'Brave new open data world?' *International Journal of Spatial Data Infrastructures Research*, no. 7, pp. 196–206. https://doi.org/10.2139/ssrn.2039305

Lindstedt, C. & Naurin, D. (2010), 'Transparency is not enough: Making transparency effective in reducing corruption,' *International Political Science Review*, vol. 31, no. 3, pp. 301–322. https://doi.org/10.1177/0192512110377602

Martini, M. & Wenzel, M. (2017), '"Once only" versus "only once": Das Prinzip einmaliger Erfassung zwischen Zweckbindungsgrundsatz und Bürgerfreundlichkeit,' *DVBl* 2017, pp. 749–758.
https://doi.org/10.1515/dvbl-2017-1206

McDermott, P. (2010), 'Building open government,' *Government Information Quarterly*, vol. 27, no. 4, pp. 401–413. https://doi.org/10.1016/j.giq.2010.07.002

Napoli, P. M. & Karaganis, J. (2010), 'On making public policy with publicly available data: The case of US communications policymaking,' *Government Information Quarterly*, vol. 27, no. 4, pp. 384–391.
https://doi.org/10.1016/j.giq.2010.06.005

Nyman-Metcalf, K. (2014), 'e-Governance in law and by law: The legal framework of e-governance,' in T. Kerikmäe (ed.) *Regulating eTechnologies in the European*
Union, Heidelberg: Springer Verlag, pp. 33−51.
https://doi.org/10.1007/978-3-319-08117-5_3

Nyman-Metcalf, K. & Papageorgiou, I. (2018), 'The European Union Digital Single Market—Challenges and impact for the EU Neighbourhood states,' *TalTech Journal of European Studies*, vol. 8, no. 2, pp. 7–23.
https://doi.org/10.1515/bjes-2018-0013

OECD (2019), 'Open, Useful and Re-usable data (OURdata) Index.' Retrieved from https://www.oecd.org/gov/digital-government/ourdata-index-policy-paper-2020. pdf [9 May 2022]

Paide, K.; Pappel, I.; Vainsalu, H. & Draheim, D. (2018), 'On the systematic exploitation of the Estonian data exchange layer X-Road for strengthening public–private partnerships,' in *ICEGOV '18: Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance*, pp. 34–41. https://doi.org/10.1145/3209415.3209441

Pau, A. (2021), 'Transpordiamet hakkab saama Telialt inimeste liikumisandmeid,' *Delfi*, 21 September. Retrieved from https://forte.delfi.ee/artikkel/94639549/ transpordiamet-hakkab-saama-telialt-inimeste-liikumisandmeid [accessed Apr 2022]

Priisalu, J. & Ottis, R. (2017), 'Personal control of privacy and data: Estonian experience,' *Health and Technology*, no. 7, pp. 441–451. https://doi.org/10.1007/s12553-017-0195-1

Principles for Managing Services and Governing Information, *Riigi Teataja* I, 31.05.2017, 7

Public Information Act Amendment Act, *Riigi Teataja* I, 30.11.2021, 3.

Republic of Estonia Information System Authority (2021a), 'Data exchange layer *X-tee*.' Retrieved from https://www.ria.ee/en/state-information-system/x-tee. html [accessed 17 Dec 2021]

Republic of Estonia Information System Authority (2021b), 'The 20th anniversary of *X-tee*.' Retrieved from https://www.ria.ee/en/calendar/20th-anniversary-x-tee. html [accessed 17 Dec 2021]

Riigiportaal eesti.ee (n.d.), 'Terms of use of State Portal eesti.ee.' Retrieved from https://www.eesti.ee/en/using-the-state-portal/terms-of-use-of-state-portaleestiee [accessed 17 Dec 2021]

Ruijer, E.; Grimmelikhuijsen, S.; Hogan, M.; Enzerink, S.; Ojo, A. & Mejer, A. (2017), 'Connecting societal issues, users and data. Scenario-based design of open data platforms,' *Government Information Quarterly*, vol. 34, no. 3, pp. 470–480. https://doi.org/10.1016/j.giq.2017.06.003

Salumaa-Lepik, K.; Kerikmäe, T. & Nisu, N. (2021), 'Data protection in Estonia,' in E. Kiesow Cortez (ed.) *Data Protection around The World. Privacy Laws in Action*, The Information Technology and Law Series, 33, Cham: Springer, pp. 23−57. https://doi.org/10.1007/978-94-6265-407-5

Saputro, R.; Pappel, I.; Vainsalu, H.; Lips, S. & Draheim, D. (2020), 'Prerequisites for the adoption of the X-Road interoperability and data exchange framework: A comparative study,' in *2020 Seventh International*

Conference on eDemocracy & eGovernment, pp. 216–222. https://doi.org/10.1109/ICEDEG48599.2020.9096704

Saxena, K. B. C. (2005), 'Towards excellence in e-governance,' *International Journal of Public Sector Management*, vol. 18, no. 6, pp. 498–513. https://doi.org/10.1108/09513550510616733

The Constitution of the Republic of Estonia, *Riigi Teataja* I, 15.05.2015, 2.

Tupay, P. K. (2020), 'Estonia, the digital nation: reflections on a digital citizen's rights in the European Union,' *European Data Protection Law Review*, vol. 6, no. 2, pp. 294–300. https://doi.org/10.21552/edpl/2020/2/16

Wijnhoven, F.; Ehrenhard, M. & Kuhn, J. (2015), 'Open government objectives and participation motivations,' *Government Information Quarterly*, vol. 32, no. 1, pp. 30–42. https://doi.org/10.1016/j.giq.2014.10.002

Zuiderwijk, A. & Janssen, M. (2013), 'Open data policies, their implementation and impact: A framework for comparison,' *Government Information Quarterly*, vol. 31, no. 1, pp. 17–29. https://doi.org/10.1016/j.giq.2013.04.003

Zuiderwijk, A.; Janssen, M.; Meijer, R.; Choenni, S.; Charalabidis, Y. & Jeffery, K. (2012), 'Issues and guiding principles for opening governmental judicial research data,' in *International Conference on Electronic Government*, vol. 91, pp. 90–101. https://doi.org/10.1007/978-3-642-33489-4_8

Appendix 1. Non-exclusive licence

A non-exclusive licence for reproduction and publication of a graduation thesis[1]

I, Elsa-Maria Tropp

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis Open Data: A Stepchild in e-Estonia's Data Management Strategy?

supervised by supervisors Dr. Thomas Hoffmann and Dr. Archil Chochia

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

29.12.2022

[1] *The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period*